Double compressed doctored image anti-forensics with statistical forensics analysis

A thesis submitted

in fulfillment of the requirement for the award of degree

of

Doctor of Philosophy

Submitted by

Gurinder Singh

Registration Number: 901406015

Under the Supervision of

Dr. Kulbir Singh

Professor, ECED

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY,
PATIALA-147004

June 2019

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "**Double compressed doctored image anti-forensics with statistical forensics analysis**", for the award of degree of **Doctor of Philosophy** in Electronics and Communication Engineering Department (ECED), Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision and guidance of Dr. Kulbir Singh, Professor, ECED, Thapar Institute of Engineering and Technology, Patiala.

The results presented in this thesis have not been submitted in part or in full to any other University or Institute for the award of any degree or diploma.

Gurinder Singh

Gurinder Singh

This is to certify that the above statement made by the candidate is correct to the best of my knowledge and belief.

Dr. Kulbir Singh

Professor, ECED

Thapar Institute of Engineering and Technology,

Patiala, India

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere, humble and deep sense of gratitude to my supervisor **Dr. Kulbir Singh**, Professor, Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala, for his support and motivation throughout the course of this research work. From last four years of research, I am unable to find any occasion when he could not spare time to discuss the problems related to my research. The enthusiastic supervision and beneficial remarks during inspiring discussions helped a lot to the accomplishment of this thesis.

I am highly grateful to **Dr. Alpana Agarwal**, Head of Electronics and Communication Engineering Department (ECED), Thapar Institute of Engineering and Technology (TIET), Patiala for her continuous support and encouragement in my research work. I would like to thank **Dr. Anil Kumar Verma**, Professor, Department of Computer Science and Engineering, TIET, Patiala for his guidance and cooperation. Moreover, I am also grateful to my doctoral committee members **Dr. Rajesh Khanna**, Professor, **Dr. Karmjit Singh Sandha**, Assistant Professor in ECED, TIET, Patiala and **Dr. M. D. Singh**, Associate professor in Electrical and Instrumentation Engineering Department, TIET, Patiala for their valuable suggestions during my entire research. I am also immensely thankful to my fellow researchers Amit, Kanwar, Amneet, and Mohit at Thapar Institute of Engineering and Technology, Patiala for helping me throughout my research.

I want to thank my parents for their love, affection, and support. It is only because of them I would able to face difficult times in my life. I am also extremely thankful to my wife Kirandeep for understanding and providing me enough time to complete my research work. Last but not the least I would like to acknowledge the love of my son, who is the most important part of my life.

This research work is supported by the Visvesvaraya PHD scheme for Electronics and IT, Ministry of Electronics and Information Technology, Government of India under Grant PhD-MLA/4(33)/2015-16/01. I would like to express my gratitude to the Ministry of Electronics and Information Technology for providing the financial support, without which it would not be possible for me to carry out this research work.

Gurinder Singh

ABSTRACT

The digital image information can be easily manipulated without leaving any footprints due to the availability of powerful image processing tools. Thus, there is an immediate need to confirm the legitimacy of digital images. Most of the cameras compress the image by employing Joint Photographic Experts Group (JPEG) standard. During the forgery creation, when this image is decompressed and re-compressed with different quantization matrix, it becomes double compressed doctored image. This JPEG double compression becomes an integral part of forgery creation. The detection and analysis of the historic information (for example, quantization matrix) related to JPEG compression in an image help the detective to find the truth of an image.

The research work is directed to design a two-stage forensic technique to evaluate the first quantization matrix from the partial double compressed JPEG images. In the first stage of the proposed scheme, automatic isolation of the doubly compressed part from doctored image is performed by exploring the JPEG ghost technique. The second stage analyzes this doubly compressed part to estimate the first quantization matrix or steps. In the latter stage, an optimized filtering scheme is also proposed to cope with the effects of the error. The experiment results confirm that the first stage of the proposed scheme provides an average percentage accuracy of 95.45%. The second stage provides an error less than 1.5% for the first ten Discrete Cosine Transform (DCT) coefficients, hence, outperforming the existing techniques. The experimental results consider the partial double compressed images in which the recompression is done with different quantization matrix.

The digital image forensics most often employs JPEG compression based forensic detectors. To confirm the capability of JPEG forensic detectors, an anti-forensic approach is desired. Thus, the further research is dedicated to design an enhanced JPEG anti-forensic technique in order to eliminate the blocking artifacts added during the JPEG compression in both spatial and DCT domains. In the presented approach, the grainy noise introduced in DCT domain by perceptual histogram smoothing can be reduced considerably with the application of suggested de-noising techniques. Two kinds of denoising operations are suggested, one is based on the minimization problem of Total Variation (TV) of energy and other on normalized weighted function. Afterwards, an advanced TV-based deblocking method is proposed to remove the blocking

artifacts in spatial domain. Subsequently, a decalibration algorithm is employed to get back the statistics of processed image to its normal situation. The experiment results indicate that the suggested anti-forensic schemes are better than the existing methods in attaining improved tradeoff between visual quality of an image and forensic undetectability, but with high computational cost.

The objective of counter JPEG anti-forensics is to expose the artifacts of JPEG compression in the presence of an anti-forensic attack. It is a challenging task because the application of JPEG anti-forensics conceals the artifacts of JPEG compression. Moreover, the analysis of JPEG anti-forensics reveals the limitations of existing forensic detectors. For example, most of the JPEG compression forensic techniques usually depend on the examination of first-order statistics based on the histogram of an image. These forensic techniques are easily circumvented by adopting an anti-forensic attack. Therefore, higher-order statistical analysis is required which is much robust against anti-forensic attacks. To resolve this issue, a counter JPEG anti-forensic approach is presented in this work by considering the second-order statistical analysis based on the Co-occurrence matrices (CMs). The proposed framework comprises of three stages: Selection of the target difference image, Evaluation of CMs, and Generation of second-order statistical feature based on CMs. In the first stage, we explore the effects of dithering operation of JPEG anti-forensics by analyzing the variance inconsistencies along the diagonals. Afterwards, CMs are evaluated in the second stage to highlight the effects of grainy noise introduced during the dithering operation. The third stage is devoted to generate an optimal second order statistical feature which is fed to the SVM classifier. The experimental results based on the UCID and BOSSBase dataset images demonstrated that the proposed forensic detector based on CM is very efficient even in the presence of anti-forensic attacks. Moreover, the proposed scheme is also evaluated in countering Median filtering and Contrast Enhancement (CE) anti-forensics. The multi-purpose nature of the proposed counter JPEG anti-forensic scheme is confirmed from the fact that it also provides better results in the detection of these anti-forensic techniques and other image operations such as Mean filtering (MeanF), Gaussian filtering (GF), Wiener filtering (WF), Scaling (Sca), and Rotation (Rot). The further research work can be concentrated to design a forensic technique based on other machine learning approaches such as Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) in order to detect the different image processing operations.

LIST OF ABBREVIATIONS

AC	Alternating Current
A-DJPG	Aligned Double JPEG
AUC	Area Under Curve
bpp	bits per pixel
CFA	Color Filter Array
CNN	Convolutional Neural Network
dB	deciBel
DC	Direct Current
DCT	Discrete Cosine Transform
DJPG	Double JPEG
GLF	Global and Local Feature
HVS	Human Visual System
IDCT	Inverse Discrete Cosine Transform
IJG	Independent JPEG Group
JPEG	Joint Photographic Experts Group
KL	Kullback-Leibler
MF image	Median Filtered image
MFLTP	Median Filter Local Ternary Patterns
MFRAR	Median Filter Residual Autoregressive
MLE	Maximum-Likelihood Estimation
MSE	Mean Squared Error
MIFT	Mirror Invariance Feature Transform
NA-DJPG	Non-Aligned Double JPEG
PCA	Principal Component Analysis
PGM	Portable Gray Map
p.m.f.	probability mass function
PRNU	Photo Response Non-Uniformity
PSNR	Peak Signal-to-Noise Ratio
QDCT	Quantized DCT
RNN	Recurrent Neural Network

RGB	Red, Green, Blue
ROC	Receiver Operating Characteristics
SAZ	Shrink-and-Zoom
SPAM	Subtractive Pixel Adjacency Matrix
SSIM	Structural SIMilarity
SVM	Support Vector Machine
TIFF	Tagged Image File Format
TV	Total Variation

LIST OF SYMBOLS

$\boldsymbol{I}$	Original uncompressed image
$\mathcal{T}$	JPEG image compressed from $\boldsymbol{I}$
X	Generic image pixel value matrix
q	Quantization table matrix
$(.)_{r,c}$	The (r, c)-th entry of an 8×8 block
$(.)_{r,c}^{l}$	The (r, c)-th entry of l-th 8×8 block of a matrix
D_{matrix}	DCT block matrix
$q_{block}(.)$	Block DCT coefficient quantization operator
γ	Laplacian parameter
c_{DQ}	Double quantized coefficient
d_e	Error function
d'	Difference calculated directly from the pixel values
S_{max}	Maximum acceptable size of the neighborhood during adaptive median filtering
C_s	Selected limited first quantization candidates
d_{out}	Improved error function
$H_{r,c}^{X}(k)$	Normalized DCT histogram
F	Noisy dithered image
U	Denoised image
$W(i,j)$	Weight function depending on the similarity between the two pixels
$d''(i,j)$	Euclidean distance between the two points
$\mathcal{G}_a(t)$	Gaussion window function
$TV(X)$	Total variation term
$T(X)$	Convex function
O_S	Projection operator
$G(X)$	Subgradient of $T(X)$
t_{step}	Positive step size
P_e	Minimum decision error
$\mathcal{F}_p$	Forgery created after the first step (i.e. Perceptual histogram smoothing) of the proposed anti-forensic framework

$\mathcal{F}_{pd}$	Forgery created after the second step (i.e. Denoising operation) of the proposed anti-forensic framework
$\mathcal{F}_{pdb}$	Forgery created after the third step (i.e. Improved TV-based deblocking) of the proposed anti-forensic framework
$\mathcal{AF}_{S_q}$	DCT histogram smoothing based anti-forensic scheme [95]
$\mathcal{AF}_{S_qS_b}$	Anti-forensic method based on dithering and deblocking operation [96]
$\mathcal{AF}_V$	A perceptual anti-forensic dithering technique [37]
$\mathcal{AF}_{S_u}$	SAZ attack based anti-forensic approach [101]
$\mathcal{AF}_F$	TV-based anti-forensic scheme [38]
$\mathcal{AF}_{Fan}$	Four-step JPEG anti-forensic scheme [39]
$\mathcal{AF}_1$	Proposed anti-forensic technique with an improved TV-based deblocking operation and suggested denoising algorithm based on constrained minimization problem of total variation of energy.
$\mathcal{AF}_2$	Proposed anti-forensic technique with an improved TV-based deblocking operation and suggested denoising algorithm based on the normalized weighted function.
K_F	JPEG blocking artifacts detector [63]
K_F^q	Quantization table estimation based detector [63]
K_{Weiqi}	JPEG recognizing detector [44]
K_{Weiqi}^q	Quantization step estimation detector [44]
K_V	JPEG forensic detector based on total variation [97, 103]
K_L	Calibration feature [98]
K_U^1 and K_U^2	JPEG blocking artifacts detectors [38]
K_{Li}^{S100}	100-D intra and inter block correlation feature [99 - 100]
K_P^{S162}	162-D SPAM feature [28]
K_{AR}^{S10}	Autoregressive model based detector [104]
K_{SPAM}^{S686}	686-D SPAM feature [28]
K_{SRM}^{S714}	Residual-based feature [29]
K_{CM}	Proposed second-order statistical feature for countering JPEG anti-forensics
$\mathcal{M}_{\mathcal{J}}$	Median filtered image from $\mathcal{J}$ by using square window of size 3×3
$\mathcal{AF}_{Wu}$	Median filtering anti-forensic scheme based on pixel difference distribution [27]

$\mathcal{AF}_{Dang}$	Anti-forensics of median filtering through random pixel modification [143]
$\mathcal{AF}'_{Fan}$	Median filtering anti-forensic approach using variational deconvolution [119]
K_{GLF}^{S56}	Detector based on the statistical analysis of pixel value difference domain [139]
K_{MFRAR}^{S10}	Autoregressive feature based forensic detector [141]
K_{LTP}^{S220}	Median filter local ternary patterns (MFLTP) feature [140]
Γ	Contrast enhanced image
$\mathcal{AF}_{Cao}$	Anti-forensic technique for contrast enhancement based on the integration of local random dithering and modification of gray level histogram [145]
$\mathcal{AF}_{Ravi}$	Contrast enhancement anti-forensics based on TV-based optimization problem [146]

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

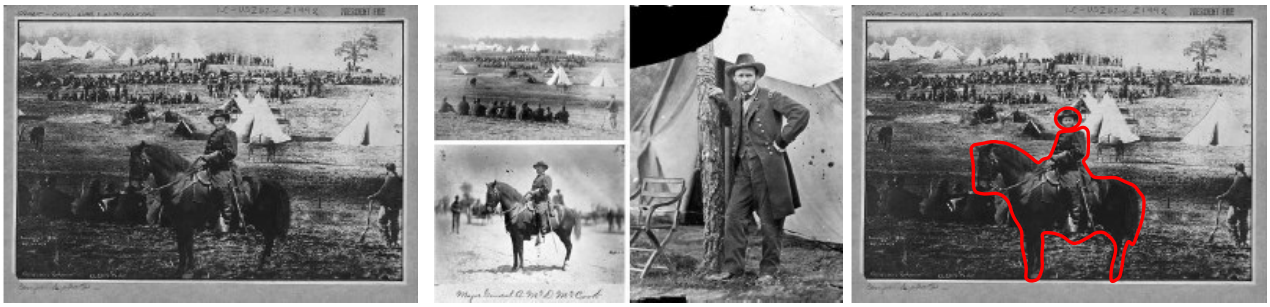
CHAPTER 1

INTRODUCTION

This chapter provides brief information related to digital image forensics and anti-forensics. Most of the information which is being shared on the internet with the help of various social networking websites is in the form of digital data. This digital information can be easily manipulated to harm the integrity of someone. Therefore, the analysis of digital evidence can significantly speed up the forensic investigation process. The number of doctored/tampered images on social networks increases day by day with the growth of technology. Thus, the truthfulness of digital images is one of the major issues in information security. The digital image forensics refers to analyze the digital image in order to evaluate its legitimacy. On the contrary, image anti-forensics aims to create barriers in the path of forensic examination.

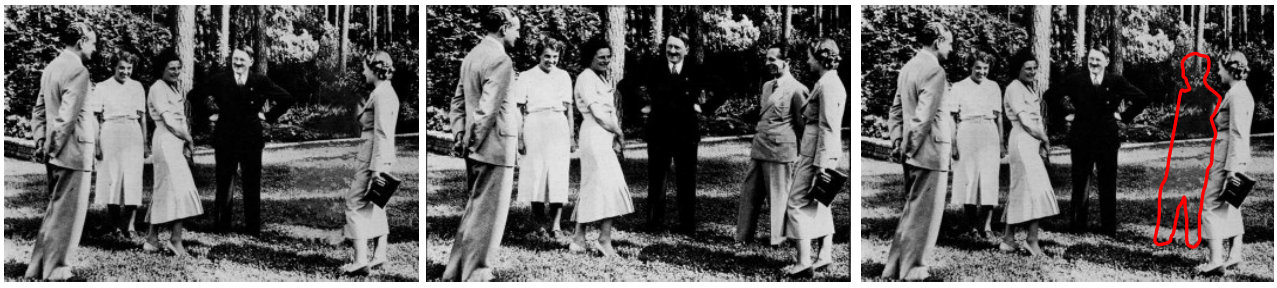
1.1 History of Image Tampering

The innocence of photography vanished several years ago. The first photograph was created by Niepce in 1814 and after only a few decades, image manipulations were started [1]. In the early years, it is very difficult to create a forged image due to restrictions in technology. Only a skilled counterfeiter can perform image tampering with the help of some tools, very stable hands, and sharp eyes. Nowadays, forgery creation became an easy task due to technological developments. One can easily manipulate digital images by utilizing the editing softwares such as Adobe Photoshop, PaintShop Pro, *etc*. Moreover, smart phones are now equipped with a number of photo editing applications [2 - 3] in order to modify the images. These applications provide varieties of image processing operations for image filtering to tune images, face poses, glamour glow, double exposure, *etc*. However, these photo editing tools are quite challenging to use for first-time users. It is essential to note that all image processing operations are not forgeries. For example, an image can be processed just to increase its visual quality [4]. The image tampering involves the alteration of original image content in such a way that it portrays false information. For example, several image forgeries available on the various social networking sites were made by using the copy/paste, splicing, and removal operations [5].



(a) This doctored image is created in 1864 showing General Ulysses S. Grant during American Civil War on a horse with his troops in the background at City Point, Virginia. The examiners at the Congress Library confirmed that this image is made from the mixture of three different images. The head is taken from Grant photograph, horse and body belong to Major General Alexander M. McCook, and background is the battle of Fisher's Hill, VA [1].

(b) In 1930, an image of Stalin is forged to remove a commissar due to lack of Stalin interest [1].



(c) Hitler had removed his loyal colleague Joseph Goebbels from his photo in 1937. The missing person Joseph Goebbels is one of the top propagandist and architects of the holocaust [1].

(d) In 1942, the horse handler was air-brushed by Benito Mussolini from his original photograph in order to show himself stronger and independent [1].

Figure 1.1: History of image tampering (Contd.).

(e) In 1961, a group of cosmonauts from Russia commanded by Yuri Gagarin was the first to complete the earth orbit. One cosmonaut named as Grigoriy Nelyubov was erased from the original image captured after the trip. He had been disqualified from the program due to his misconduct [1].

(f) National Guardsmen fired into a mob of presenters at Kent State University in 1970, thereby killed four people and wounded nine. This forged picture was printed in LIFE Magazine showing Mary Ann Vecchio sitting near the body of student Jeffrey Miller and the fence post straight behind Vecchio was concealed [1].

(g) This forged image of Oprah Winfrey was presented by TV Guide in 1989. Actually, this doctored image was formed by merging the Winfrey head on Ann-Marget body, which was taken in 1979 [6].

Figure 1.1: History of image tampering (Contd.).

(h) This doctored photo was presented by the Iran army in 2008 in which one extra missile is shown in order to strengthen the army power [7].

(i) This doctored image OJ Simpson published on the Time magazine cover just after the custody of Simpson for murder. This picture was tampered from the original image printed on the Newsweek cover. Afterward, the Time magazine was alleged for this forgery to make the Simpson appearance darker and dangerous [8].

(j) In 1993, an image was doctored by the University of Wisconsin, Madison by adding a black student in the photograph of white football fans to show its diversity [9].

Figure 1.1: History of image tampering (Contd.).

(k) This doctored image is related to Mr. Narendra Modi, PM of India, during the Chennai floods in 2015. The circular window portion of the image is forged to make it look more convincing [10].

(l) During the celebration of Eid al-Adha in 2016, a large number of animals was slaughtered as a sacrifice. But due to heavy rains, the streets in Bangladesh turned into a river of blood [11].

(m) US president Donald Trump photos were doctored in 2019 to show his little fingers longer and hairs fluffy [12].

Figure 1.1: History of image tampering.

Figure 1.1 provides the history of image tampering started from the mid-1800s by showing some key forgeries, where doctored images are shown on the left side, original images are shown in the middle and illustration of doctored images is provided on the right side. Some of these doctored images resulted in severe financial and reputation losses, false propaganda, political controversies, extortion, and also conveyed negative impacts to the society.

1.2 Digital Image Forensics

The reliability of digital images is important in numerous regions such as scientific examination, criminal examination, observation frameworks, knowledge administrations, medicinal imaging and news coverage. Digital image forensics uses the scientifically derived and proven image forensic approaches for the study of image under investigation to find out if an image has undergone any kind of forgery or not [13 - 14]. The revealed footprints during the forensic examination questioning the image integrity can be presented in the court for justice.

With the growth of multimedia services, a number of social networking sites such as Facebook, Instagram, Snapchat, Youtube, *etc*. are available to share the digital information in the form of audio, image, and video. For example, around 1 billion images are being shared only on Facebook every day [13]. Therefore, the number of doctored images related to politics, publicity, and individual attacks increases significantly with the growth of multimedia services. Thus, maintaining the authenticity of this big data is one of the primary concerns. The digital image forensics aims to employ efficient tools which can generate the historical information of an image related to the camera or device properties used for shooting. The analysis of this information discloses the reliability of an image.

Every digital image we encounter in our daily life might have gone through several processing stages to increase its quality. There is a need for reconstruction of digital image history for its truthfulness verification. Digital forensics is working for security applications with the aim of restoration of acceptance and trust in digital media [15 - 16]. There are basically two approaches for detecting the authenticity of an image and estimating its processing history *i.e.*, Active and Passive approaches [4]. The fragile digital image watermarking was one of the commonly used approaches in order to authenticate the digital images [17]. Fragile watermarking is considered as active forensics [18]. In this approach, the authentication information or watermark is inserted into the image during the capturing process or before transmission. On the other end, if there is a failure in the extraction of watermark or any disparity found between the mined and inserted watermark then the considered image is doctored/tampered otherwise it is authentic. In this case, it is mandatory to have a distinctive image acquisition device. The idea of a truthful camera having a watermarking system was suggested in early 1993 [19]. The realization of this concept

in the industry faced several problems, which are still difficult to resolve. Primarily, it is a difficult task for the manufacturers of different cameras to follow a common standard protocol. Moreover, it is inconvenient for the customers to compromise with the image visual quality due to watermarking. In addition, it will become a problematic issue, if the watermarking system equipped in the trustworthy camera is hacked. For instance, Beijing Huaqi Information Digital Technology Cooperation tried to promote Aigo V80PLUS camera [20] in 2005. However, due to these issues, it failed in its attempt to popularize a trustworthy camera.

These limitations of active forensics gradually shift the attention of the researchers to the passive forensics [18, 21]. The passive forensic approaches evaluate the legitimacy of the particular image in a blind manner, without requiring any prior inserted information (or watermark) related to the image. It is expected that one can perform image tampering by creating forgeries without any visual footprints. However, it will possibly alter the intrinsic properties of the original image. Consequently, inconsistencies or deviations in the fundamental image statistics can be examined for image tampering detection.

1.2.1 Classification of Digital Image Forensics

Digital image forensics is based on the fact that when an image is processed with some operations to create its forgery, the intrinsic properties of an image such as statistical, physical or geometrical, *etc*. will get disturbed. The digital image forensics is categorized into five different classes as shown in Figure 1.2 as provided below [21]:

Pixel-based Forensic Techniques

Pixel-based forensic methods are based on detecting the statistical abnormalities which are introduced at pixel level when images are being forged. Analysis of the pixel level correlation is performed in order to detect a forgery in spatial or transform domain. Copy-move, splicing, removal, resampling and median filtering operations are some regularly used for image manipulations. Different image forensic techniques are proposed to target each of these image operations [21].

Format-based Forensic Techniques

For efficient storage and transmission, every image undergoes compression at least once during its life cycle. Doctored images are also compressed after tampering. This compression leaves several traces which may reveal tampering. Set Partitioning In Hierarchical Trees (SPIHT), JPEG and JPEG2000 based on DCT and wavelet transform respectively are some widely used compression techniques [21].

Camera-based Forensic Techniques

Digital image ballistics [22] is examined from the image creation phase happening inside the camera by the camera-based image forensic techniques. Every camera introduces some amount of artifacts in the captured image. Camera-based forensic techniques detect the traces of any modification at various stages of the image creation process by using Color Filter Array (CFA), chromatic aberration, sensor noise and camera response [21].

Physically-based Forensic Techniques

The irregularities of interaction between the objects in the image, lighting environment, and the device capturing the three-dimensional real physical world are examined in physically based image forensics. Actually, matching the lighting conditions of different images is a difficult task. The inconsistencies of the lighting environment from distinct objects in an image can be used for forensic purposes [21].

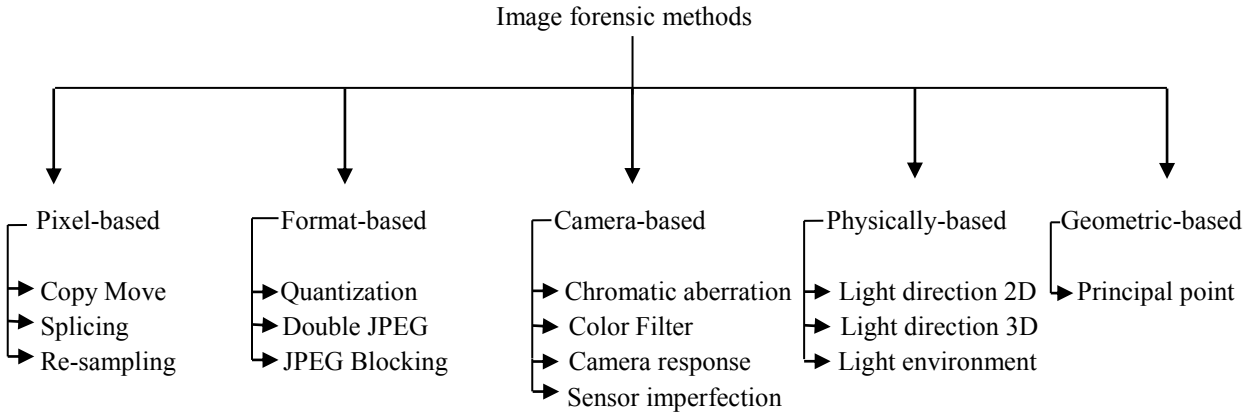


Figure 1.2: Classification of digital image forensic methods [21].

Geometric-based Forensic Techniques

The position of the physical objects in the image is measured in the geometric-based image forensics with respect to the camera. Every image has a principle point at its center which shifts when these images are modified by copy move or splicing [21].

1.3 Digital Image Anti-Forensics

The coin referred to image authentication has two sides *i.e.*, forensics and anti-forensics in a similar way as cryptography works against cryptanalysis and steganography opposite to steganalysis. Digital image anti-forensics is employed by the counterfeiters to conceal the traces of different image processing or editing operations such as re-sampling, JPEG compression, median filtering, *etc*. in order to mislead or create a barrier in the forensic investigation process. Therefore, the anti-forensics ultimate goal is to improve the forensic schemes by revealing the limitations of forensic techniques [23], so the direction of this research work is essential. Moreover, this work is also dedicated towards the counter anti-forensics. The purpose of the counter anti-forensics [24] is to reveal the introduced footprints related to the particular image processing operation in the presence of a corresponding anti-forensic attack. Most of the existing counter anti-forensic approaches are based on the footprints of a specific image operation and detect only one type of anti-forensic attack at a time. These counter anti-forensic schemes do not work for anti-forensic techniques related to the other image processing operation. Therefore, the researchers are much inspired to design a multi-purpose counter anti-forensic method which is alone proficient of detecting different anti-forensic techniques based on various image processing operations. It is worth noting that robustness of anti-forensic techniques is evaluated by considering various forensic attacks. On the other side, the efficacy of counter JPEG anti-forensic scheme is evaluated against different anti-forensic attacks.

Digital image forensics is still a new and interesting area for the researchers and image anti-forensics is an even younger field as compared to the forensics [25]. It can be observed from the literature that there are more publications related to forensics than those on anti-forensics. Furthermore, the existing anti-forensic methods are based on simple image processing operations (for example, application of filtering to mask the artifacts of compression [26] or adding noise to cover the traces left by filtering [27]) to conceal the footprints added by the targeted operation.

These anti-forensic methods can easily fool various forensic detectors by hiding the traces of targeted operation. However, some advanced forensic techniques [28 - 29] are capable of exposing these anti-forensic schemes. Also, the resultant image forgery created by these anti-forensic methods suffers from low image visual quality (for example, blur or noisy image). Therefore, it is a problematic concern because low image quality can create doubt on the image originality.

A good forensic undetectability along with high image visual quality is a two-fold end of image anti-forensics [30]. From image anti-forensics point of view, forensic undetectability is much vital as compared to image quality. Any anti-forensic technique is not considered to be fruitful if it is exposed by a certain forensic detector.

When we are dealing with image processing, we observe that the aim of image anti-forensics is similar to image restoration to certain level *i.e.*, to reacquire the lost information due to the degradation of an image by resolving an ill-posed inverse problem. On the contrary, this concept does not hold for some anti-forensic cases, when the evaluation is performed by considering physically or geometric-based forensic techniques. This analysis is beyond the scope of this study and we have mainly devoted our attention towards the anti-forensics of JPEG compression (both single and double). The improvement of image visual quality of degraded images is the main objective of the image restoration process, while recovering the underlying statistics of the original image is the main requirement in image anti-forensics so that the resultant forged image seems genuine. High image quality is also the main factor desired in image anti-forensics. But high forensic undetectability is an additional essential goal of image anti-forensics, when compared to image restoration.

The present work firstly aims to the forensic examination of double JPEG (DJPG) compressed images. In this approach, the JPEG ghost detection technique is explored to identify and extract the DJPG compressed region in an image which is further processed for the estimation of the first quantization matrix. Subsequently, an anti-forensic framework is proposed to conceal the JPEG compression (both single and double) artifacts in order to fool the forensic detectors. Numerous natural image statistical models are used in this framework. Moreover, some anti-forensic approaches are also integrated to enhance the forensic undetectability. Different

numerical optimization schemes are used to solve the image anti-forensic problems. By following this approach, the desired JPEG forgery is attained with superior image quality and forensic undetectability. Lastly, the work is devoted to counter JPEG anti-forensics by considering higher-order statistical analysis based on CMs. This scheme also works under different image operations such as median filtering and CE anti-forensics.

1.3.1 Classification of Digital Image Anti-Forensics

The anti-forensic methods create barriers in the forensic investigation process by concealing the footprints used by the forensic detectors, thereby enlightening the detectors limitations. Thus, anti-forensic approaches also motivate the researchers to work in the area of digital image forensics. The image anti-forensics is divided into the following three classes as follows [23]:

Robustness versus Security

The robustness or security weaknesses of digital image forensics are exploited by the image counterfeiters for anti-forensic purposes. Firstly, the robustness refers to the reliability of the digital image forensics under reasonable post-processing operation. For instance, several forensic techniques (for example, lighting-based forensics) do not deliver acceptable results, when the considered image is processed with strong JPEG compression. Therefore, this type of post-processing operation can work as an anti-forensic method, till it is capable to keep the forgeries away from the recognition area of forensic techniques. Secondly, the image forensics security refers to its capability of revealing the deliberately hidden footprints of reliable post-processing. The weaknesses of the image model utilized by image forensic techniques are exploited by the image falsifiers. A capable anti-forensic approach can create image forgeries moving away from the decision zone of trustworthy images [23].

Post-Processing and Integrated Attacks

When the images are processed by using post-processing anti-forensic attacks, the forensic detectors are unable to detect these images. This happens because the anti-forensic attacks conceal the traces left by JPEG compression, which are used by forensic detectors for image forensics. On the contrary, the image generation process is directly interfered by integrated anti-forensic attacks. Also, the robustness of image forensics is not addressed by these attacks [23].

Targeted and Universal attacks

When the weakness of a particular forensic tool is exploited by an anti-forensic technique, then this anti-forensic scheme is considered as targeted. It is also possible that some other forensic algorithm based on improved image models can detect this type of anti-forensics. In the case of universal anti-forensic attacks, the statistical properties of the created forgery are preserved to a maximum extent, so that it goes on untraceable even against unfamiliar forensic detectors. This is a challenging task to perform and can be considered as an exciting open research problem [23].

1.4 Motivation

The majority of digital devices or cameras, various image processing software tools and websites generally utilize the JPEG compression format. Moreover, the JPEG image format is used by 72.6 % of all the websites based on the data provided by [31] on January 12, 2019. Therefore, for the purpose of image forensics, the study has been vastly concentrated on estimating that an image is JPEG compressed (single or double) or not. This JPEG compression becomes a significant part during the image falsification process. For instance, the image is already JPEG compressed once during the acquisition phase. During the forgery creation, when the portion of some other image having different quality is pasted into this image results in DJPG compression artifacts. The recognition and analysis of JPEG compression (*i.e.*, both single and double) in an image help the investigator to find the authenticity of an image.

The DJPG compression detection techniques such as the ones presented by Farid [32], Puglisi *et al*. [33] and Galvan *et al*. [34] are the motivation behind the presented forensic investigation of DJPG compression. Moreover, the distribution of quantized JPEG coefficients follows Benford-like logarithmic law after single compression. This Benford-like logarithmic law is violated due to double compression [35]. It is also mentioned in [36] that DCT coefficients histogram does not follow generalized Gaussian distribution after double compression. The forensic study of JPEG compression can be performed based on the analysis of these properties. These schemes suggest that research work can be extended to explore the partially DJPG compressed images. Therefore, initial research work is devoted to design a forensic scheme for DJPG compression to retrieve the historic information related to an image such as quantization matrix.

The idea of the proposed JPEG anti-forensics was motivated by the research of Valenzise *et al*. [37] and Fan *et al*. [38 - 39] on JPEG compression anti-forensics. The study of these works reveals various aspects that can be used for the further enhancement of anti-forensics. For instance, the JPEG anti-forensic approach recommended by Fan *et al*. [39] utilizes the concept of perceptual histogram smoothing and TV-based deblocking to misguide the different forensic detectors by masking the compression artifacts. The grainy noise added during the perceptual smoothing can be decreased for better image restoration. Thus, the proposed JPEG anti-forensic scheme aims to achieve a better tradeoff between image quality and forensic undetectability.

The work done by Fan *et al*. [39] also inspires to extend the research work to counter the JPEG anti-forensics. Moreover, the IEEE future directions [5] also recommends that digital image forensics is a promising line of research work. Thus, the further work is stretched to design a forensic technique to identify the compression artifacts (single or double) in the presence of JPEG anti-forensics. The existing JPEG anti-forensic methods eradicate the first-order statistics or histogram-based footprints but most of the anti-forensic approaches are not able to properly conceal the second-order statistical footprints. Therefore, in this research work, a second-order statistical analysis based on CM is carried out for countering the JPEG anti-forensics. The CM-based second-order feature component analysis is limited to image steganalysis and has not been considered for the counter JPEG anti-forensics previously.

Most of the existing counter anti-forensic techniques focus is to detect only one type of anti-forensic technique related to a particular image operation. These techniques do not provide satisfactory performance against anti-forensic attacks based on other image operations. Therefore, the research is inspired to design a multi-purpose counter anti-forensic approach.

1.5 Contribution of Research Work

The major contributions of the presented research work are as follows:

- In this research work, a two-stage forensic technique is proposed to investigate the DJPG compression. In the first stage of the proposed approach, the detection of the double compressed region through JPEG ghost technique is extended to the automatic isolation

of the doubly compressed part from an image. The second stage is devoted to analyze the doubly compressed part to estimate the first quantization matrix or steps.

- An improved JPEG anti-forensic framework is designed by removing the compression artifacts in both spatial and DCT domain. The presented anti-forensic framework is capable of providing better image visual quality and forensic undetectability.
- The robustness of the proposed JPEG anti-forensics is evaluated against different types of forensic attacks including various existing scalar-based and Support Vector Machine (SVM)-based forensic detectors.
- The research work is also focused to design a counter JPEG anti-forensic scheme by performing a second-order statistical analysis based on CMs.
- Moreover, the competency of the suggested counter JPEG anti-forensic method is also evaluated in countering median filtering and CE anti-forensics.
- The proposed counter JPEG anti-forensic scheme is also capable of detecting other image processing operations such as Mean filtering, Gaussian filtering, Weiner filtering, Scaling, and Rotation, thereby revealing its multi-purpose nature.

1.6 Limitation Analysis

Now, this section summarizes and examines the limitations of the research work presented in this thesis on the basis of experimental results and discussions.

It is a challenging task to design a detector which is alone capable of countering the anti-forensic methods of various image operations such as JPEG compression, Median filtering, CE and Resampling by considering all of the existing anti-forensic techniques corresponding to each image operation. This is due to the different strengths of various anti-forensic techniques. If the forensic investigator is going to design a detector to counter one anti-forensic technique, the other may not be countered by that detector. Therefore, a universal detection approach is required to detect the various image manipulations.

The minimum decision error values increase with the decrease in the size of the image under investigation due to the inadequate image statistics. This may have negative effects on some forensic applications such as tampered region localization. Therefore, it is required to make a

hybrid feature which includes some other parameter like image content information to detect the small size forged regions.

The SVM and CNN-based machine learning approaches are designed for different situations. For instance, SVM-based methods are generally used for binary classification with small feature dimensionality, whereas CNN-based approaches are used for complex classification of larger datasets. Therefore, the comparison of SVM and CNN-based forensic techniques is not provided in this research work. It is required to utilize the deep learning approaches in the proposed counter anti-forensic scheme for further enhancement and comparative analysis.

1.7 Organization of Thesis

The thesis is arranged as follows:

Chapter 1 presents the general introduction and depiction of the thesis. It provides a detailed description related to the history of image tampering, digital image forensics and anti-forensics with their classification, motivation behind the research work, contributions, limitation analysis and organization of the thesis.

Chapter 2 elaborates the detailed study which includes the basics of JPEG compression and its artifacts. The existing forensic, anti-forensic, and counter anti-forensic approaches of JPEG compression are discussed in detail in this chapter. Afterward, explanation is provided about the various evaluation metrics, image datasets for forensic testing. The research gaps, objectives, and research methodology are also described in this chapter.

Chapter 3 presents a forensic technique for DJPG compression to recover the historic information lost during the DJPG compression. Firstly, a technique is suggested to automatically separate the double compressed region from the considered image based on the JPEG ghost detection approach. Later, an approach is recommended to compute the primary quantization steps from the extracted double compressed region. In the experiment results section, the proposed scheme is compared with the existing methods to confirm the efficacy of the presented scheme.

Chapter 4 introduces an improved JPEG anti-forensic framework to misguide the various forensic detectors by concealing the JPEG compression footprints. The primary focus of the suggested JPEG anti-forensics is to achieve better image visual quality and forensic undetectability. The performance of the proposed method is evaluated by considering both the scalar and SVM-based forensic detectors.

Chapter 5 explains the presented forensic algorithm to counter the various anti-forensic techniques of JPEG compression. In this approach, a second-order statistical analysis is performed based on CMs. The experimental results confirm the efficiency of the recommended forensic technique in detecting various JPEG anti-forensic techniques under both the worst-case and optimistic scenarios.

Chapter 6 describes the various applications of the proposed counter JPEG anti-forensic scheme. This approach is further evaluated in this chapter to counter the median filtering and CE anti-forensic schemes. Moreover, it is also noticed that this technique offers improved results in the detection of other image processing operations.

Chapter 7 defines the conclusions, main highlights and future scope of the research work performed in this thesis.

CHAPTER 2

LITERATURE SURVEY

This chapter is dedicated to study and analyze the literature related to different JPEG compression forensic, anti-forensic and counter anti-forensic methods. The different evaluation metrics are also discussed based on which the performance of various forensic, anti-forensic methods is evaluated. It also provides detailed information about the image datasets, settings and forensic testing used for evaluation purposes. Moreover, this chapter covers the research gaps, objectives, and research methodology.

2.1 JPEG Forensics and Anti-Forensics

This section provides the discussion related to the basic concept of JPEG compression and its artifacts in both spatial and DCT domain. It also includes the study of various JPEG compression detection techniques, JPEG anti-forensic techniques, and Counter JPEG anti-forensic techniques.

2.1.1 Basics of JPEG Compression

JPEG is a widely used compression standard which was formed in 1980 by members of ISO and ITU [40]. Wallance *et al.* [41] provided an overview of JPEG compression. In order to support variety of applications for continuous-tone images, the JPEG standard aims to be generic. JPEG compression is classified into lossless and lossy compression. The predictive method is used for lossless and baseline method is used for lossy compression. Lin *et al*. [42] developed a method to evaluate the coding efficiency based on the degree of distortion. The main idea of data compression is to decrease the data correlation by applying DCT as shown in Figure 2.1. DCT is used to transform the data from time domain to frequency domain. As human visualization is less sensitive to high frequency, so image data can be compressed by suppressing its high frequency component.

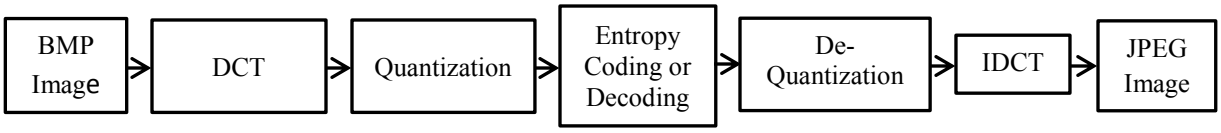


Figure 2.1: Single JPEG compression and de-compression.

Firstly, the genuine uncompressed image $\boldsymbol{I}$ is divided into L non-overlapping 8×8 pixel blocks. Afterward, DCT is applied on each pixels block to acquire its equivalent DCT coefficients block. Due to the orthogonal linear nature of DCT, the mapping of this operation can be expressed as a matrix multiplication denoted by $D_{matrix}\boldsymbol{I}$, where D_{matrix} is a DCT block matrix. Then, the (r, c)-th $(r, c = 1, 2, 3, \dots, 8)$ DCT coefficient $(D_{matrix}\boldsymbol{I})^{l}_{r,c}$ of the l-th $(l = 1, 2, 3, \dots, L)$ block is uniformly quantized as [43]:

$$(q_{block}(D_{matrix}\boldsymbol{I}))^{l}_{r,c} = round\left(\frac{(D_{matrix}\boldsymbol{I})^{l}_{r,c}}{q_{r,c}}\right) \tag{2.1.1}$$

where, $round(.)$ denotes rounding function and $q_{r,c}$ represents the (r, c)-th entry of the quantization table matrix. Subsequently, these quantized DCT coefficients $q_{block}(D_{matrix}\boldsymbol{I})$ are encoded losslessly.

In the case of decompression process, the quantized DCT coefficient obtained from the decoded bitstream is de-quantized by performing its multiplication with corresponding quantization step denoted as [43]:

$$(q^{-1}_{block}(q_{block}(D_{matrix}\boldsymbol{I})))^{l}_{r,c} = (q_{block}(D_{matrix}\boldsymbol{I}))^{l}_{r,c} \times q_{r,c} \tag{2.1.2}$$

Then, Inverse Discrete Cosine Transform (IDCT) is utilized to transform the dequantized DCT coefficients into the spatial domain. This operation can be represented as the multiplication of the dequantized DCT coefficients with IDCT matrix as $D^{-1}_{matrix}q^{-1}_{block}(q_{block}(D_{matrix}\boldsymbol{I}))$. Finally, rounding and truncation process represented by $RT_{error}(.)$ is employed in order to make the pixel values in the integer range [0, 255], so the decoded JPEG image is attained as [43]:

$$\mathcal{T} = RT_{error}(D^{-1}_{matrix}q^{-1}_{block}(q_{block}(D_{matrix}\boldsymbol{I}))) \tag{2.1.3}$$

There are some issues related to JPEG compression. Dividing an image into 8×8 blocks results in compressed image with blocking artifacts [41, 43]. There is an absence of smooth transition between the blocks in a compressed image. Every block is transformed and quantized independently. When we try to exploit the homogeneity of a region that is larger than 8×8 block then decoupling of the image occurs. DCT is computed from samples of cosine function and thus works best only when input data is periodic. DCT is a global transformation matrix in

which every element is affected by every other element of input matrix. Therefore, if there is any perturbance in input matrix then it also affects every element in the resultant transformed matrix. A digital image undergoes various steps in its life cycle. Starting from acquiring an image, coding, then editing is also performed on it in order to enhance its quality. Then, this image may further undergo for enhancement of its features such as contrast, brightness adjustment and correction of gamma function. These enhancement operations introduce pixel modifications or inconsistencies in the resultant image which are used by the forensic detectors for examination.

2.1.2 JPEG Artifacts

In JPEG compressed images, there are basically two types of artifacts *i.e.*, quantization artifacts in DCT domain and blocking artifacts in spatial domain [43 - 44]. The identification of these artifacts reveals the compression history of an image under investigation. The uncompressed Lena image is JPEG compressed with quality factor 20 to show the induced compression artifacts as revealed in Figure 2.2. The DCT coefficients histograms of (2, 2) sub-band corresponding to original and JPEG compressed Lena image are provided in Figures 2.2 (c) and (d) respectively. It is observed from the DCT coefficients histograms that most of the neighboring bins coefficients are shifted to the center bin in case of compressed image because most of the quantized coefficients become zero. Note that during the JPEG decompression process, the rounding and truncation operation introduces the DCT coefficient error. This DCT coefficient error is not counted in Figure 2.2 (d).

2.1.2.1 Quantization Artifacts in DCT Domain

The multiplication of quantized DCT coefficient $(q_{block}(D_{matrix}I))^{l}_{r,c}$ with its equivalent quantization step results in the dequantized DCT coefficient represented by $(q^{-1}_{block}(q_{block}(D_{matrix}I)))^{l}_{r,c}$. Thus, the DCT coefficients of JPEG compressed image are gathered nearby the integer multiples of quantization step [43]. In compressed image, the DCT coefficients arrange themselves in the form of comb-like distribution as shown in Figure 2.2 (d). There are periodic gaps present in the DCT coefficients histogram of JPEG compressed images. This type of artifacts is known as the quantization artifacts in DCT domain. These artifacts are usually used in the forensic investigation of the image tampering based on JPEG compression.

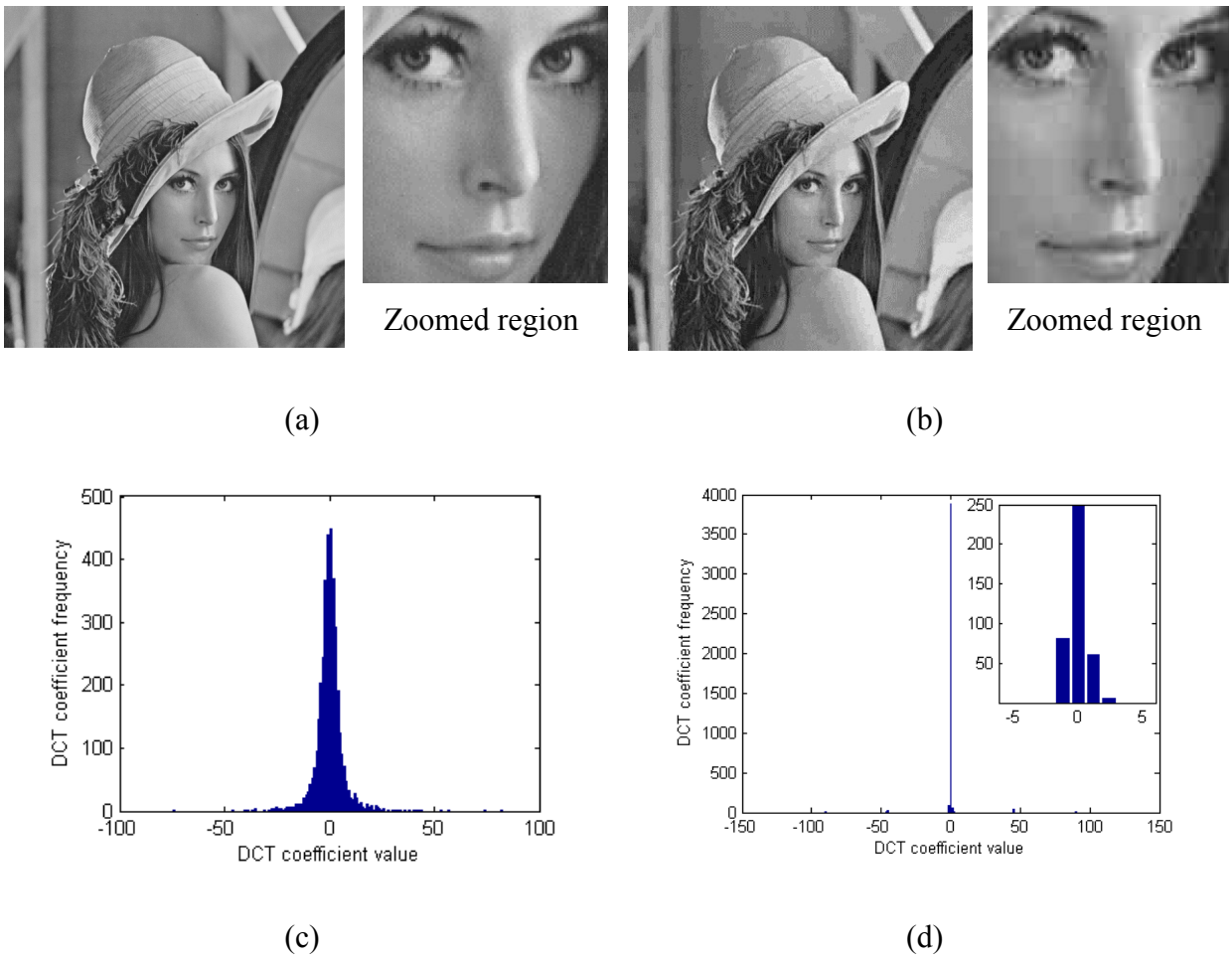


Figure 2.2: (a) Uncompressed Lena image, (b) JPEG Lena image with quality factor 20, DCT coefficients histogram of (2, 2) sub-band for (c) uncompressed Lena image and (d) JPEG Lena image with quality factor 20.

2.1.2.2 Blocking Artifacts in Spatial Domain

The blocking artifacts induced in spatial domain due to JPEG compression as exposed in Figure 2.2 (b) are because of the application of block based DCT transform. Primarily, the image is partitioned into 8×8 non-overlapping blocks in the JPEG compression process. Later, these blocks are DCT transformed and quantized which results in the discontinuities or blocking artifacts in the pixel value across the block borders [21].

It is also pointed by Robertson and Stevenson [45] that compression noise is generally correlated in spatial domain. The low-frequency sub-bands contain more energy for the moderately smooth signal. On the contrary, high-frequency sub-bands have relatively low energy

and therefore, add less quantization noise. The succeeding locations to the block boundaries have high error variance because low-frequency sub-bands have significant quantization noise because of DCT basis functions as displayed in Figure 2.3. The textured region of an image is an example of a complex signal and in this case, high error variance appears in the middle of the block as compared to the borders.

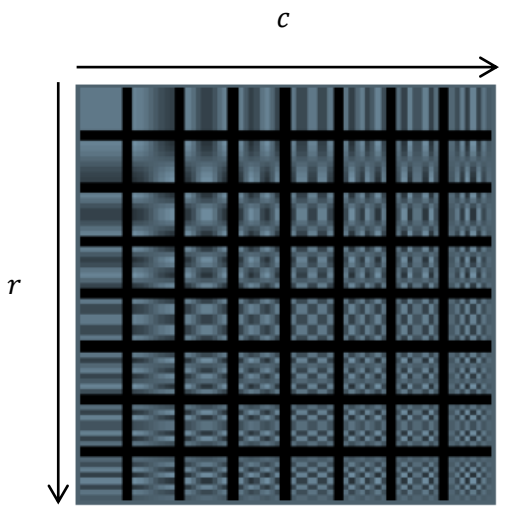


Figure 2.3: DCT basis functions.

2.1.3 Forensic Investigation of JPEG Compression

The digital investigation of an image provides the historic information of an image related to the camera or device properties used for shooting. Based on this information, one can find that the considered image is a doctored/tampered or not [46 - 47]. JPEG is a generally utilized format by numerous image processing tools and cameras for data compression. The image is compressed once during a shooting in the camera device, and if this image is further decompressed and resaved with different compression quality during forgery creation, the resultant image becomes double compressed. Therefore, the forensic investigator can easily detect the image manipulations by revealing the double compression artifacts [48]. In an advanced examination, various acquisition devices and systems generally utilize the JPEG compression for images. The issues faced during image examination can be divided into two broad categories, the first regarding the legitimacy of the visual document, and the other concerning the identification of the device which is used for the image acquisition [34].

2.1.3.1 Detection of Image Tampering based on JPEG Compression Artifacts

Numerous methodologies are available to discover the JPEG images manipulations. These techniques include acquisition-based schemes, coding-based schemes and editing-based schemes in order to recognize the source of digital image and to validate its authenticity without any prior knowledge [49]. Stamm *et al*. [50] discussed the evolution of information forensics over the last decade. It provides very useful information about the various applications of information forensics. This information can be used in future to develop efficient forensic algorithms [50]. Different methodologies deal with the analysis of the statistical distribution of the DCT coefficient values. The performances of these state-of-the-art techniques are evaluated by considering different image datasets, compression ratio and different types of forgeries [51]. It is conceivable to figure out that an image is JPEG compressed or not by analyzing the related histogram. Various statistical methods are presented by Popescu and Farid [52] to detect the traces of digital tampering in the absence of any digital watermark or signature. The statistical correlations between the neighboring pixels of an image become inconsistent due to the digital manipulations. Therefore, these statistical correlations are examined to check the authenticity of digital images [52]. An effective method based on machine learning (SVM classifier) is presented to differentiate between single and DJPG compressed images. Initially, difference JPEG 2-D arrays obtained by calculating the difference between the magnitude of JPEG coefficient 2-D array of particular JPEG image and its shifted versions along different directions, are used to enhance the DJPG compression artifacts. Afterwards, Markov random process is utilized to model difference 2-D arrays to employ second-order statistics [53]. Moreover, Thing *et al*. [54] suggested a JPEG compression detection technique based on a periodic function to identify the altered regions. A scheme is recommended in [55] to analyze the double compression using the same quantization matrix. Based on the estimated primary quantization matrix, a new technique is suggested in [56] to recognize the DJPG compressed images. Furthermore, a technique is depicted in [57] to identify the DJPG compression by utilizing the same quantization matrix.

Moreover, a robust technique is presented in [58] to reveal the copy-move falsification based on high JPEG compression artifacts. This method comprising feature extraction, feature matching and duplicate block identification for copy-move forgery detection. The extraction is

done by utilizing the Fast Fourier Transform (FFT), Singular Value Decomposition (SVD) and Principal Component Analysis (PCA) while their cascading matchers are used for feature matching. Then, the pixels on upper left corners of detected duplicate blocks are used for visual inspection. This approach also shows robustness against various attacks such as JPEG compression, Gaussian noise and blurring attacks. Li and Zhou [59] presented a fast and effective method for copy-move detection through hierarchical feature point matching. This method solved the keypoint matching problems over a massive number of keypoints. An iterative localization technique is also proposed for reduction of false alarm rate and accurate localization of tampered regions by utilizing the dominant orientation, scale and color information of each keypoint. Khuspe and Mane [60] presented a robust image tampering detection approach based on Mirror Invariance Feature Transform (MIFT) and k-means clustering. The keypoints from each of the training image are mapped into a unified dimensional histogram vector after K-means clustering [61] with a vector quantization technique. This histogram is fed to the multiclass SVM for classification. Similar process is done in case of testing stage. In the case of a duplicate operation, the image recompression by utilizing same quantization table is analyzed in [62], concluding that the grid of the pasted part has a significant probability that it is not aligned with the existing one.

Blocking artifacts left during the JPEG compression is taken as evidence of compression. A forensic approach is proposed in [63] on the basis of the fact that in the case of uncompressed image, the pixel difference taken over the boundaries of 8×8 block and within the blocks must be same. The blocking signature parameter based on this fact is the energy difference between histograms and it can be represented as:

$$K_F = \sum_n |H_1(n) - H_2(n)| \tag{2.1.4}$$

where, $H_1(n)$ and $H_2(n)$ are the normalized histograms based on the difference of pixel values across the boundaries of block, and within the block respectively. Moreover, a forensic algorithm is suggested in [64] to detect the JPEG compression which does not require an original image and hence known as blind blocking artifact measurement method. The goal of blocking effect measurement algorithm is to detect and estimate the strength of a blocky signal. Therefore, the

blocking artifacts measures are usually engaged in the forensic examination of JPEG compressed images.

An efficient forensic detection technique is proposed in [65] for DJPG compressed images by considering the DCT coefficients histograms. These histograms of DCT coefficients encompass certain periodic artifacts which are analyzed to create the feature vector for SVM classifier. Different quantization steps have been used for primary and secondary compressions which result in the occurrence of certain irregular statistical patterns in the Quantized DCT (QDCT) coefficients histogram. Depending on the periodicity measure, a detection process is introduced in [52] on the basis of the fact that whether Fourier transform of histogram has specific artifacts or not. Actually, image recompression results in periodic artifacts and histogram discontinuity. The SVM classifier is trained with the features based on these artifacts/discontinuities in order to detect the JPEG re-compression [66].

Moreover, a method is proposed by He *et al.* [67] that has the capacity to identify images tampered by various types of synthesizing approaches like alpha matting [68] and inpainting [69]. Moreover, it is the fastest method which can work without completely decompressing the JPEG image which reduces memory requirement and computational complexity. The detection becomes difficult when the original image contributing the non-tampered section is not a JPEG image. In this situation, double quantization effect of non-tampered part cannot be detected. Secondly, this method also fails if the quality factor after image forgery is kept lower. Thus, a forensic method is proposed in [32] to expose the image forgeries by analyzing the difference domain. In this method, tested image is re-compressed at various quantization factors and compared with the given tampered image. The apperance of spatial local minima (JPEG ghost) in the difference between the given image and its JPEG compressed version confirms that the given image tampered with double compression. This approach works in the case when quality factor of tampered region is smaller than the rest of image. Furthermore, based on the analysis of JPEG compression and characteristics of blocking artifacts, a Blocking Artifact Characteristics Matrix (BACM) is designed in [70] to evaluate the symmetrical property of blocking artifacts added by JPEG encoder. BACM shows symmetrical shape for genuine JPEG image. The cropping and recompression operations can alter this symmetrical property. Therefore, the SVM classifier is trained by using the features derived from BACM in order to recognize that whether

the image is a genuine JPEG image or cropped from some other image and resaved as JPEG image. Better outcomes are obtained, when quality factor of first compression is smaller than the quality factor of last compression. This method is trustworthy for large-sized forged region [70]. This approach is further enhanced in [71] to localize the tampered region without any previous knowledge.

Chen *et al.* [72] suggested a technique to analyze the periodic nature of blocking artifacts by generating a linear dependency model of pixel differences and then construct a periodicity map of each pixel associated with this model. Lastly, a peak window is extracted from Fourier spectrum of periodicity map. The peak energy distribution behaves differently for single and DJPG compressed images. This property is exploited to derive the statistical features from the peak windows for classification purposes. Furthermore, Chen *et al.* [73] recommended a robust forensic method by performing the analysis of periodic characteristics of JPEG compression in spatial as well as in DCT domain in order to detect both the block aligned and misaligned recompression operations. It is assumed that genuine images are initially JPEG compressed and all forgery processes include recompression. It is also perceived that the performance of [73] is better when compared to BACM scheme [70] in most of the cases. Meng *et al.* [74] presented a copy-paste block detection approach by analyzing the artifacts of DJPG compression and it is noticed that these characteristics are closely related to quality factor. The copy-paste tampering disturbs the JPEG compression footprints of the resultant doctored image and it is observed that the DCT blocks are different for the two compressions.

Some methods do not rely on the classifier to recognize the presence of DJPG compression artifacts. These approaches are based on a simple threshold detector. A single feature is evaluated in [75] based on the integer periodicity of blockwise DCT coefficients, when DCT is evaluated with respect to the grid of preceding JPEG compression. The NA-JPEG compression is detected by observing the clustering of DCT coefficients nearby a particular lattice for any possible grid shift. Bianchi and Piva [75] performs the comparison with Luo *et al.* [70] method and Chen *et al.* [73] method by computing their features on same database and then feed them to SVM using radial basis function kernel. Compared to method [70], method [75] detector is 5% to 15% more accurate for similar sized images. While comparing to the method [73], it has 10% to 25% more detection accuracy for small sized images.

Most of the detection methods require previous knowledge of characteristics related to authentic and forged regions. To recognize the forged region in a blind way, processing of large number of image blocks is required, which also increases the computational load. Method [76] works on a particular JPEG image by dumping its DCT coefficients and quantization matrices for one Luma and two Chrominance (YUV) channels. This approach is capable of detecting the doctored regions automatically, which is not possible with the previous methods.

The limitation of method [76] is that if x is the DCT coefficient value and $H_0(H_1)$ indicates the hypothesis of being tampered then the conditional probability $p(x|H_1)$ is computed conforming to the detected histogram of x. Such a histogram is the combination of $p(x|H_1)$ and $p(x|H_0)$ for tampered images. Therefore for large forgeries, the histogram of x is expected to be a poor estimation of $p(x|H_1)$ [77]. This constraint of [76] is resolved in [77] by separating the two conditional probabilities from the observed mixture. It is also found that efficiency of the technique [77] is superior as compared to the approach [76].

2.1.3.2 Estimation of First Quantization Matrix from Double JPEG Compression

The recreation of the first quantization matrix utilized by the acquisition device which is lost during double compression is important in digital image forensics. The model of the camera devices utilizing the same quantization tables is identified by estimating some part of the first quantization matrix. Therefore, the estimation of the first quantization matrix from double compressed images is a challenging task for the researchers due to its importance in the digital investigation [63]. Zhang and Wang [78] proposed a technique to detect the in-camera JPEG compression for double compressed images along with the estimation of quantization steps. Besides, a novel technique for image analysis based on three visualization learning strategies is revealed in [79] to identify DJPG compression clues including the estimation of first quantization matrix.

Wang *et al*. [80] additionally points out image falsifications but does not provide a proper estimation of the first quantization matrix. A DCT coefficients histogram analysis is utilized in [33] to estimate the first quantization matrix from DJPG compressed image. The DJPG compressed images are investigated in [34] to evaluate the first quantization matrix for the case when first quantization step is larger than the second. The compression history of digital images

is exploited by the approach proposed in [44], which is based on the JPEG error investigation. It is observed that for JPEG compressed image with quantization steps equal to or greater than 2, the Alternating Current (AC) coefficients increase in the range $(-1, +1)$ and drop considerably in the union regions of $(-2, -1]$ and $[+1, +2)$. An effective 1-D feature is obtained based on this observation to differentiate between the uncompressed and JPEG compressed images. Moreover, a feature is formed to estimate the quantization steps from JPEG decompressed images by reducing the rounding error.

Pevný and Fridrich [81] proposed a method to reveal the DJPG compression artifacts along with the estimation of first quantization matrix lost during the process of recompression. Both the suggested methods are important in order to create the precise targeted and blind steganalysis approaches for JPEG images, specifically those that rely on calibration. Both methods are based on the SVM classifier trained on the features which are formed by analyzing the low-frequency DCT coefficients histograms. Additionally, Fan *et al.* [82] exploited the characteristics of DCT coefficients histogram. Gaussian and Laplacian distributions are used as a reference for Direct Current (DC) and AC coefficients respectively to approximate the envelopes of these histograms. The estimation of quality factor is achieved by applying the Maximum-Likelihood Estimation (MLE) method. It is worth noting that pixel values are rounded to integers during the reconstruction of JPEG image in spatial domain.

Fu *et al*. [35] observed that the distribution of most significant digits of DCT coefficients follows Benford's law [83 - 84] and that of the quantized JPEG coefficients follows Benford-like logarithmic law in the case of single JPEG compressed image. This distribution is easily affected by DJPG compression because logarithmic law is offended after DJPG compression. This attribute is suitable for digital image forensics based on JPEG compression and evaluation of first quantization steps [35]. The absolute QDCT coefficients histogram is investigated in [85] in order to estimate the quantization steps and a histogram-based feature is developed which is then provided to neural network for the purpose of classification. In this approach, firstly the considered image is investigated to calculate the absolute DCT coefficients histogram. Later, the JPEG blocks structure of an image is disturbed by performing a cropping operation and the resultant image is compressed with nominated quantization tables. Afterward, decompression operation is applied on the attained JPEG files and compressed again with secondary

quantization table. From all these JPEG files, different histograms are obtained. Estimator selects the quantization table to match the resulting histogram with the original image histogram [85]. Furthermore, the probabilities of the first digits of quantized DCT coefficients from specific AC modes are utilized for the detection of DJPG compressed images [86]. A two class classification strategy is employed to differentiate between the single and double compressed images.

The inherent statistics of the image which is processed with double compression is different from the statistics of single compressed image. Due to double compression, histogram of DCT coefficients does not follow generalized Gaussian distribution and results in zeros and double peaks. A reliable detection method is designed in [36] based on the characteristics acquired from the first-order statistical examination of individual DCT modes of low frequency coefficients by using SVM classifier. A maximum likelihood estimator is also employed to compute the primary quality factors in DJPG compressed images [36].

An improved DCT coefficient analysis is performed in [77] to distinguish between the single and double compressed regions along with the estimate of first quantization table. Bianchi and Piva [87] proposed a model to separate the genuine and tampered regions in JPEG images by characterizing the artifacts occurred in Non-Aligned Double JPEG (NA-DJPG) and Aligned Double JPEG (A-DJPG) compressions. A forgery localization method is recommended that follows the Bayesian approach. However, if some image processing operation such as image resizing is applied in between the two successive compressions then this method fails to detect the footprints of DJPG compression. Traces of A-DJPG compression can be correctly identified for $QF_2 = QF_1$ or $QF_2 << QF_1$, whereas for NA-DJPG only when $QF_2 > QF_1$. Here, QF_1 and QF_2 represent the quality factors used in first and second JPEG compression respectively.

2.1.3.3 Deep Learning based Detection Techniques

The recent literature on the JPEG compression detection techniques has been shifted to deep learning based forensic approaches. A general purpose forensic technique is proposed in [88] based on CNN. In this approach, a constrained convolutional layer is developed which is capable to mutually suppress an image's content along with the learning of tampering detection features adaptively. Verma *et al*. [89] suggested a forensic technique based on the deep CNN in DCT

domain to identify the multiple JPEG compressions. Many tests are executed to improve the features of the system such as CNN depth, number of DCT frequencies, and execution time.

The processing history of digital images is detected by using deep learning in [90]. The goal of this approach is to design a scalable detector for the cases when the image captured by the camera is processed, downscaled with different scaling factors, and JPEG compressed again. This kind of processing is widely employed, for example when images are uploaded to social networking sites such as Facebook, *etc*. Moreover, the detection of DJPG compression with same quantization matrix is an interesting task for the researchers due to very few footprints left in double compressed images with same quantization matrix. This issue is resolved in [91] by presenting a comprehensive feature based on the dense CNN framework, which is sensitive to double compression artifacts and is not associated with image content.

A detection method is proposed in [92] for DJPG compression artifacts based on CNN by considering the fact that histograms of DCT coefficients are different for single and double compressed regions. It is clear from the experiment results that this CNN-based forensic approach provides better results in terms of detection accuracy and forgery localization, particularly when the primary compression quality factor is larger than secondary quality factor. A CNN-based DJPG compression detection scheme is suggested in [93] by exploiting the statistical histogram features from each block with a quantization table in vector form. This approach is capable of handling mixed quality factors and appropriate for real-world situations. Moreover, a new data-driven method [94] based on a constrained CNN classifier is presented to extract the manipulation detection features, detect the multiple editing operations, and also estimate the order in which they were applied. The performance of this CNN-based approach is evaluated by considering various kinds of commonly used residual features.

The comparative analysis of SVM and CNN-based forensic techniques is still not commonly available in the existing literature. This is due to the fact that both approaches are designed for different scenarios. For example, SVM-based forensic techniques are used for simple classification of small-sized datasets, while CNN-based techniques are used for larger datasets and complex classification. Therefore in this thesis, the presented research work is evaluated by considering most of the recent SVM-based detectors in order to make the comparison feasible.

2.1.4 Anti-Forensics of JPEG Compression

Stamm *et al.* [95] offered a JPEG anti-forensic scheme that fills the gaps present in the DCT coefficients histogram of each sub-band to hide the traces of compression. DCT histogram smoothing is achieved by the dithering operation of [95] based on Laplace distribution of AC coefficients. The forensic detector suggested in [63] can detect the compression artifacts in DCT domain but it is effectively deceived by the dithering process suggested in [95].

Stamm *et al.* [96] recommended a deblocking procedure based on the median filtering which is applied after the DCT histogram smoothing to disguise the spatial domain forensic detector [63]. Later, the traces left during the anti-forensic scheme [95] can be identified by two advanced forensic detectors [97 - 98]. The anti-forensic technique in [95] degrades the image visual quality significantly, but the perceptual dithering method in [37] improves the quality of an image to some extent.

Li *et al*. [99] proposed a forensic technique for the detection of anti-forensically processed JPEG images. It is found that the dithering operation disturbs the statistical correlation between the 8×8 intrablock and interblock within the image. The forged images are classified from the original JPEG decompressed and uncompressed images on the basis of transition probability matrix of DCT coefficients. It is also observed that the JPEG forgery proposed by Stamm *et al*. [93] is unable to fool the machine learning detection method based on the steganalysis feature of [100]. A variational energy minimization based anti-forensic method is suggested in [38] to fool the current forensic methods in spatial domain by removing the blocking traces with high image quality. Some relative work is dedicated toward the anti-forensics of DJPG compression in [101] and JPEG forensics based on steganalysis approach using machine learning in [28].

The footprints of JPEG compression were concealed efficiently by the anti-forensic technique proposed in [95]. A dithering operation was introduced in this approach for the DCT histogram smoothing. The gaps of the comb-like DCT histograms of all the sub-bands are filled by this dithering operation to remove the artifacts of JPEG compression. Therefore, the resultant image processed through the dithering operation can be recognized as an anti-forensically processed image. In the case of an uncompressed image, the AC coefficients of the same sub-band follow Laplacian distribution defined as:

$$P(Y = y) = \frac{\gamma}{2} e^{-\gamma|y|} \tag{2.1.5}$$

where, Y denotes the DCT coefficient of original uncompressed image at the (r, c)-th sub-band, and γ represents the Laplacian parameter. The distribution of quantized AC coefficients follows discrete Laplacian distribution for JPEG image. For the (r, c)-th sub-band coefficients with quantization step $q_{r,c}$ of the quantization matrix q, the distribution can be modeled as [95]:

$$P(Z = z) = \begin{cases} 1 - e^{-\frac{\gamma q_{r,c}}{2}} & if\ z = 0 \\ e^{-\gamma|z|} \sin\left(\frac{\gamma q_{r,c}}{2}\right) & if\ z = k q_{r,c} \\ 0 & otherwise \end{cases} \tag{2.1.6}$$

where, $Z = q_{r,c}.round(Y/q_{r,c})$, and MLE is employed to generate the parameter $(\gamma = \gamma_{mle})$. In the dithering operation, the comb-like DCT histograms for each sub-band are formed due to the discreteness of Laplacian distribution. Therefore, to approximately reconstruct DCT coefficients histogram of each sub-band, noise is added to the AC coefficients of each sub-band as follows:

$$D = Z + N \tag{2.1.7}$$

Here D is the dithered image coefficient, N is the added noise and the noise distribution for the coefficient Z having zero value at the (r, c)-th position which can be modeled as [95]:

$$P(N = n|Z = 0) = \begin{cases} \frac{1}{c_0} e^{-\gamma|n|} & if\ \frac{-q_{r,c}}{2} \le n < \frac{q_{r,c}}{2} \\ 0 & otherwise \end{cases} \tag{2.1.8}$$

where, $c_0 = 1 - e^{-\gamma q_{r,c}/2}$, and the distribution for the non-zero coefficient values is given as:

$$P(N = n|Z = z) = \begin{cases} \frac{1}{c_1} e^{-sgn(z)\gamma(n + q/2)} & if\ \frac{-q_{r,c}}{2} \le n < \frac{q_{r,c}}{2} \\ 0 & otherwise \end{cases} \tag{2.1.9}$$

where, $c_1 = (1/\gamma)(1 - e^{-\gamma q_{r,c}})$.

Moreover, an optimal anti-forensic scheme is presented in [102] based on the convex cost function in order to fool the forensic methods that rely on the analysis of first-order image histogram. Similarly, a JPEG anti-forensic technique comprising of four-steps is proposed in [39]

which includes first-round TV-based deblocking, perceptual DCT histogram smoothing, second round TV-based deblocking and decalibration operation. The gaps in the DCT coefficients histogram are partially filled by the TV-deblocking operation. An adaptive local dithering signal model [39] is applied to completely fill the gaps left during the TV-based deblocking on the basis of Laplace and uniform distributions. Afterward, second round of TV-based deblocking is applied to remove the blocking artifacts in spatial domain. This second round of TV-based deblocking provides a JPEG forgery capable of fooling most of the forensic detectors except calibration based forensic detector. Therefore, a decalibration operation is engaged to fool the calibration based forensic detector.

2.1.5 Counter JPEG Anti-Forensics

The previous countering JPEG anti-forensic techniques [37, 97, 103] proposed by Valenzise *et al.* suggested that dithering operation introduced in [95] reduced the visual quality of an image. An efficient forensic detector is designed by Valenzise *et al.* [103] to detect the traces of dithering by analyzing the effects of noise in the re-compressed forms of considered image. This noisiness measure is based on the TV of re-compressed image. The image under test is re-compressed by the detector with different quality factors $q = \{1, 2, 3, \ldots, 100\}$. Then, TV of the re-compressed image $TV(q)$ is calculated as the function of the quality factor (q). The forensic measure can be defined as:

$$K_V = \max_{q \in \{1,2,3,\ldots,100\}} \Delta TV(q) \tag{2.1.10}$$

where, $\Delta TV(q)$ is the first-order backward finite difference, which can be evaluated as:

$$\Delta TV(q) = TV(q) - TV(q-1) \tag{2.1.11}$$

A calibration-based detector is proposed by Lai and Bohme in [98] against the JPEG anti-forensic scheme suggested in [95]. In this detector, the variance of the sub-bands from a given image X is compared with the variance of the sub-bands from the calibrated version X_{cal} of given image X. The calibrated measure K_L can be defined as:

$$K_L = \frac{1}{28} \sum_{k=1}^{28} \left| \frac{var(D_k X) - var(D_k\, X_{cal})}{var(D_k X)} \right| \tag{2.1.12}$$

where, $var(.)$ is the variance function and D_k denotes the DCT coefficients matrix for k-th high frequency sub-band.

The process of creating JPEG forgeries [95 - 96] is considered as data hiding by Li *et al.* [99] according to the JPEG steganalysis point of view. The image statistics based on intra and inter-block are modified by the anti-forensic process. These changes can be measured by using the Markov Transition Probability Matrix (MTPM) [100]. The Subtractive Pixel Adjacency Matrix (SPAM) feature [28] is utilized for countering the anti-forensics of JPEG compression [103].

JPEG blocking artifacts can be identified by using a family of measures suggested in [38] as:

$$K_U^p = \left| B_{gr}^p(X) - B_{gr}^p(X_{cal}) \right| \tag{2.1.13}$$

where, B_{gr}^p denotes the gradient aware blockiness defined as the normalized l_p norm of weighted gradient calculated from every cluster of four adjacent pixel values across 8×8 block borders. A family of different measures can be obtained by varying the parameter p. Furthermore, a multi-purpose forensic detector based on the autoregressive model is proposed in [104] to counter the image anti-forensics.

An adversary-aware DJPG compression recognition method is proposed in [105] based on SVM classifier having the capability to detect the compression traces even in the presence of anti-forensic techniques. The classifier is fed with huge number of features and training is performed to identify the footprints added during the DJPG compression. It is difficult to consider all the anti-forensic attacks, so limited number of anti-forensic attacks is used in training for evaluation purposes.

Besides, a multi-purpose technique is presented in [106] based on the novel CNN to detect the various image manipulations processed with anti-forensic schemes. In this approach, the propagation of general features related to the detection of image tampering is enhanced by exploring the dense connectivity pattern. This counter anti-forensic approach based on CNN architecture provides better performance with 13% improvement in detection accuracy for low-quality JPEG images. Li *et al*. [107] suggested a data-driven technique for counter JPEG anti-forensics based on CNN by taking input from raw JPEG DCT coefficients as well as decompressed image pixels. The complex relationship both within and between DCT sub-bands

along with the spatial artifacts both inside and between JPEG grids are explored to incorporate the expert information regarding JPEG artifacts in CNN design. This deep learning based approach can efficiently identify the DJPG compression and associated anti-forensic processes. Both the DCT and spatial domains information is taken into account by the end-to-end CNN.

The numerous JPEG forensic approaches used to estimate the capability of the proposed JPEG forensic and anti-forensic techniques are as follows:

- K_F, JPEG compression blocking artifacts detector [63].
- K_F^q, represents the detector based on the quantization table estimation [63].
- K_{Weiqi}, JPEG identifying detector [44].
- K_{Weiqi}^q, quantization step estimation based detector [44].
- K_V, TV-based JPEG forensic detector [97, 103].
- K_L, calibration feature based JPEG detector [98].
- K_U^1 and K_U^2, represents the JPEG blocking artifacts detectors [38].
- K_{Li}^{S100}, detector based on 100-D intra and inter-block correlation feature [99 - 100].
- K_P^{S162}, detector based on 162-D SPAM feature [28].
- K_{AR}^{S10}, an autoregressive model based detector [104].
- K_{SPAM}^{S686}, 686-D SPAM feature based detector [28].
- K_{SRM}^{S714}, detector based on residual-based feature [29].

The JPEG anti-forensic techniques employed to authenticate the performance of presented counter anti-forensic approach of JPEG compression are as follows:

- $\mathcal{AF}_{S_q}$, represents the DCT histogram smoothing anti-forensic scheme [95].
- $\mathcal{AF}_{S_qS_b}$, dithering and deblocking operation based anti-forensic method [96].
- $\mathcal{AF}_V$, represents a perceptual anti-forensic dithering technique [37].
- $\mathcal{AF}_{S_u}$, anti-forensic technique with Shrink-and-Zoom (SAZ) attack [101].
- $\mathcal{AF}_F$, represents the TV-based anti-forensic approach [38].
- $\mathcal{AF}_{Fan}$, adaptive dithering model based four-step JPEG anti-forensic scheme [39].

2.2 Evaluation Metrics

The image anti-forensics aims to achieve good image visual quality and better forensic undetectability of the anti-forensically processed image as mentioned in Chapter 1. The forensic undetectability can be evaluated from the Receiver Operating Characteristics (ROC) curve [39]. The anti-forensic method having good forensic undetectability can efficiently disguise the forensic techniques. On the contrary, the forensic detectors with good forensic detectability can competently reveal the traces of anti-forensics.

Certainly, the main objective of anti-forensics is to achieve better forensic undetectability of the processed image. However, the image visual quality is also a significant concern to be considered during the evaluation of a particular anti-forensic technique. This is due to the fact that a low quality image may raise doubt on the authenticity of the processed image. The evaluation of the image quality is done by using Peak Signal-to-Noise Ratio (PSNR) and Structural SIMilarity (SSIM) metrics.

2.2.1 Forensic (Un)detectability

The ground truth is compared with the classification output of the forensic detectors attained on a group of images to evaluate the forensic or anti-forensic method performance. The forensic detector's classification output attained on a group of images is compared with the ground-truth in order to estimate the performance of a forensic or an anti-forensic method. Let us consider N_N genuine (unprocessed) images as negative cases and N_P forged (processed) images as positive cases for forensic testing. Assume that N_{FP} represents the number of negative cases that are wrongly categorized as positive among the N_N negative cases. On the other hand, let N_{TP} signifies the number of positive cases that are correctly categorized as positive among the N_P positive cases. Therefore, False Positive Rate (FPR) and True Positive Rate (TPR) for every classification scheme of forensic detector are evaluated as [108]:

$$FPR = \frac{N_{FP}}{N_N}, \quad TPR = \frac{N_{TP}}{N_P} \tag{2.2.1}$$

The various classification strategies of a forensic detector provide (FPR, TPR) pairs based on which ROC curve is plotted. Afterward, the accuracy of the classifier can be measured from the

Area Under Curve (AUC) [109]. For example, AUC of value 0.5 corresponds to 50% accuracy. The ROC can be categorized into five types based on different classification strategies [110] as shown in Figure 2.4. Moreover, in steganalysis approaches [111] and [112], the performance of forgeries against different forensic detectors is normally evaluated on the basis of minimum decision error (P_e). The JPEG (anti-forensic) and original images are considered as positive and negative cases respectively to evaluate the ROC curve for JPEG forensic detectors. The minimum decision error (P_e) is denoted by a point on the ROC curve having minimum number of incorrectly classified images [39]. It is worth noting that the more the curve is close to the diagonal (random guess), the higher is the forensic undetectability against the considered detector.

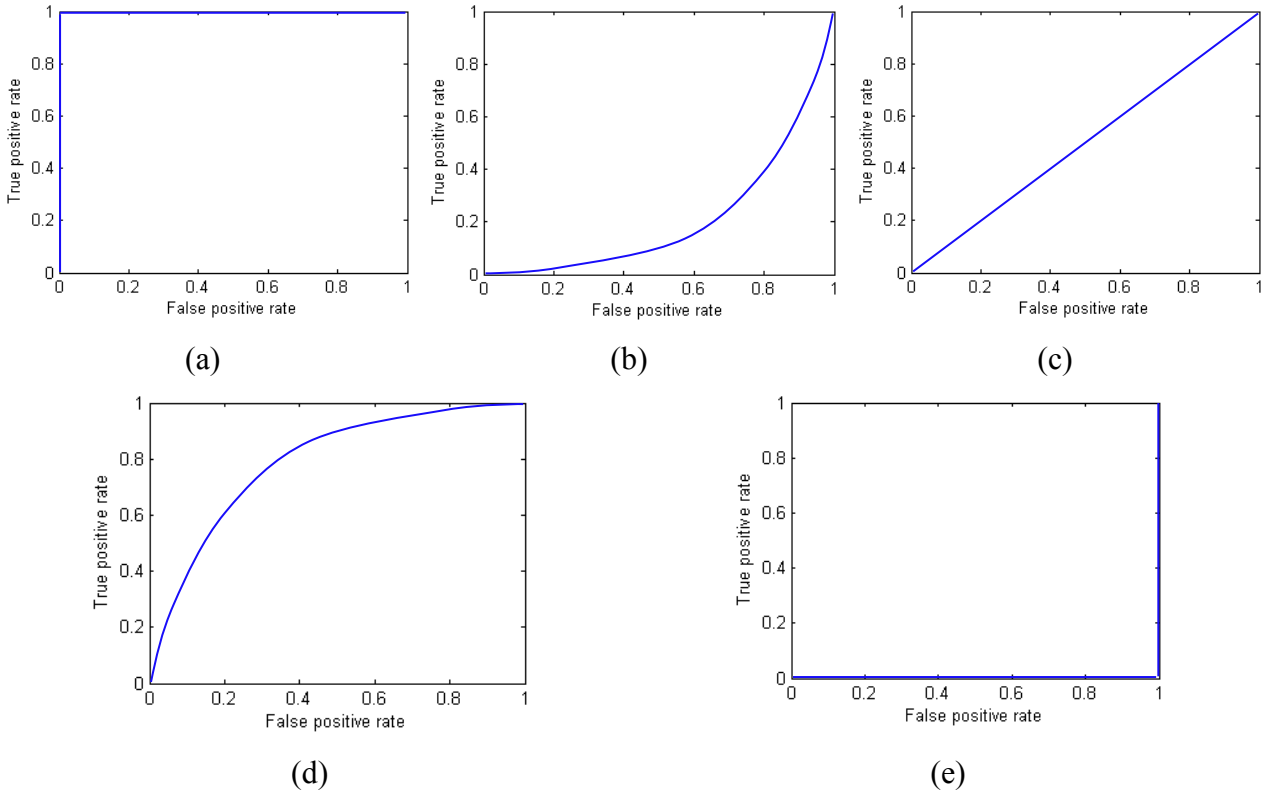


Figure 2.4: ROC curves having AUC (a) 1, (b) between 0 and 0.5, (c) 0.5, (d) between 0.5 and 1, (e) 0.

Both the original and doctored images datasets along with a forensic detector are required to perform forensic testing. The datasets containing genuine images as described in Section 2.3 are used in this thesis for forensic testing purposes. Each image is processed with different anti-forensic techniques to create the databases of corresponding image forgeries. Finally, forensic

testing is performed by considering an equal number of original and processed images. On the contrary, the feature of a particular forensic technique can either be scalar or vector, based on which the forensic tests are different to some extent. The SVM is often adopted to train the forensic detector in the case when feature is vector-based. The forensic test is conducted for the evaluation of forensic (un)detectability by considering the various scalar and SVM-based detectors.

2.2.1.1 Scalar-based Forensic Detectors

The output of a scalar-based forensic detector is a single feature value for a given image. Based on the comparison between this feature and a pre-defined threshold, the image under analysis can be classified as authentic or forged by forensic detector. If the value of feature is large (or small) as compared to the value of threshold, then the considered image is categorized as forged (or original) [38].

Different classification outcomes are created with the variation in threshold value. The detector yields the feature value corresponding to each image in the experiments of forensic testing. These feature values are considered as different thresholds values to produce different classification strategies. Then, ROC is plotted and minimum decision error is calculated [39].

In the case of highly compressed JPEG images, most of the DCT coefficients that correspond to high-frequency sub-bands are quantized to zero. Thus, it results in the difficulty in determining the quantization steps [39]. Thus, in the scalar-based forensic detector K^{q}_{Weiqi}, initially the quantization steps values are calculated and then the values greater than 1 are used as a feature. The output of all scalar-based forensic detectors K_F, K_{Weiqi}, K^{q}_{Weiqi}, K_V, K_L, K^{1}_{U}, K^{2}_{U} considered in this thesis to measure the capability of the projected anti-forensics and counter anti-forensics is a single value feature for given test image. On the basis of threshold value, the given image can be classified as an uncompressed or compressed by the forensic detector.

2.2.1.2 SVM-based Forensic Detectors

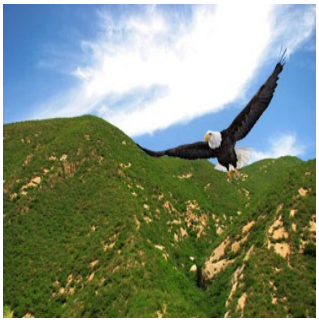
The output of numerous forensic detectors is in vector form. The employment of two-class SVM is the most common method in image forensics to construct the detector on the basis of vector-based feature [39]. In this work, the SVM classifier is utilized to calculate the efficacy of

proposed JPEG forensics and anti-forensics. In the case of SVM-based detectors, it is assumed that forensic detective is aware of different forensic and anti-forensic techniques. Therefore, the examiner is capable to produce a forged images dataset for training the detector. This can be taken as the worst-case scenario for the anti-forensic techniques. In this scenario, the existing SVM-based detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} can efficiently overcome the JPEG anti-forensic techniques. It is also supported by the fact in [23, 39] that it is a difficult task for anti-forensic schemes to fool the machine learning based detectors. This is the worst case for the JPEG anti-forensics but beneficial for the JPEG compression forensics. For the given feature vector, the SVM-based detector is trained with each type of JPEG anti-forensic image. The SVM-based forensic detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} are generally utilized in steganalysis, having high detection accuracy with minimum decision error values less than 0.1. Afterwards, the further analysis is performed by considering the less challenging situation (optimistic scenario) for the JPEG anti-forensics. In this scenario, now the original and JPEG compressed images are used to train a single forensic detector for each type of feature vector.

In image steganalysis, modification of DCT coefficients results in a high modification rate represented by bits per pixel (bpp). The performance analysis of the presented schemes is done by creating the JPEG forgeries by using the substitution process [39]. In this method, the central portion of a particular uncompressed image is replaced by the image processed with JPEG anti-forensics. The replacement rate is varied from 0.05 to 1 in the substitution process. Forensic testing is based on both the processed and uncompressed images. The SVM training is performed by considering the LIBSVM [113] with a Gaussian kernel. The five-fold cross validation [28] is employed with multiplicative grid to obtain the SVM parameters. The uncompressed images and their equivalent JPEG (anti-forensic) images are utilized to train SVM classifiers. Figure 2.5 shows the creation of composite JPEG forgery [114]. Firstly, the eagle portion is taken from the image of quality q_2 and is pasted to an image of quality q_1. Afterward, this image is JPEG compressed again with a quality factor q_3 result in composite JPEG forgery.

(a) JPEG compressed image with quality q_1

(b) JPEG compressed image with quality q_2



(c) DJPG compressed image

Figure 2.5: Illustration of generating a composite JPEG image.

The SVM classifier outputs a decision value for each image when forensic testing is performed by considering a given SVM-based forensic detector. Different classification strategies are realized similar to the scalar-based forensic detectors by changing the threshold values. Then, a plot of ROC curve is generated along with the estimation of minimum decision error. It is worth noting that designing a SVM-based counter JPEG anti-forensic method is also the main focus of the research work conducted in this thesis along with the enhancement of JPEG anti-forensics.

2.2.2 Image Quality

The assessment methods for image quality are categorized into two classes *i.e.*, no-reference and full-reference techniques based on the fact that whether the original image is accessible [115]. The original image is commonly unknown in real-world scenarios. Though, in scientific research, we often maintain the ground truth. Therefore, the performance of the algorithm is calculated by considering the full-reference approach. Only 8-bit grayscale images are used in this thesis for performance analysis. To measure the image quality, we use two generally employed full-reference evaluation metrics: PSNR and SSIM.

PSNR is the widely used image quality measure which is expressed by using famous Mean Squared Error (MSE). Let us consider a reference grayscale image X of size $T \times T'$ and its anti-forensically processed version is denoted by Y. The PSNR value in decibel (dB) can be calculated as [115]:

$$PSNR(\mathrm{X}, \mathrm{Y}) = 10\, log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{2.2.2}$$

where, MAX represents the maximum value of a pixel in an image ($MAX = 255$ for 8-bit grayscale images) and MSE is defined as:

$$MSE(\mathrm{X},\mathrm{Y}) = \frac{1}{T \times T'} \sum_{i=1}^{T} \sum_{j=1}^{T'} [\mathrm{X}(i,j) - \mathrm{Y}(i,j)]^2 \tag{2.2.3}$$

The PSNR is a traditional evaluation metric of image quality which is further improved by Wang *et al.* [116] by suggesting the SSIM metric with enhanced correlation with subjective scores of image quality. The SSIM metric is based on the Human Visual System (HVS) properties as compared to the PSNR. Suppose X is a reference grayscale image and its approximated version is represented by Y, and then SSIM can be denoted as:

$$SSIM(\mathrm{X},\mathrm{Y}) = (lum(\mathrm{X},\mathrm{Y}))^{\boldsymbol{a}} \times (con(\mathrm{X},\mathrm{Y}))^{\boldsymbol{b}} \times (str(\mathrm{X},\mathrm{Y}))^{\boldsymbol{c}} \tag{2.2.4}$$

where, $lum(\mathrm{X},\mathrm{Y})$, $con(\mathrm{X},\mathrm{Y})$ and $str(\mathrm{X},\mathrm{Y})$ functions compare the luminance, contrast, and structure respectively. These three comparison functions are balanced by using the parameters $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{c}$ (where $\boldsymbol{a} = \boldsymbol{b} = \boldsymbol{c} = 1$ is one of the commonly used settings). Moreover, the SSIM is also a symmetric measure $SSIM(\mathrm{X},\mathrm{Y}) = SSIM(\mathrm{Y},\mathrm{X})$. More is the value of SSIM measure, higher is the image quality of processed image Y.

2.3 Natural Image Datasets for Forensic Testing

Some natural image datasets having genuine images are required to perform forensic testing. In this section, information is provided regarding the public natural image datasets used in the comprehensive experimental tests conducted in this thesis for JPEG forensic testing.

The effectiveness of the suggested anti-forensic and counter anti-forensic approaches in Chapter 4 and Chapter 5 respectively is evaluated by conducting numerous test on Uncompressed Color Image Database (UCID) [117]. The UCID dataset comprises of 1338 Tagged Image File Format (TIFF) images of Red, Green, Blue (RGB) scale having size 512×384 with a sure disparity in terms of scene contents. These images are firstly converted from RGB to $Y'C_BC_R$ during the JPEG compression. The data is separately JPEG compressed in each of the luma (Y'), blue-difference chroma (C_B), and red-difference chroma (C_R) components. In

this thesis, the JPEG forensic testing is executed by considering only luma component of the image. The luma data for each RGB UCID image is extracted by using the Matlab function rgb2ycbcr. Afterward, this luma data is saved in Portable Gray Map (PGM) format as an 8-bit grayscale image. The images from UCID dataset are compressed with different quality factors in the range $\{50, 51, 52, \ldots, 95\}$ that are subsequently processed anti-forensically in order to create JPEG forgeries database. The training dataset (UCIDTrain) is created by selecting 669 images randomly from UCID dataset and remaining images are used for testing dataset (UCIDTest).

Furthermore, another relatively large image database is also considered to evaluate the performance of the presented counter JPEG anti-forensics called as BOSSBase dataset [118]. This BOSSBase dataset contains 10,000 images in raw format having high resolution. The original raw images of BOSSBase dataset are transformed to 8-bit grayscale PGM images after converting them into PPM format by using *UFRaw* utility [119]. Each grayscale BOSSBase image is cropped from the center to provide a sub-image of size 512×512 for the purpose of forensic testing. The strategy as used for UCID images is followed to prepare the training and testing datasets for BOSSBase images. To test the SVM-based detectors, we select 5000 images from the BOSSBase image database for forensic testing dataset named as BOSSBaseTest and remaining images constitute BOSSBaseTrain dataset for training purposes. Then, these images are processed with various image operations to create the processed image datasets.

2.4 Research Gaps

From the above mentioned literature review, the following gaps are obtained:

- In the previous JPEG anti-forensic work, most of the methods were motivated by the need to remove the JPEG blocking artifacts in spatial domain. Therefore, there is a scope to optimize the anti-forensics by removing the compression artifacts both in spatial and DCT domains.
- There is a scope to improve the robustness of the anti-forensic technique against various forensic detectors.
- Most of the JPEG anti-forensic techniques are unable to make a proper balance between forensic undetectability and image quality. Therefore, there is a scope to achieve a better tradeoff between the quality of image and forensic undetectability.

- Most of the forensic techniques for the detection of JPEG compressed (both single and double) images usually rely on the analysis of first-order statistics derived from the image histogram. These forensic techniques based on first-order statistical analysis can be easily circumvented by adopting anti-forensic attacks. Therefore, there is a scope to conduct a higher order statistical analysis for better detection.
- Moreover, the existing counter JPEG anti-forensic schemes have not considered all of the existing JPEG anti-forensic methods due to the issue of different strengths of anti-forensic schemes. Therefore, there is a scope to resolve this issue by creating an effective feature which is capable of fooling most of the existing JPEG anti-forensic methods.
- The forensic technique based on a particular image processing operation is not able to detect other operations. Most of the existing approaches in the literature are based on this fact. Thus, a multi-purpose forensic method is required to detect the different image operations without considering the specific artifacts of a particular image operation.
- Various techniques are being used for the detection of JPEG compression (*i.e.*, single and double) and to estimate the first quantization steps/matrix that help in digital investigation to find the authenticity of an image. Most of these techniques ignore the effect of the error introduced by rounding, truncation, color conversions (for example, YCbCr to RGB), *etc*. Here Y is the luma component and Cb and Cr are the blue and red chroma components. Therefore, there is a scope to deal with this error properly.
- All the techniques in the literature are based on the concept of estimating the first quantization steps/matrix from double compressed JPEG images. There is a scope to estimate the first quantization matrix from the partial DJPG compressed images.

2.5 Research Objectives

Based on the initial studies, literature survey (as reported) and the understanding established the following objectives are proposed:

1. To study and analyze the existing forensics and anti-forensics techniques for double compressed doctored JPEG images.
2. To propose the anti-forensic technique for double compression in DCT domain by removing the compression artifacts in order to fool the existing JPEG forensic detectors.

3. To evaluate the robustness of the proposed technique against different types of forensic attacks.
4. To conduct a statistical analysis of double compressed JPEG doctored images to cope with double compression anti-forensics.

2.6 Research Methodology

The main emphasis of the research work is to enhance the digital image forensic and anti-forensic techniques based on JPEG compression. Thus, the existing JPEG forensic and anti-forensic techniques are analyzed in order to find out the various limitations and present issues. Based on these limitations, the research work is initially targeted to design a forensic technique for DJPG compression. In the first stage of this approach, the double compressed region is automatically isolated from the considered partial double compressed image. Then, the isolated region is processed in the second stage to estimate the first quantization matrix.

The research work is also devoted to design an anti-forensic technique for JPEG compression (both for single and double) by removing the compression artifacts in both spatial and DCT domain. The analysis would be carried out by considering the histogram of DCT coefficients obtained from the given image. The histogram analysis provides the information of the compression artifacts and these artifacts would be removed by using various techniques such as histogram smoothing, filtering and by filling the histogram gaps. Two denoising algorithms are suggested in this scheme to eliminate the grainy noise left during the histogram smoothing. Then, the spatial blocking artifacts are reduced by using TV-based deblocking process. Moreover, the performance of the proposed JPEG anti-forensics is evaluated against various forensic attacks.

Moreover, a higher order statistical forensic analysis based on CM is performed to design a counter JPEG anti-forensic scheme. In this analysis, a second-order statistical feature is generated to identify the variance discrepancies introduced by the dithering operation of anti-forensic techniques. The considered JPEG forensic and anti-forensic techniques are evaluated by considering the UCID and BOSSBase image datasets. All the simulations are performed by using MATLAB R2016a software on a PC with 2.13 GHz CPU and 3 GB RAM. The flow of the research work carried out in this thesis is provided in Figure 2.6.

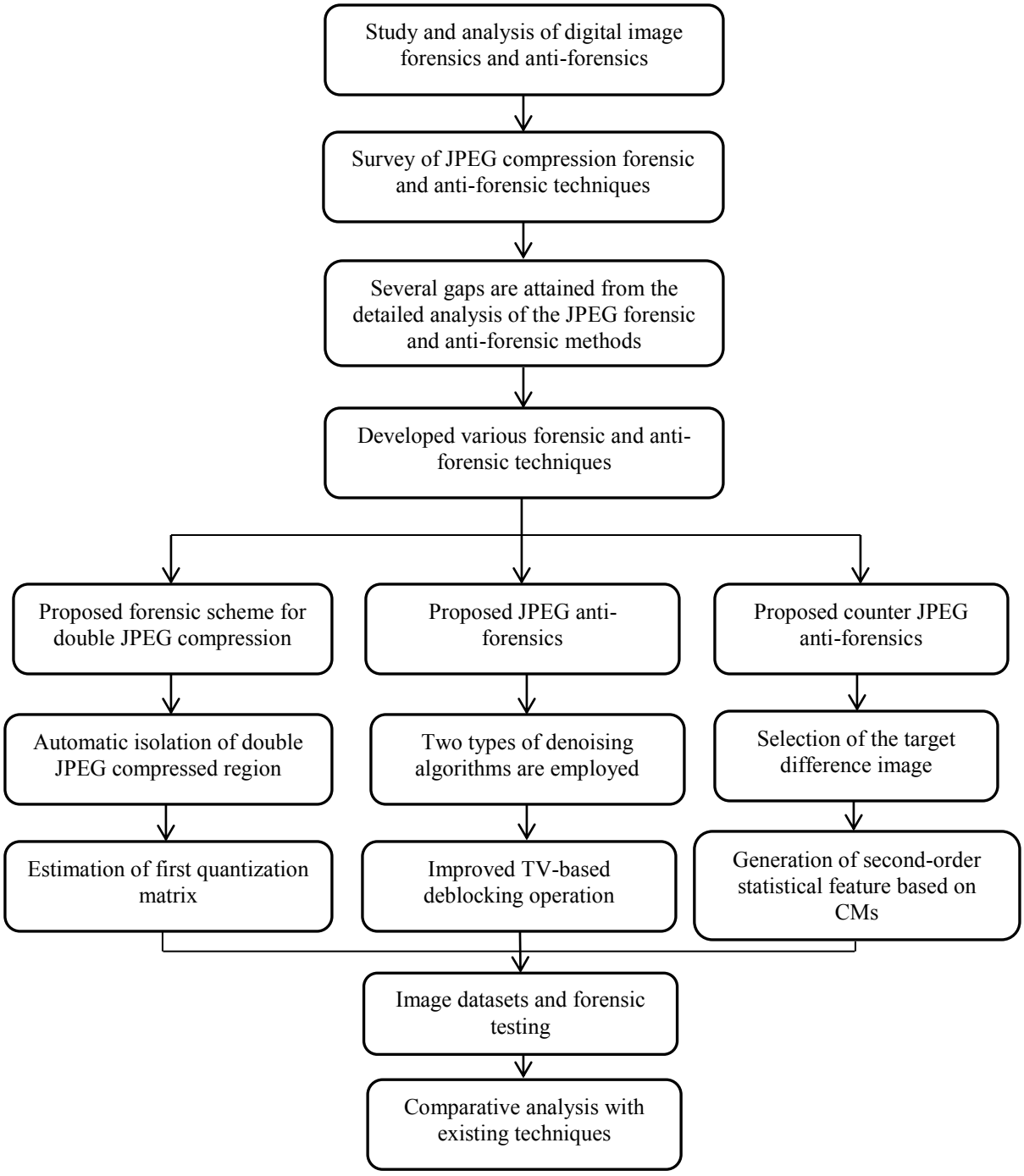


Figure 2.6: Research methodology for the proposed work.

CHAPTER 3

FORENSICS OF DOUBLE JPEG COMPRESSION

The comprehensive study of the literature related to digital image forensics and anti-forensics creates the necessity to further explore the JPEG compression artifacts in order to design an efficient forensic technique. In this chapter, the forensic analysis is performed on the double compressed JPEG images to recover the historic information lost during the double compression such as quantization matrix. The estimation of first quantization matrix plays an important role in the digital investigation process. Numerous forensic methodologies for DJPG compression are available in the literature for the approximation of primary quantization matrix. However, most of the forgeries are created by pasting some portion of an image on the other image and then the resultant image is resaved with different quality. Therefore, the estimation of primary quantization matrix from partial DJPG compressed images will further enhance the forensic investigation process. Therefore, in this work, an attempt is being made to analyse the partial DJPG compressed images to evaluate the primary quantization matrix. In the first stage, a technique is proposed not only to detect but also to automatically isolate the doubly compressed region from the image. Therefore, this isolation of double compressed region solves the problem of primary quantization matrix estimation from partial DJPG compressed images. The second stage analyzes the isolated doubly compressed region to estimate the first quantization matrix. In the latter stage, a filtering technique is proposed to optimize the performance of the algorithm by reducing errors. It is worth noting that the proposed approach is solely dedicated to detect the region which is re-compressed using a different quantization matrix. The experimental results confirm that the proposed forensic method provides improved results in comparison to the existing methods.

3.1 Analysis of Double JPEG Compression Artifacts

The first step in the JPEG compression is the DCT. The DCT of the image is performed by dividing the whole image into non-overlapping blocks of 8×8 blocks. The DCT is performed to segregate the high frequency components from the low frequency components of the image.

Then a quantization is applied by using the 8×8 quantization matrix integer value for each DCT coefficient. The error generated in this phase is known as quantization error. This error is the key reason of loss of information in JPEG compressed images. After this, it is transformed into a data stream with the utilization of classic entropy coding [44]. The process of image compression is backtracked conversely while achieving the JPEG decompression. If the same scheme is employed on JPEG image, with a different quantization matrix, the result would yield a double compressed image.

The quantization is followed by the rounding and truncating of real values to transform the range of integers into the range of [0, 255]. In this process, rounding values and truncation error are produced. In addition to these errors, another type of error occurs due to the conversion between RGB and YCbCr color spaces [44]. The error analysis can be performed on the 8-bit gray scale images. After double compression, the value of each double quantized coefficient c_{DQ} can be modeled as [32]:

$$c_{DQ} = \left[\left(\left[\frac{c'}{q_1}\right] q_1 + e\right)\frac{1}{q_2}\right] \tag{3.1.1}$$

where, c' denotes the single DCT coefficient value, q_1 and q_2 are the first and second quantization steps. The operator $[.]$ indicates the rounding function, and e includes the error due to various operations like rounding, truncation, color space conversions, *etc*. To infer the value of q_1, further compression is performed in a proper range with a novel quantization step q_3 and this error is computed by using an error function as follows [32]:

$$d_e(c', q_1, q_2, q_3) = \left|\left[\left[\left[\frac{c'}{q_1}\right]\frac{q_1}{q_2}\right]\frac{q_2}{q_3}\right] q_3 - \left[\left[\frac{c'}{q_1}\right]\frac{q_1}{q_2}\right] q_2\right| \tag{3.1.2}$$

When double compression is carried out on an image, only the last quantization steps are accessible but the first ones cannot be accessed because they are lost. Figure 3.1 (c) indicates the DCT histogram of an image after double quantization with its zoomed version for better understanding. The primary quantization is carried out by taking a quantization step $q_1 = 11$ and then acquired values of DCT coefficients are de-quantized with the same quantization step. Conclusively, the values are again quantized using a quantization step $q_2 = 7$. Apparently, the

distribution of the doubly quantized values contains periodic empty bins. This happens because during the second quantization, the coefficient values are re-distributed into more bins than in the first quantization. On the contrary, some bins contain more coefficients as compared to the neighboring bins when quantization step size increases. This occurs for the reason that even bins obtain coefficients from more original histogram bins as compared to the odd bins [21].

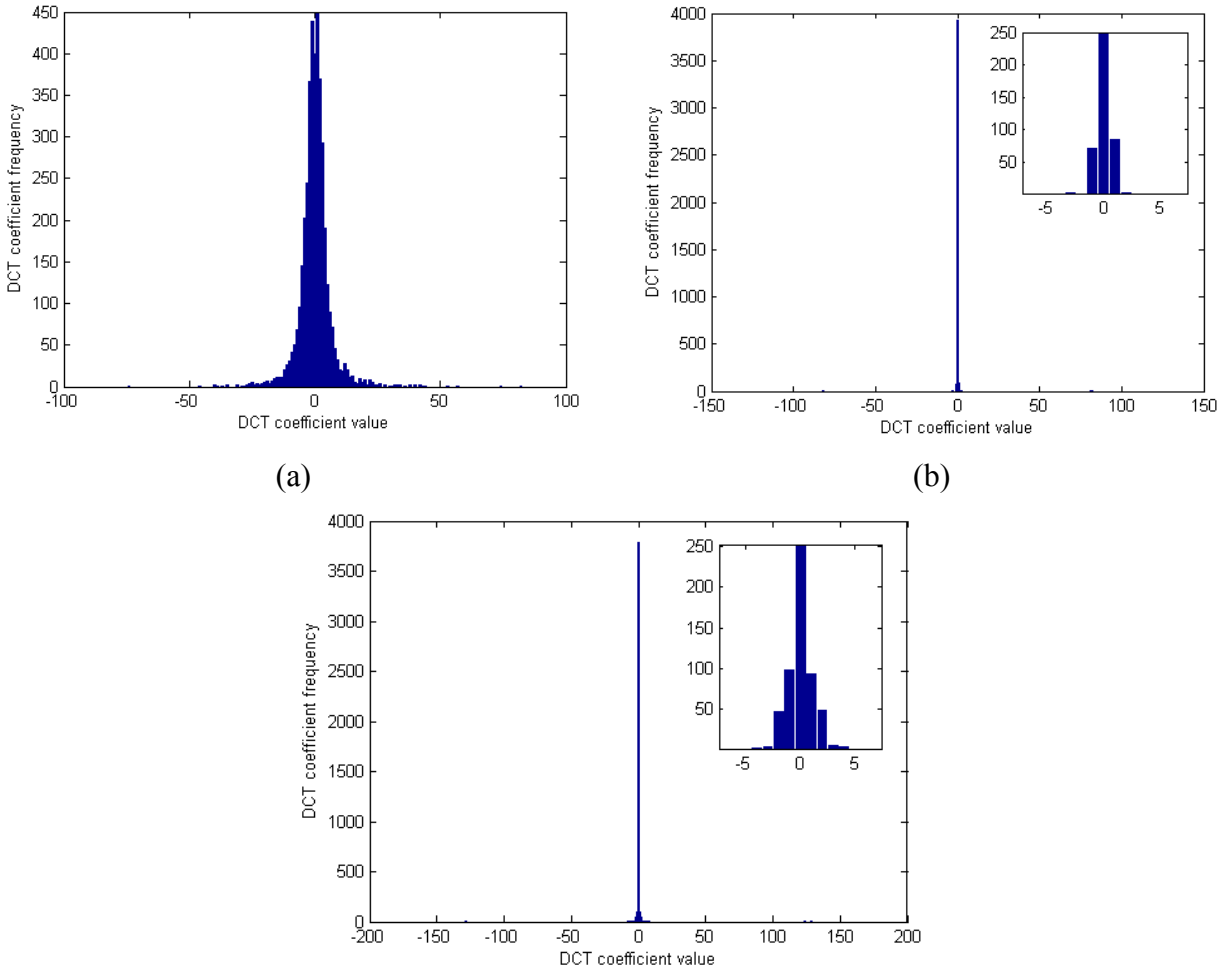


Figure 3.1: DCT histogram of sub-band (2, 2) for (a) uncompressed image, (b) after the first compression with $q_1 = 11$, and (c) after second compression with $q_2 = 7$.

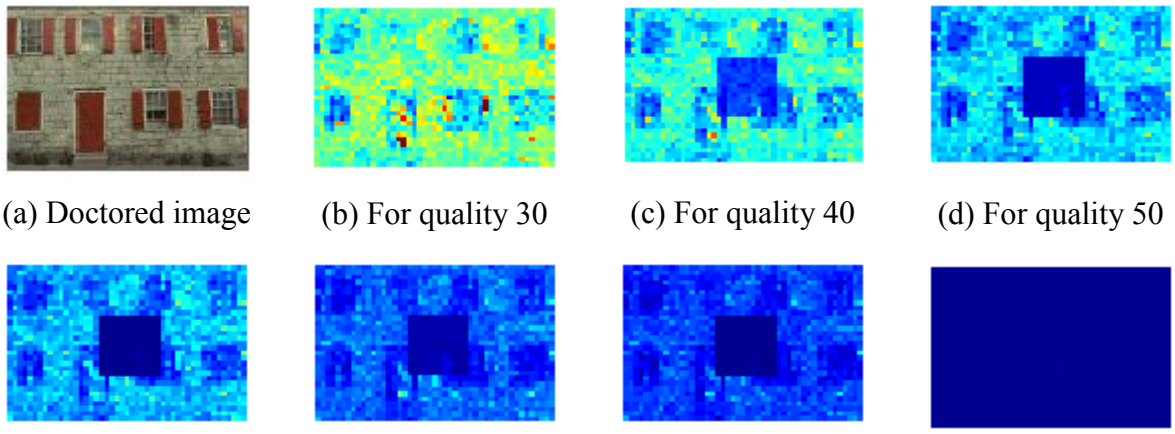
3.2 The JPEG Ghost Detection

Many forensic techniques are available in the literature to detect the DJPG compression. The JPEG ghost detection technique is one of the frequently used detection approach [32, 120] which has the capacity to localize the parts of an image which have gone through double compression.

Consider a DCT coefficient c_1' which is quantized by an amount q_1. Then the resultant coefficient from first quantization is subsequently quantized second time by quantization step q_2, which results in coefficient c_2'. With the exception of $q_2 = 1$, the difference between c_1' and c_2' will be minimum when $q_2 = q_1$ and increases with the increase in the difference between q_2 and q_1. The JPEG ghost can be identified in all three color channels individually by considering every spatial frequency independently. However, the comparison of integer multiple quantization values provides various minima points. The pixel values are directly utilized to calculate the difference given as [32]:

$$d'(x, y, q) = \frac{1}{3}\sum_{i=1}^{3}\left[f(x, y, i) - f_q(x, y, i)\right]^2 \tag{3.2.1}$$

where, $f(x, y, i)$, i = 1, 2, 3, indicates each of three RGB color channels, and $f_q(.)$ is the result of compressing $f(.)$ at quality q.



(a) Doctored image (b) For quality 30 (c) For quality 40 (d) For quality 50

(e) For quality 60 (f) For quality 70 (g) For quality 80 (h) For quality 90

Figure 3.2: Double compressed region detection through JPEG Ghost: (a) Partial double compressed doctored image, (b)-(h) Difference images corresponding to the different quality factors.

The inherent image content results in specific disparity in the difference images. These difference images reveal the dissimilarity between the tampered and non-tampered regions in an image which can be used for forensic examination. The central portion of size 200×200 of an original image is saved at quality factor 60. This portion is re-inserted into the image with quality 90 and resaved with quality factor 90, results in a partially double compressed image or tampered

image as shown in Figure 3.2 (a). The difference between this partially double compressed image and its re-compressed versions at different quality factor q ranging from 30 to 90 is shown in Figures 3.2 (b) to (h).

3.3 Double JPEG Compression Forensic Analysis

In this section, the research work is focused to detect/isolate the DJPG compressed region in an image automatically and estimation of the primary quantization matrix is performed. The estimation of first quantization matrix from the partial DJPG compressed images has significant importance in the forensic investigation. Thus, a two-stage scheme is proposed for the evaluation of primary quantization matrix from partial DJPG compressed images as shown in Figure 3.3. In

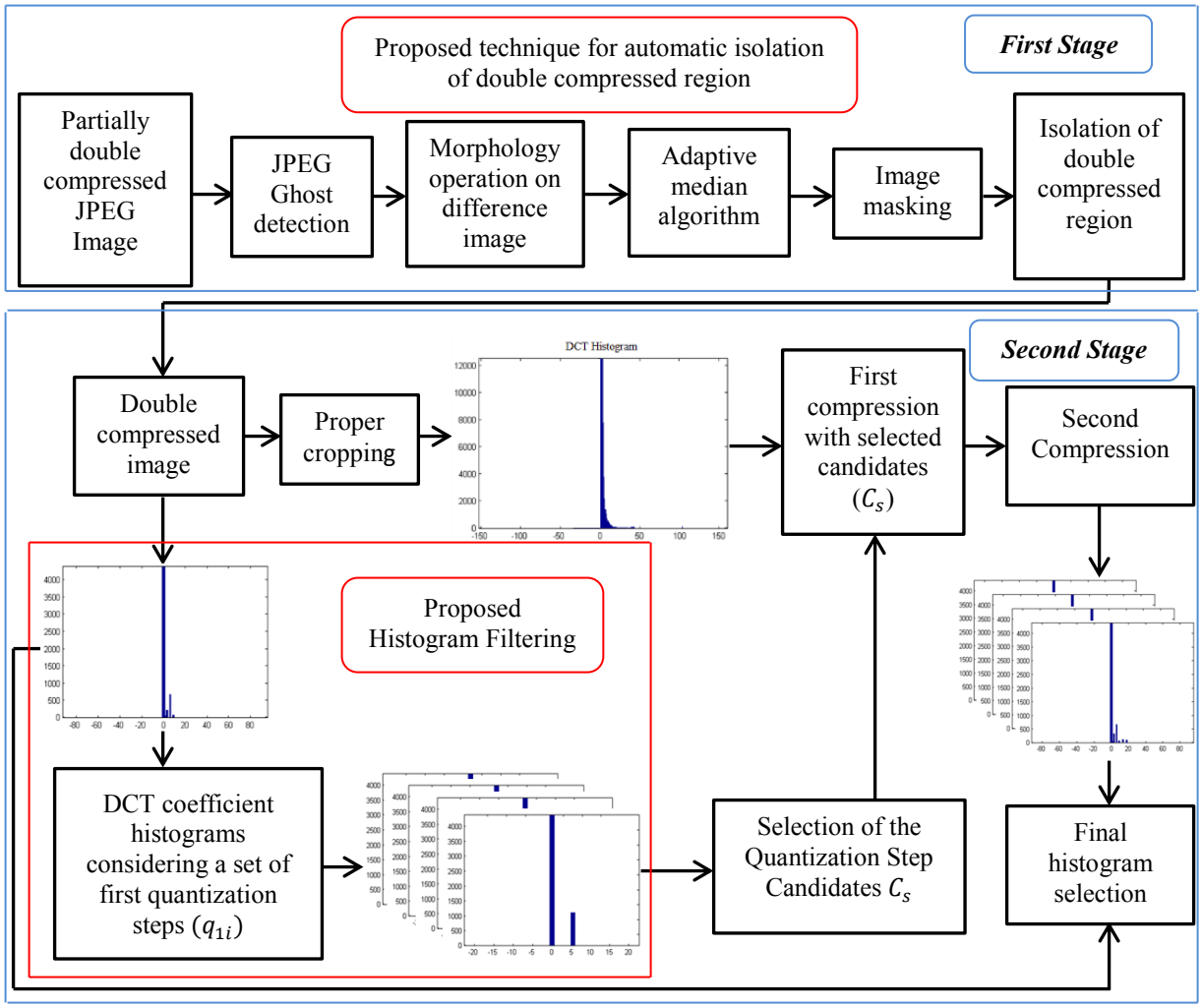
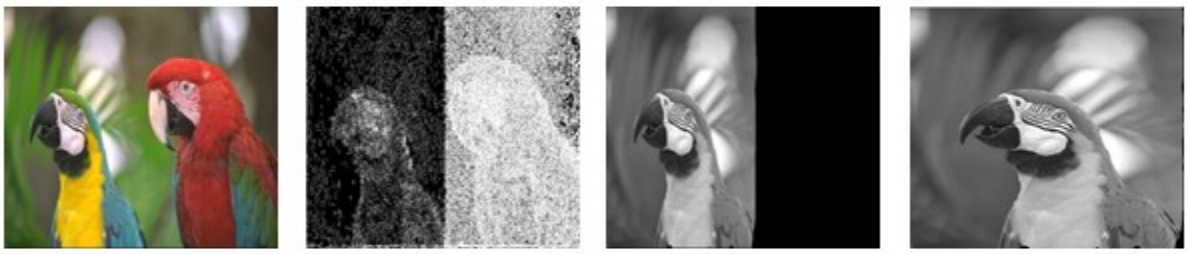


Figure 3.3: Proposed scheme for the detection and automatic isolation of double JPEG compressed region from an image and to estimate the first quantization matrix.

the first stage, a method is proposed for the automatic isolation of double compressed region from an image, and then this region is analyzed in second stage to determine the first quantization matrix. In the second stage, a filtering scheme is suggested to effectively reduce the effects of the error. The proposed scheme is applicable for the scenarios when the image is re-compressed with different quantization matrix than the first.

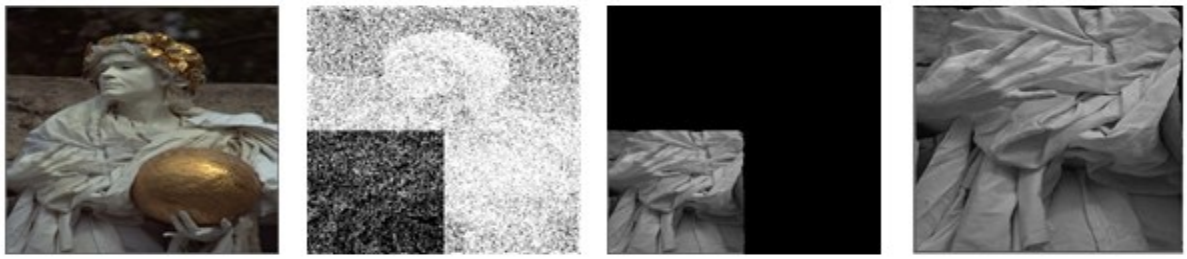
3.3.1 Automatic Isolation of Double Compressed Region from an Image

In the proposed technique, the first stage is based on the automatic isolation of double compressed region from an image by employing an enhanced JPEG Ghost detection technique. The conventional JPEG Ghost detection technique provides the gray scale difference image. The holes that occur in the gray scale difference image are then filled through morphology operation. Consequently, the adaptive median algorithm is applied after image complement which results in a binary image. The adaptive median algorithm classified the pixel values as noise by comparing each pixel value to its surrounding neighbors in the image. The pixel is considered as an impulse noise which is not structurally aligned with those pixels to which it is similar as well as which is different from a majority of its neighbors. These noise pixels are then replaced by the median pixel value of pixels in the neighborhood which have already passed the noise labeling test. The value of S_{max} (maximum allowed size of the neighborhood) is adjusted according to the intensity value of double compressed part in difference image to bring it in the reasonable range of $21 \leq S_{max} \leq 41$. The given doctored JPEG image is then masked with the binary image which provides the masked image. The desired part is then cropped from the masked image. The stepwise output of the first stage in the form of obtained images is depicted in Figures 3.4 to 3.7.



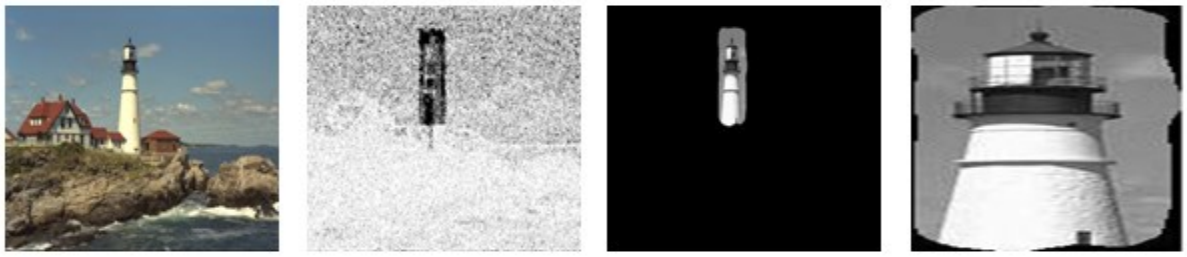
(a) (b) (c) (d)

Figure 3.4: (a) Partial double compressed Parrot image, (b) Difference image through JPEG ghost, (c) Image after morphology, adaptive filtering, and masking operation, (d) Isolated double compressed region of size 392×512 pixels.



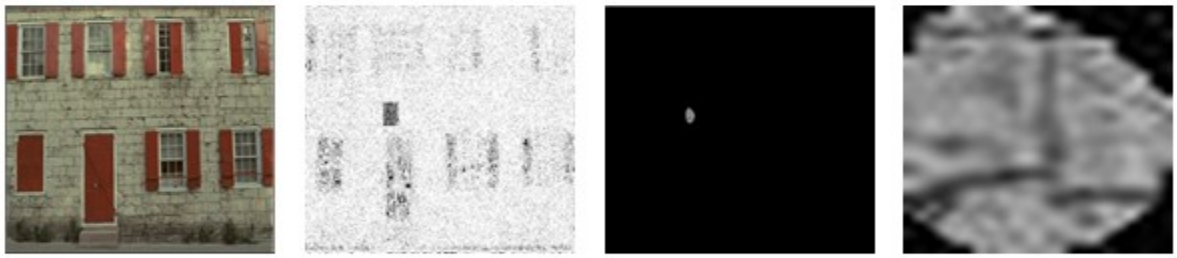
(a) (b) (c) (d)

Figure 3.5: (a) Partial double compressed Roman image, (b) Difference image through JPEG ghost, (c) Image after morphology, adaptive filtering, and masking operation, (d) Isolated double compressed region of size 260×385 pixels.



(a) (b) (c) (d)

Figure 3.6: (a) Partial double compressed Tower image, (b) Difference image through JPEG ghost, (c) Image after morphology, adaptive filtering, and masking operation, (d) Isolated double compressed region of size 82×205 pixels.



(a) (b) (c) (d)

Figure 3.7: (a) Partial double compressed Wall image, (b) Difference image through JPEG ghost, (c) Image after morphology, adaptive filtering, and masking operation, (d) Isolated double compressed region of size 23×30 pixels.

3.3.2 Estimation of First Quantization Matrix from the Double Compressed Region

The second stage analyzes the double compressed region to estimate the first quantization matrix as shown in Figure 3.3. The resultant image from the first stage is properly cropped in the second

stage and then the DCT coefficients of the image are extracted. The reason behind this cropping operation is that the extracted double compressed part would show some irregularities at the edges. These irregularities can be observed in Figures 3.4 (d), 3.5 (d), 3.6 (d) and 3.7 (d). These irregularities are present only at the edges and not at any other region. Thus, the error transferred to the second step can be minimized by proper cropping of the extracted double compressed part at the edges as shown in Figure 3.8. The merits of proper cropping have already been discussed in [121] such as improvement of visual composition and image quality by eliminating the irrelevant parts.

(a) (b)

Figure 3.8: (a) Resultant double compressed region from the first stage, (b) Image after proper cropping.

Now the estimation of the first quantization matrix is carried out through the analysis of DCT coefficient histogram. The DCT histogram is filtered out through the proposed filtering scheme to reduce the effects of error e in (3.1.1). This filtering provides a set of filtered histograms. The rounding error e is modeled by approximating it as Gaussian noise. This error proclaims itself by spreading peaks around the quantization step multiples. It will affect the second quantization step behavior along with the magnitude and statistics of the DCT coefficients. Due to this error, two type of noises *i.e.*, split and residual noise are encountered by the filtering strategy. The proposed histogram filtering scheme further reduces the effects of error e. Based on primary quantization steps in the range $q_{1i} \in \{q_{1min},\ q_{1min} + 1, \ldots, q_{1max}\}$, several filtering operations are then performed.

The properties of successive quantizations are exploited more efficiently by function (3.3.1) as compared to the error function (3.1.2). Therefore, by exploiting the q_1 localization property of (3.3.1), limited first quantization candidates (C_s) are selected. The improved error function d_{out}

becomes nearly zero in the case $q_3 = q_{1i}$ as shown in Figure 3.9, when the filtering is done with the right first quantization step by using the formulation as follows:

$$d_{out}(c', q_1, q_2, q_3) = \left| \left[\left[\left[\left[\frac{c'}{q_1} \right] \frac{q_1}{q_2} \right] \frac{q_2}{q_3} \right] \frac{q_3}{q_2} \right] q_2 - \left[\left[\frac{c'}{q_1} \right] \frac{q_1}{q_2} \right] q_2 \right| \tag{3.3.1}$$

Each d_{out} is evaluated for $q_3 = q_{1i}$ by considering a single DCT frequency. If this value approaches to zero, it is included to the limited candidates set C_s otherwise, discarded.

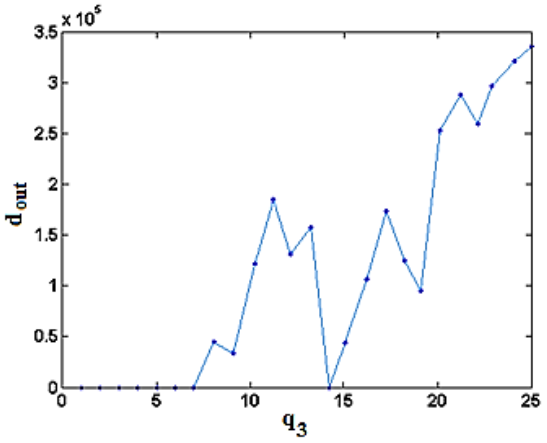


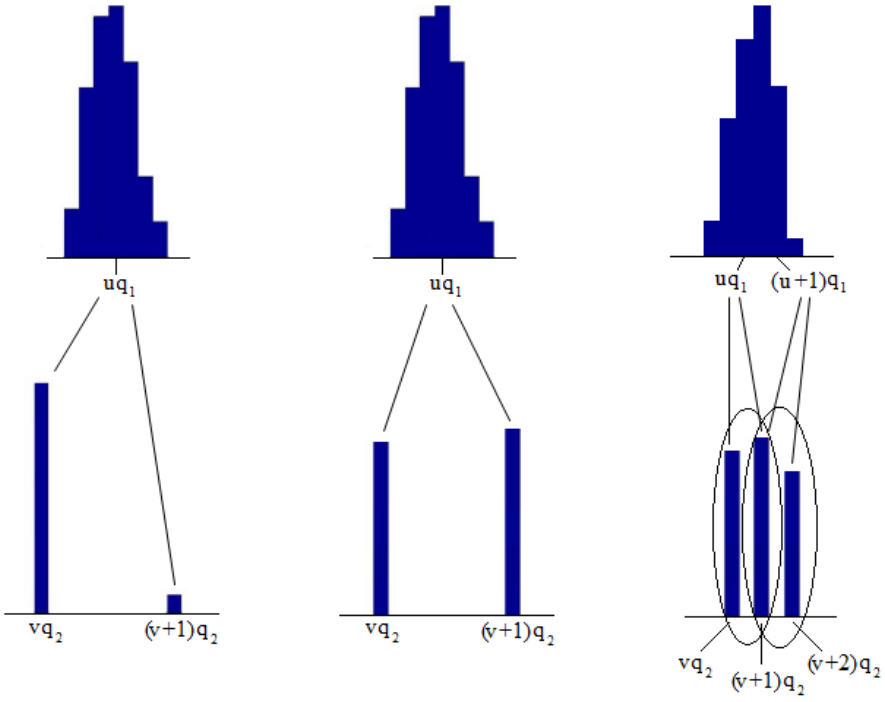
Figure 3.9: Error function (3.3.1) for a AC coefficient with $q_1 = 14$, $q_2 = 7$ and $q_3 \in \{1, 2, \ldots, 25\}$.

The double quantization process is simulated by considering the selected candidates. In this process, the first compression is performed by using selected candidates C_s and the second compression with known quantization step and finally a histogram is selected that best exploits the original histogram. Therefore, the desired first quantization step is selected which corresponds to the final selected histogram from a pool of selected candidates C_s.

3.3.2.1 DCT Histogram Filtering

Numerous methodologies [32, 34, 52, 76] generally do not consider the error e in (3.1.1) while employing the impacts of consecutive quantizations that take place after the de-quantizations. The performance of these methodologies reduces significantly when this source of error is neglected. But this simplification permits to handle the included mathematical equations easily.

This error is introduced during the operations like color space conversions, rounding, and truncation of the values [34]. Based on the actual implementation, to examine each source of error separately is a challenging task. Therefore, the Gaussian distribution is used to model the overall effect of this error [34].



(a) (b) (c)

Figure 3.10: (a) Residual noise, (b) Split noise and (c) Proposed split noise scenario.

Several situations can arise due to the magnitude of primary and secondary quantization steps, when an image is compressed more than once. In the first case, wrong bin DCT coefficient elements are propagated in the resultant histogram when a small perturbation occurs as shown in Figure 3.10 (a). In the second scenario, the bin containing original information in the histogram is divided equally into two adjoining bins and out of these two bins, one is a wrong bin, as shown in Figure 3.10 (b). This undesired situation arises when a primary quantization bin in position uq_1 falls exactly halfway between two back to back bins in position vq_2 and $(v+1)q_2$ coming from the second quantization related as follows:

$$uq_1 = \frac{vq_2 + (v+1)q_2}{2}, \quad u, v \in N^+ \tag{3.3.2}$$

At this point, an issue arises which has not been discussed previously, in which the bin from the second quantization $(v+1)q_2$ becomes common to the two different cases of split noise, as shown in Figure 3.10 (c). The bin in position uq_1 of primary quantization is positioned precisely in the middle of two back to back bins in position vq_2 and $(v+1)q_2$ acquired from second quantization. Similarly, the bin in position $(u+1)q_1$ is positioned absolutely in the middle of two bins attained from second quantization in the positions $(v+1)q_2$ and $(v+2)q_2$. Thus, to cope with this problem a filtering algorithm has been proposed. The proposed algorithm first finds out the wrong bins in the double quantized histogram with the help of (3.3.2) by considering the particular values of quantization steps q_1 and q_2. The identified wrong bins are then moved to the right locations according to the proposed algorithm as shown in Figure 3.11 (b). On the other hand, the residual noise is removed by setting the proper threshold as shown in Figure 3.11 (c).

Filtering algorithm for the proposed split noise scenario

Parameters:

N_{bins} : Number of bins in DCT coefficients input histogram

bin_2: Bin height of the double compressed input histogram

uq_1: Bin centre position of single compressed histogram

vq_2: Bin centre position of double compressed histogram

begin

for $k = 1: N_{bins}$ **do**

$find(uq_1(k) == [vq_2(k) + (v+1)q_2(k)]/2)$ % Applying equation (3.3.2)

if $bin_2(vq_2(k)) < bin_2((v+1)q_2(k))$ **then**

$bin_2((v+1)q_2(k)) = bin_2(vq_2(k)) + bin_2((v+1)q_2(k))$

$bin_2(vq_2(k)) = 0$

else

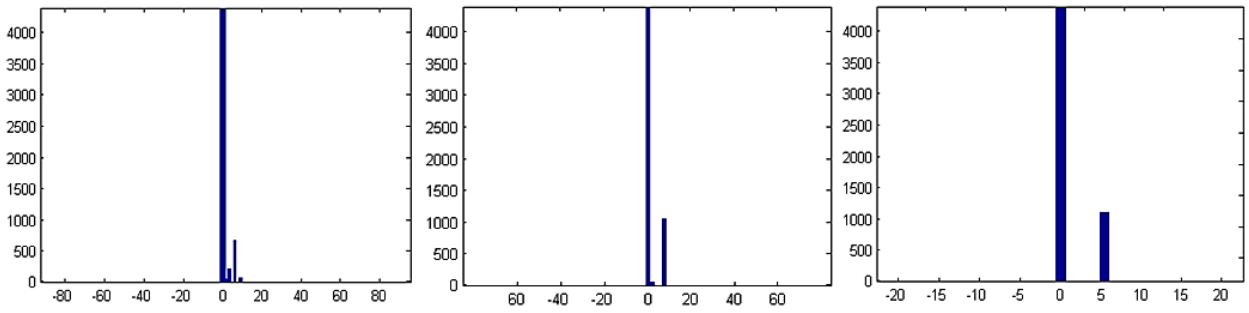
$bin_2(vq_2(k)) = bin_2(vq_2(k)) + bin_2((v+1)q_2(k))$

$bin_2((v+1)q_2(k)) = 0$

end

end

end



(a) (b) (c)

Figure 3.11: (a) Double quantized DCT histogram, DCT histogram (b) after split noise removal and (c) after residual noise removal.

3.4 Experiment Results

In this section, the efficacy of the proposed approach is examined by conducting several tests on different datasets images. The JPEG encoding is used with standard JPEG quantization matrices recommended by Independent JPEG Group (IJG) [122]. The database is generated by considering the Kodak lossless true color image (PhotoCD PCD0992) dataset [123] and UCID dataset [117] images. A set of 560 partial double compressed images is obtained from both the datasets considering the quality factors (QF_1, QF_2) in the range 50 to 100. The supporting idea for the arrangement of images is to consider an uncompressed JPEG image and to double compress the regions by considering the image replacement rate from 0.05 to 1. Instead of the particular quantization steps, the outputs are described in accordance with the quality factors. The study of results is simplified by this step because a quantization matrix comprising of 64 quantization steps is represented by a single quality factor. Generally, these 64 quantization steps are of different values for different frequencies as shown in Figure 3.12. Since most of the information is carried by the lower frequency DCT coefficients, therefore the experimental analysis is based on the first 15 components [34]. The proposed partial double compression detection technique does not provide satisfactory results for the images in which recompression is performed with a cropping attack and the same quantization matrix. Since, after the cropping attack, if the image is re-compressed with same quantization matrix, it will lead to the desynchronization of DCT blocks [124 - 125]. The main problem is then to evaluate the desynchronization of DCT blocks introduced into the image. The proposed detection scheme is unable to detect this desynchronization. Thus, the case of recompression with same quantization matrix is not considered in this work.

$$QF_{50} = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Figure 3.12: Quantization matrix for quality factor 50 according to the JPEG standard.

3.4.1 Performance Analysis of the Proposed Scheme

The performance analysis of first stage of the proposed technique has been done by considering the different detection parameters on two different datasets. The blocking artifacts introduced in double compressed regions are computed using different detection parameters as shown in Tables 3.1 and 3.2. It is clear from Tables 3.1 and 3.2 that the values of blockiness signature measure (K_F) [63], gradient aware blockiness measure (B_{gr}^{p}) [126], and the calibrated feature (K_L) [98], vary according to the present artifacts and the size of the double compressed region. The discussed detection parameters measure the smoothness of the image, whereas for smooth images their values approach to zero. Therefore, these parameters also confirm that the isolated region is actually double compressed. These blocking artifacts detection parameters measure the effectiveness of the first stage in automatic isolation of double compressed region. The Tables 3.1 and 3.2 also shows the average values of various detection parameters by considering a set of 560 images build from the Kodak lossless true color image (PhotoCD PCD0992 dataset) as well as the UCID dataset. Therefore, the average values of various detection parameters further confirm the efficacy of first stage.

Table-3.1: Different detection parameters obtained by the first stage of proposed scheme by considering the Kodak lossless true color image dataset.

Uncompressed Images	Double compressed region size	K_F [63]	B_{gr}^{p} [126]	K_L [98]
Parrot (768×512)	392×512 pixels	0.862	4.731	1.899
Roman (512×768)	260×385 pixels	0.486	3.773	0.356
Tower (768×512)	82×205 pixels	0.387	9.424	0.393
Wall (768×512)	23×30 pixels	1.428	4.003	1.319
Average values of detection parameters on the 560 images built from Kodak dataset		0.976	6.574	2.984

Table-3.2: Different detection parameters obtained by the first stage of proposed scheme by considering the UCID dataset.

Uncompressed Images	Double compressed region size	K_F [63]	B_{gr}^{p} [126]	K_L [98]
Booth (384×512)	392×512 pixels	0.735	5.132	1.456
Car (512×384)	260×385 pixels	0.512	2.976	0.438
Flower (384×512)	82×205 pixels	0.262	8.313	0.381
Trophy (384×512)	23×30 pixels	1.107	4.747	1.421
Average values of detection parameters on the 560 images built from UCID dataset		0.814	5.921	2.138

The percentage error of the first stage due to the edge irregularities of the isolated part increases with the reduction in the double compressed region size. The percentage error in isolation of double compressed region on the two different datasets *i.e.*, Kodak lossless true color image (PhotoCD PCD0992) and UCID dataset is shown in Figure 3.13. It is clear from the Figure 3.13 that the error is larger in the case of UCID dataset due to their small image size which leads to the processing of fewer blocks as compared to the Kodak lossless true color image dataset.

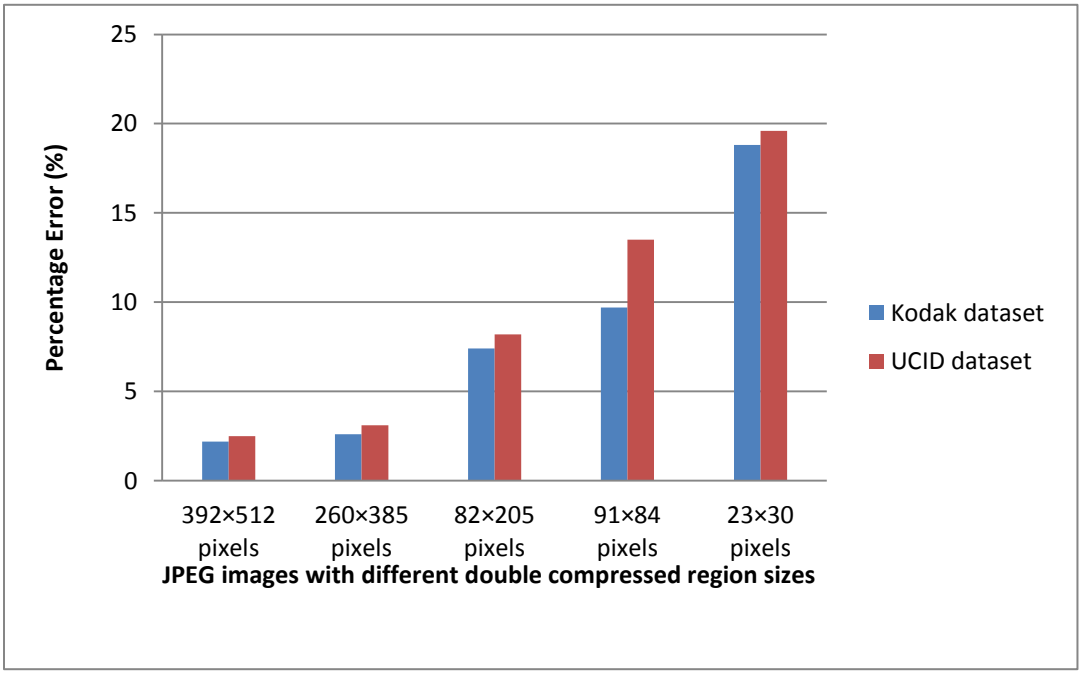


Figure 3.13: Percentage error (%) in the automatic isolation of the double compressed region through the first stage by considering Kodak lossless true color image (PhotoCD PCD0992) and UCID datasets.

The adaptive median algorithm is applied to the difference image generated from the JPEG ghost technique in which the boundary irregularities in the resultant binary image can be observed. The error due to the edge irregularities changes as the function of different JPEG compression factors. Tables 3.3 and 3.4 report the average percentage of error in the first stage as a function of various JPEG compression factors on the Kodak lossless true color image (PhotoCD PCD0992 dataset) and UCID dataset respectively. It can be seen from Tables 3.3 and 3.4 that the accuracy decreases in the case of UCID dataset as compared to the Kodak lossless true color image dataset due to their small image sizes.

Table-3.3: Average percentage of error in the first stage as a function of various JPEG compression factors on the Kodak lossless true color image dataset.

$QF_2 \backslash QF_1$	50	60	70	80	90
50	–	7.455	15.395	11.555	69.780
60	10.875	–	7.564	34.895	34.988
70	13.321	8.766	–	12.044	55.875
80	2.739	12.306	4.775	–	9.125
90	5.775	1.885	3.431	9.705	–

Table-3.4: Average percentage of error in the first stage as a function of various JPEG compression factors on the UCID dataset.

$QF_2 \backslash QF_1$	60	70	80	90	100
50	–	9.775	17.635	12.550	71.703
60	12.766	–	8.414	36.750	36.999
70	14.975	10.650	–	13.120	57.845
80	3.886	14.285	5.745	–	11.535
90	8.746	4.250	6.455	12.548	–

3.4.2 Comparative Analysis with Existing Techniques

In this subsection, the comparative analysis of the proposed scheme is done with the existing techniques to authenticate the competency of the presented scheme. Tables 3.5 and 3.6 report the average percentage error of the second stage by considering 560 partial double compressed images created from Kodak lossless true color image (PhotoCD PCD0992 dataset) as well as the UCID dataset. The percentage of error is calculated by estimating the q_1 values at different quality factor values. Since the analysis is performed on the partial double compressed image

datasets, therefore the isolated double compressed region is processed in the second stage to estimate the first quantization matrix whereas in the existing state-of-the-art techniques full double compressed images are used [32 - 34, 85, 87]. The DCT coefficients that correspond to low frequencies results in small estimation error and do not essentially rely on particular quality factor concerned with primary and secondary quantization. On the other hand, the estimation error for higher frequencies has significant correlation with quality factors. It is noticed that the higher values of QF_1 and QF_2 provide better results in comparison to lower quantization. The comparative analysis of Tables 3.5 and 3.6 depicts that the percentage error in estimating the q_1 values corresponding to first 15 DCT coefficients at different quality factors is more for UCID dataset as compared to the Kodak lossless true color image dataset due to the small size of images in UCID dataset.

Table-3.5: Performance of proposed scheme in terms of average percentage error in the estimation of q_1 values at different quality factors corresponding to the first 15 DCT coefficients on Kodak lossless true color image dataset.

$QF_1 \backslash QF_2$	60	70	80	90	100
50	10.352	9.205	3.759	4.675	2.503
60	–	14.263	8.445	5.537	2.149
70	–	–	5.597	4.433	1.200
80	–	–	–	3.250	0.950
90	–	–	–	–	0.255

Table-3.6: Performance of proposed scheme in terms of average percentage error in the estimation of q_1 values at different quality factors corresponding to the first 15 DCT coefficients on UCID dataset.

$QF_1 \backslash QF_2$	60	70	80	90	100
50	11.251	10.523	4.940	7.125	3.340
60	–	16.221	9.246	5.565	2.458
70	–	–	7.252	4.986	1.467
80	–	–	–	4.745	1.126
90	–	–	–	–	0.356

In order to study the effectiveness of the proposed approach, further analysis is performed with respect to the specific DCT coefficient. Tables 3.7 and 3.8 show the average percentage of error in the estimation of q_1 values that corresponds to the DCT coefficients on two different

datasets. For the DCT coefficients corresponding to the high frequencies, the performance of the proposed scheme degrades but it provides high accuracy with an error less than 1.5% for the first 10 DCT coefficients as shown in Table 3.7.

A comparative analysis of this second stage of proposed scheme is done with the various algorithms proposed in [32, 34, 85, 87]. The application of the second stage of the proposed scheme, when first 9 DCT coefficients are considered in a zig-zag manner, mixed results are obtained with few coefficients providing high error values. However, after the 9^{th} DCT coefficient, the percentage error recorded is much low from the previously established techniques as shown in Table 3.7. If Table 3.7 is closely examined, the percentage error can be conveniently justified. It can be inferred that the proposed scheme outperforms the method proposed by Bianchi [87] for all the considered 15 DCT coefficients. Whereas, the proposed scheme lags behind the schemes provided by Galvan [34] and Lukas [85] in only one DCT coefficient. Farid [32] surpass the proposed scheme for only two DCT coefficients.

Table-3.7: Average percentage of error in estimated q_1 values corresponding to the DCT coefficient in zig-zag order considering several state-of-the-art approaches on the Kodak lossless true color image dataset.

Techniques / DCT coefficient	Lukas [85]	Farid [32]	Bianchi [87]	Galvan [34]	Proposed Scheme
1	0.41	0.25	0.31	0.14	**0.11**
2	0.42	**0.21**	0.82	0.92	0.82
3	0.53	**0.22**	1.09	0.95	0.93
4	5.81	2.52	4.21	1.57	**1.42**
5	3.77	1.83	2.33	0.84	**0.81**
6	**1.26**	1.80	13.82	1.36	1.38
7	8.00	12.91	5.97	2.51	**1.41**
8	6.21	5.82	6.12	0.86	**0.80**
9	4.01	6.01	8.23	**0.83**	1.07
10	8.52	6.10	6.22	1.22	**1.13**
11	7.33	20.06	11.08	8.57	**5.01**
12	10.28	18.23	12.16	8.02	**6.02**
13	12.02	18.07	7.02	4.02	**4.00**
14	14.01	16.12	10.08	7.05	**5.02**
15	24.42	29.23	16.20	13.01	**12.01**

The proposed filtering step considerably improves the performance of the second stage that copes up with rounding and truncation error efficiently. Tables 3.7 and 3.8 show that the proposed scheme provides less percentage error as compared to the other considered methods in estimating the q_1 values corresponding to DCT coefficient in zig-zag order on both datasets. It is clear from Table 3.8 that the proposed scheme outperforms the existing techniques proposed by Farid [32], Lukas [85] and Bianchi [87] for all the considered 15 DCT coefficients. The technique provided by the Galvan [34] outperforms the proposed scheme for only two DCT coefficients.

The considered methods provide better results on Kodak lossless true color image dataset as shown in Table 3.7 as compared to the UCID dataset as shown in Table 3.8. The efficiency of considered schemes varies in accordance with the image resolution. The analysis is less reliable because of small sized images in UCID dataset as shown in Table 3.8. Nevertheless, in today's scenario working with small images is not so common.

Table-3.8: Average percentage of error in estimated q_1 values corresponding to the DCT coefficient in zig-zag order considering several state-of-the-art approaches on the UCID dataset.

Techniques / DCT coefficient	Lukas [85]	Farid [32]	Bianchi [87]	Galvan [34]	Proposed Scheme
1	4.71	5.27	5.05	3.52	**3.49**
2	2.82	2.45	4.37	**1.81**	2.01
3	3.01	2.66	5.80	2.07	**1.80**
4	3.83	2.89	10.08	3.02	**2.07**
5	3.57	2.62	7.81	2.01	**1.82**
6	3.42	4.23	16.06	3.88	**3.06**
7	5.52	7.07	8.07	5.07	**4.63**
8	8.51	4.28	13.80	4.92	**3.04**
9	4.03	4.07	11.81	**3.96**	6.05
10	6.80	5.06	12.23	5.07	**5.03**
11	15.02	8.07	8.07	10.91	**8.02**
12	7.03	7.81	12.06	5.20	**4.01**
13	8.04	10.67	8.01	**7.91**	10.02
14	13.02	10.25	13.50	8.23	**7.04**
15	20.01	19.83	12.02	14.50	**11.43**

3.5 Summary

In this chapter, a two-stage forensic technique is recommended to detect and analyze the double compressed region in an image. In the first stage, the JPEG ghost detection scheme is further expanded to make it capable of isolating the double compressed region automatically. Afterward, the isolated region is examined to estimate the first quantization matrix. It is confirmed from the experimental results that the first stage of the proposed scheme provides an average percentage accuracy of 95.45%. Moreover, the proposed filtering strategy in the second stage results in a minimum error which is less than 1.5% for the first 10 DCT coefficients for Kodak lossless dataset, which is not the case with the existing state-of-the-art techniques as revealed in Table 3.7. Based on the forensic analysis of JPEG compression performed in this chapter, the further work is devoted to design an anti-forensic technique for JPEG compression (*i.e.*, both for single and double) in the next chapter.

CHAPTER 4

JPEG COMPRESSION ANTI-FORENSICS

This chapter presents a four-step anti-forensic framework based on the forensic analysis performed in the last chapter by considering JPEG artifacts both in DCT as well in spatial domain to disguise the existing forensic detectors. All the existing anti-forensic techniques degrade the processed image quality. The presented anti-forensic schemes provide high image quality with better forensic undetectability. Two denoising algorithms are employed in the proposed framework to achieve high image quality. The robustness of the proposed scheme is verified by its undetectability with high visual quality of an image against various forensic detection attacks [38, 44, 63, 97 - 98] in both spatial and DCT domains. The capability of recommended schemes is also evaluated by using machine learning based detectors [28, 99]. Furthermore, the DJPG compression detectors proposed in [36, 75, 87] are also considered to analyze the efficacy of the proposed anti-forensic approaches based on JPEG compression. The experimental results validate the competency of presented JPEG anti-forensic techniques. The suggested methods attain good forensic undetectability by concealing single as well as DJPG compression artifacts, with improved processed image quality.

4.1 Improved JPEG Anti-Forensic Technique

The JPEG anti-forensic scheme suggested in [39] provides better image visual quality and forensic undetectability. Based on the analysis of this anti-forensic technique, a new JPEG anti-forensic technique is presented in this section to achieve a good tradeoff between image quality and forensic undetectability. The proposed scheme comprises of four stages which include perceptual DCT histogram smoothing, proposed denoising operation, improved TV-based deblocking, and decalibration operation, as shown in Figure 4.1. Also, two types of denoising algorithms based on constrained minimization problem of TV of energy and normalized weighted function are presented to reduce the grainy noise added by perceptual histogram smoothing. The blocking artifacts left after the JPEG compression in spatial domain are removed

by utilizing a new TV-based deblocking operation based on the combined effect of TV of energy in horizontal, vertical and diagonal directions.

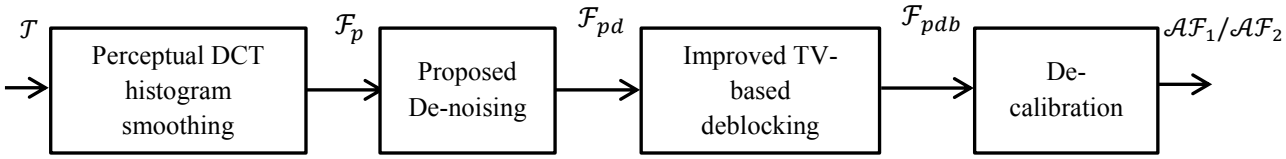


Figure 4.1: Proposed JPEG anti-forensic technique.

4.1.1 Perceptual DCT Histogram Smoothing

In the proposed anti-forensic framework, initially the JPEG compressed image is processed by using the perceptual histogram smoothing (adaptive dithering operation) of [39] in order to remove the periodic artifacts present in the comb-like histogram of DCT coefficients of each sub-band. Laplacian and uniform distributions are considered to generate an adaptive local dithering signal model in this process to achieve an improved goodness-of-fit. Let X be a given image and $(D_{matrix}X)_{r,c}^{l}$ represents the DCT coefficient value of (r,c)-th sub-band of l-th 8×8 block of a matrix. In this operation, the dithering signal N is added to the quantized DCT coefficient which results in dithered coefficient $(D = Z + N)$ in order to eliminate the gaps present in the DCT coefficients histogram. It is an important task to estimate the proper distribution of dithering signal N. The model of dithering signal is generated by processing one quantization bin through another, starting from quantization bin $b = 0$. The constrained fitting problem based on weighted least-squares is solved for the parameter γ_b of Laplacian distribution for a quantization bin b as [39]:

$$\gamma_b = \underset{\gamma_b^- \le \gamma \le \gamma_b^+}{\arg min} \sum_{k=B_{r,c}^- q_{r,c} - \left\lfloor \frac{q_{r,c}}{2} \right\rfloor}^{B_{r,c}^+ q_{r,c} + \left\lfloor \frac{q_{r,c}}{2} \right\rfloor} w_k \times \left(H_{r,c}^X(k) - P(Z = k) \right)^2 \tag{4.1.1}$$

where, $B_{r,c}^+ = max\left(\left(q_{block}(D_{matrix}X)\right)_{r,c}^{l}\right)$ and $B_{r,c}^- = min\left(\left(q_{block}(D_{matrix}X)\right)_{r,c}^{l}\right)$ represent the non-empty quantization bins with largest and smallest bin center values respectively. The operator $q_{block}(.)$ represents the block DCT coefficient quantization and $H_{r,c}^X(k)$ represents the normalized DCT histogram as follows:

$$H_{r,c}^{X}(k) = \frac{1}{L}\sum_{l=1}^{L} \delta\left(round\left((D_{matrix}X)_{r,c}^{l}\right) - k\right), k \in \mathbb{Z} \tag{4.1.2}$$

Here, $\delta(x) = 1$ if the value of $x = 0$, otherwise $\delta(x) = 0$. To realize the parameter γ_b, weight can be modeled as:

$$w_k = \left(\left|round\left(\frac{k}{q_{r,c}}\right) - b\right| + 1\right)^{-1} \tag{4.1.3}$$

Besides, γ_b^- denotes lower bound and γ_b^+ represents upper bound of factor γ in (4.1.1). The fitting problem can be initiated and γ_b is estimated by solving (4.1.1), if $\gamma_b^-$and γ_b^+ are well defined. Otherwise, γ_b cannot be found and the fitting problem cannot be established. If γ_b can be found by solving the fitting problem in (4.1.1) for the quantization bin b then the Laplacian model is used by following the model of [95]. The distribution of the dithering signal N is given as:

$$P(N = n|Z = 0) = \begin{cases} c_0 e^{-\gamma|n|} & if\ \frac{-q_{r,c}}{2} < n < \frac{q_{r,c}}{2} \\ 0 & otherwise \end{cases} \tag{4.1.4}$$

$$P(N = n|Z = z, z > 0) = \begin{cases} c_1 e^{-\gamma n} & if\ \frac{-q_{r,c}}{2} \leq n < \frac{q_{r,c}}{2} \\ 0 & otherwise \end{cases} \tag{4.1.5}$$

$$P(N = n|Z = z, z < 0) = \begin{cases} c_1 e^{\gamma n} & if\ \frac{-q_{r,c}}{2} < n \leq \frac{q_{r,c}}{2} \\ 0 & otherwise \end{cases} \tag{4.1.6}$$

where, $c_0 = \frac{\gamma}{2}\left(1 - e^{-\gamma q_{r,c}/2}\right)^{-1}$ and $c_1 = \gamma e^{-\gamma q_{r,c}/2}(1 - e^{-\gamma q_{r,c}})^{-1}$. Let P_m^o and P_m^e (function of γ) are the probability mass function (p.m.f.) for odd and even $q_{r,c}$ values respectively for the rounded dithering signal. The p.m.f. is used for searching γ_b^- and γ_b^+ of (4.1.1). When γ_b cannot be found, the uniform model is used to generate the dithering signal N as follows:

$$P(N = n|Z = z) = \begin{cases} \frac{1}{q_{r,c}} & if\ n \in \mathcal{N} \\ 0 & otherwise \end{cases} \tag{4.1.7}$$

where, $\mathcal{N} = \left(-\frac{q_{r,c}}{2}, \frac{q_{r,c}}{2}\right)$ when $z = 0, \mathcal{N} = [-\frac{q_{r,c}}{2}, \frac{q_{r,c}}{2})$ when $z > 0$, and $\mathcal{N} = (-\frac{q_{r,c}}{2}, \frac{q_{r,c}}{2}]$ when $z < 0$.

The searching of the bounds γ_b^- and γ_b^+ used in (4.1.1) is performed by considering the center (*i.e.*, quantization bin $b = 0$) of the DCT coefficients histogram as a starting bin. For the natural images, the value of the parameter γ of Laplacian model frequently lies in the range from 10^{-3} to 1. Therefore, the value of γ_b^- is set to 10^{-3}. This searching process is restricted on the basis of fact that with an increase in the magnitude of coefficient, there is a decrease in probability in the DCT coefficients distribution. For instance, when $q_{r,c}$ is an odd number, it is constrained that the probability of the DCT coefficient falling in the leftmost integer bin $-\left\lfloor\frac{q_{r,c}}{2}\right\rfloor$ (or rightmost integer bin $\left\lfloor\frac{q_{r,c}}{2}\right\rfloor$) of quantization bin $b = 0$ must be no smaller than either that in the rightmost integer bin of the quantization bin $b = -1$ or that in the leftmost integer bin of the quantization bin $b = 1$. It is expected that the DCT coefficients follow a uniform distribution in the neighboring quantization bins -1 and 1. Then the following equation is solved to determine the parameter γ_b^+ [39].

$$\gamma_b^+ = \underset{10^{-3} \le \gamma \le 1}{\arg max}\, \gamma\,, subject\ to: P_m^o\left(N = \left\lfloor\frac{q_{r,c}}{2}\right\rfloor | Z = 0\right) \times M_0 \ge max\left(\frac{M_{-1}}{q_{r,c}}, \frac{M_1}{q_{r,c}}\right) \quad (4.1.8)$$

where, M_0, M_{-1}, and M_1 represent the probability approximation of DCT coefficient that fall in quantization bins $0, -1, 1$ respectively. The γ_b^+ is chosen as the largest number satisfying constraints in (4.1.8). Almost similar procedure is followed to find the value of γ_b^+, when $q_{r,c}$ is an even number.

4.1.2 Denoising Algorithms

In this section, two different types of denoising algorithms are employed as the second step of the recommended JPEG anti-forensic framework to remove the grainy noise added by the perceptual histogram smoothing. The complete explanation of these denoising algorithms is provided in the succeeding subsections.

4.1.2.1 Image Denoising based on TV-based Energy Minimization Problem

The resultant dithered image of perceptual histogram smoothing contains a significant amount of grainy or unnatural noise, thus reducing the image visual quality. Actually, this grainy noise is introduced during the dithering operation of JPEG anti-forensic techniques. Most of the dithering operations are not able to properly eliminate the gaps of comb-like histogram of DCT coefficients without adding any unnatural noise. Therefore, a denoising algorithm is suggested based on the TV [127 - 128] to obtain good visual quality of an image. Consider the noisy dithered image obtained from the perceptual histogram operation $F: \Omega \to V$ of size $T \times T'$, where Ω is bounded open subset of V^2, and U denotes the resultant denoised image. It is desired to solve the following constrained minimization problem based on the TV of energy [129]:

$$U^* = \arg\min_{U} \sum_{i,j} \left\{ \left| U_{i,j} \right| + \lambda \left\| F_{i,j} - U_{i,j} \right\|^2 \right\} \tag{4.1.9}$$

where, $\left| U_{i,j} \right|$ denotes the bounded variation semi-norm, where $i = 1, 2, 3, \ldots, T$ and $j = 1, 2, 3, \ldots, T'$, and λ represents the adjusting parameter between the two energy terms. The scaling factor λ determines the denoising level. If the value of λ is large, the denoising is minimum, whereas, small values of λ provide maximum denoising. However, the small λ value degrades the image quality. Therefore, to achieve better visual quality of an image, the value of λ is set at 0.8 [130]. Moreover, the analysis of forensic undetectability and image quality based on the various values of λ is provided in Section 4.4. The term $\left\| F_{i,j} - U_{i,j} \right\|^2$ represents the estimated variance of the unnatural noise added during the perceptual histogram smoothing. By considering $\left| U_{i,j} \right| = K(U_{i,j})$ and $\lambda \left\| F_{i,j} - U_{i,j} \right\|^2 = J(F_{i,j}, U_{i,j})$, (4.1.9) becomes:

$$U^* = \arg\min_{U} \sum_{i,j} \left\{ K(U_{i,j}) + J(F_{i,j}, U_{i,j}) \right\} \tag{4.1.10}$$

where, $K(U_{i,j})$ represents the positive convex regularization function and $J(F_{i,j}, U_{i,j})$ is a positive convex fitting function of $U_{i,j}$ for certain value of $F_{i,j}$. This convex nature of $U_{i,j}$ is responsible for the existence of a minimizer U^*. The sub differential of the term $(K(U_{i,j}) + J(F_{i,j}, U_{i,j}))$ which is the combination of two convex functions is zero at U^*, expressed as [130]:

$$\partial_{U_{i,j}} K(U^*) + \partial_{U_{i,j}} J(U^*, F_{i,j}) = 0 \tag{4.1.11}$$

The sub differential of the function $J(F_{i,j}, U_{i,j})$ is given as:

$$\partial_{U_{i,j}} J(U_{i,j}, F_{i,j}) = 2\lambda(U_{i,j} - F_{i,j}) \tag{4.1.12}$$

Also, the sub differential of the convex function $K(U_{i,j})$ can be written in the form as [129]:

$$\partial_{U_{i,j}} K(U_{i,j}) = -div\left(\frac{\nabla U_{i,j}}{|\nabla U_{i,j}|}\right) \tag{4.1.13}$$

where, div denotes the divergence function and (4.1.11) can be written in the form of Euler-Lagrange differential equation as [129]:

$$-div(\nabla U_{i,j}/|\nabla U_{i,j}|) + 2\lambda(U_{i,j} - F_{i,j}) = 0 \tag{4.1.14}$$

Thus, (4.1.14) can be re-written as:

$$U = \sum_{i,j}\left\{F_{i,j} + \frac{div(\nabla U_{i,j}/|\nabla U_{i,j}|)}{2\lambda}\right\} \tag{4.1.15}$$

Hence by solving the constrained minimization problem based on the TV of energy, the unnatural noise left during the perceptual DCT histogram smoothing is removed to a great extent.

4.1.2.2 Image Denoising based on the Normalized Weighted Function

To reduce the grainy noise efficiently from the adaptive dithered image, another denoising algorithm is presented exploiting the concept of self-similarity in natural images. It was initially recommended in [131] that every pixel in an image can be represented as the linear combination of all other pixels, but due to the computational complexity, all the pixels are not considered. Let the noisy dithered image is represented as $F = \{F(i)|i \in I\}$. Then the estimated value of each pixel i can be computed as the weighted average of all the pixels in the image as follows [132]:

$$U[F](i) = \sum_{j \in I} W(i,j)F(j) \tag{4.1.16}$$

The weight function $W(i,j)$ depends upon the similarity between the two pixels i and j. The neighboring pixels similar to the pixel under evaluation are allocated with larger weight and the different neighborhood pixels are allocated with small weights.

The function $f_2(x)$ is the estimated function based on the data observations generated for the original function $f_1(x)$. The estimation can be performed by considering a window and the weighted sum of all the pixels falling inside the window will contribute to the value of pixel under process. The estimation of function value $f_2(x_0)$ at point x_0 can be performed by taking the average of all the pixels inside the considered window as shown in orange color.

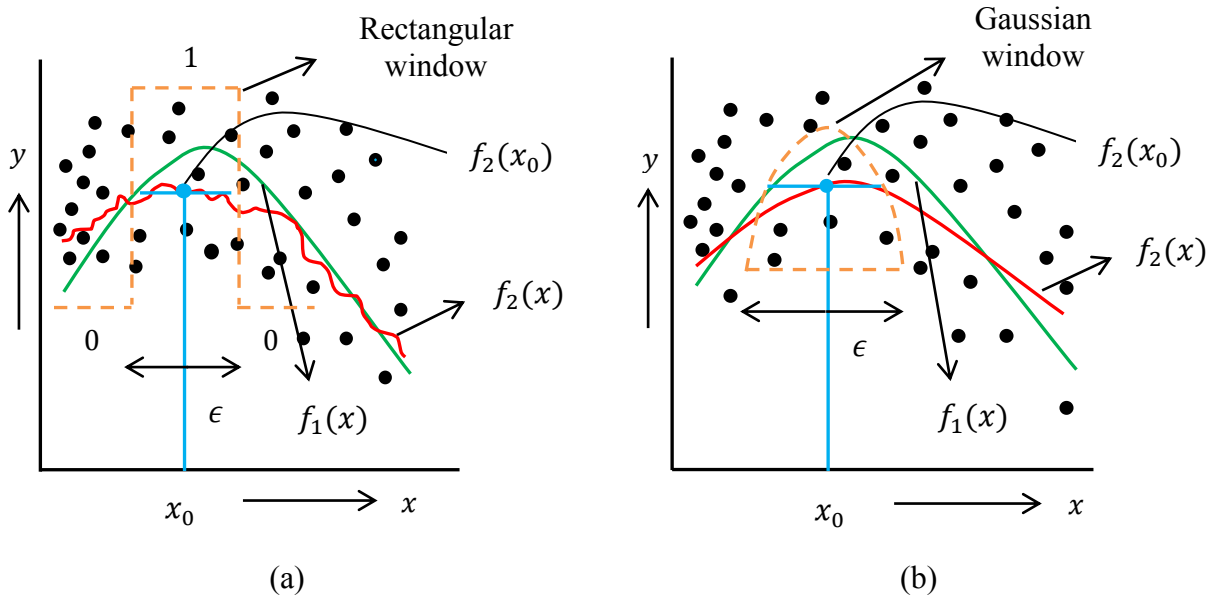


Figure 4.2: Estimation of function value $f_2(x)$ at position x_0 using (a) Rectangular window and (b) Gaussian window.

Basically, two types of windows are considered for the evaluation purposes, one is rectangular and the other is Gaussian window function or inverted parabola as shown in Figure 4.2. The Gaussian window provides better estimation as compared to the rectangular window function as shown in Figure 4.2. This is due to the fact that in the shifting of rectangular window function to right or left, the estimation shifts up and down in a discrete manner. Here, the allocated weight is exactly either zero or one, which is the reason behind the rough estimation. On the other hand,

Gaussian window function provides zero weight to the points which are too far away and then gives a weight that increases or decreases, thus, providing continuous estimation. There are some regions which have more data points than others, so normalization is needed for the weighted number of data points that are actually inside the prediction window. The normalized weighted function can be represented as [132]:

$$W(i,j) = \frac{e^{\left(-\frac{d''(i,j)^2}{2h^2}\right)}}{\sum_j e^{\left(-\frac{d''(i,j)^2}{2h^2}\right)}} \tag{4.1.17}$$

So, the consequence of this normalization creates the conditions $0 \leq W(i,j) \leq 1$ and $\sum_j W(i,j) = 1$. Where, $d''(i,j)$ denotes the Euclidean distance between two points, therefore point out the dissimilarity between the two pixels. The weighting function $W(i,j)$ allocated weights according to this dissimilarity $d''(i,j)$. Although, the image is discrete in nature, its continuous formulation can be written as [132]:

$$d''(i,j) = \int_{R^2} [F(i+t) - F(j+t)]^2 \, \mathcal{G}_a(t) \, dt \tag{4.1.18}$$

where, $\mathcal{G}_a(t)$ represents the Gaussian window function with standard deviation (a) and i, j and t belong to the 2-Dimensional vector R^2. The integral in (4.1.18) depicts that the similarity between the pixels i and j which depends not only on the pixels i and j but also on their surrounding pixels. The Gaussian window function only decays to zero but never becomes quite zero. Therefore, better results can be obtained by using the b-spline function which becomes exactly zero.

4.1.3 TV-based Deblocking Operation

The researchers utilize effective methods to investigate and remove the JPEG blocking artifacts. But these methods focus only on improving the processed image quality. It is necessary for the anti-forensics to maintain a proper balance between image quality and forensic undetectability. Therefore, the purpose of this improved deblocking scheme applied in the third step of the proposed JPEG anti-forensics is to minimize the TV-based energy. The energy term includes TV

term and blocking measurement term based on TV. By considering an image X of size $T \times T'$, the TV term can be represented as follows [39]:

$$TV(X) = \sum_{1 \le i \le T, 1 \le j \le T'} t_{i,j} \tag{4.1.19}$$

For the evaluation of TV term proposed in [39], only the horizontal and vertical directions were considered. Therefore, a new definition is proposed for the TV term $t_{i,j}$ by considering combined effect of energy variation along horizontal, vertical and diagonal directions modeled as:

$$t_{i,j} = \frac{t'_{i,j} + t''_{i,j}}{2} \tag{4.1.20}$$

where, $t'_{i,j}$ represents the TV along horizontal and vertical directions and $t''_{i,j}$ denotes the variation along diagonal direction as shown in Figure 4.3. This proposed definition of TV- term provides better results than the TV term proposed in [39] by providing enhanced tradeoff between the visual quality of an image and forensic undetectability.

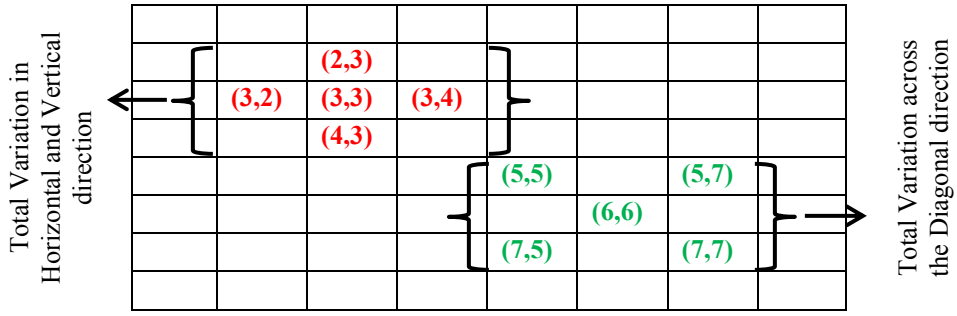


Figure 4.3: Total variation in horizontal, vertical and diagonal directions.

$$t'_{i,j} = \left(\left(X_{i-1,j} + X_{i+1,j} - 2X_{i,j} \right)^2 + \left(X_{i,j-1} + X_{i,j+1} - 2X_{i,j} \right)^2 \right)^{1/2} \tag{4.1.21}$$

$$t''_{i,j} = \left(\left(X_{i-1,j-1} + X_{i+1,j+1} - 2X_{i,j} \right)^2 + \left(X_{i-1,j+1} + X_{i+1,j-1} - 2X_{i,j} \right)^2 \right)^{1/2} \tag{4.1.22}$$

where, $X_{i,j}$ represents the value of the pixel at the (i,j)-th location. The statistical footprints of JPEG blocking artifacts are removed by using the TV-based blocking measurement term. This

term is based on the concept that energy sum obtained from the variation of pixel values along the boundaries of block must be closer to that of energy sum attained from the variation of pixels within the block. Statistically in the image matrix the energy sum does not depend upon on the starting point of 8×8 DCT block. Therefore, depending upon the pixel positions in the block, the image pixels are divided into two groups as shown in Figure 4.4. The shaded pixels locations are considered in set A, while the others are put into the set B. The second term is based on this concept and it can be modeled as [39]:

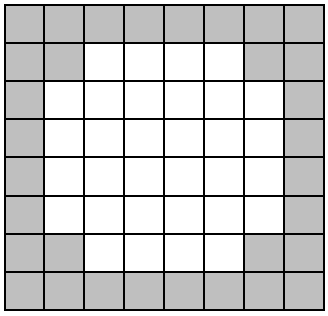


Figure 4.4: Classification of pixels into two sets A (shaded) and B (white).

$$E(X) = \left| \sum_{X_{i,j} \in A} t_{i,j} - \sum_{X_{i,j} \in B} t_{i,j} \right| \tag{4.1.23}$$

The processed image with good quality and forensic undetectability is obtained by constraining the image space (S) defined as [38]:

$$S = \left\{ X \in M^{T \times T'} | (D_{matrix} X)^l_{r,c} \in \left[\left(h^l_{r,c} - \beta \right) q_{r,c}, \left(h^l_{r,c} + \beta \right) q_{r,c} \right] \right\} \tag{4.1.24}$$

where, M denotes the integers set with range $[0, 255]$. Here the constraint image space (S) can be controlled by using the parameter β which is a small positive number and $h^l_{r,c} = (q_{block}(D_{matrix} \boldsymbol{I}))^l_{r,c}$ represents the quantized DCT coefficients for the original uncompressed image $\boldsymbol{I}$. This constraint space keeps the processed image DCT coefficients in the original quantization bins or in the neighboring bins as those of JPEG image which is compressed from the original uncompressed image. The TV-based minimization problem can be defined as [39]:

$$X^* = \arg\min_{X \in S} T(X) = \arg\min_{X \in S} \left(TV(X) + \alpha E(X)\right) \tag{4.1.25}$$

To balance the two energy terms, α acts as a regularization parameter with a positive value. It is easily demonstrated that $T(X)$ is a non-differentiable convex function, whereas S is a convex set [133 - 134]. The projected subgradient method is used to solve the energy minimization problem as [38]:

$$X^{(h+1)} = O_S\left(X^{(h)} - t_{step} \times G\left(X^{(h)}\right)\right) \tag{4.1.26}$$

where, $X^{(h)}$ represents the resultant image obtained after h iterations such that $X^{(0)}$ denotes the given JPEG image and O_S represents the projection operator [38], $G(X)$ is the subgradient of $T(X)$, and t_{step} denotes the positive step size. The step size t_{step} and the regularization parameter α can be adjusted to achieve a better tradeoff between the processed image visual quality and restored DCT histogram quality. The optimized value of α is 1.5 and the step size $t_{step} = 1/h$ is set at the h-th iteration. Also, the optimized value of β is set to 0.5, which helps to constrain the processed DCT coefficients to remain in the original quantization bin [39]. Therefore, proper adjustment of these parameters provides better image visual quality and forensic undetectability.

When the processed DCT coefficients fall outside the original quantization bins, then these coefficients will be mapped back to the original quantization bins with the help of projection operator O_S. The selection of deblocked image candidate is done on the basis of measure K_F that relies on blocking artifacts. The value of K_F has a lower standard deviation as compared to another blocking signature K_U^p in the case of uncompressed images. Also, the detection strength of K_F parameter is more than the parameter K_U^p. Therefore, parameter K_F is used for the selection of deblocked image. In the experiment, 50 iterations are performed and the image with smallest K_F value is selected as the resultant deblocked image.

4.1.4 De-Calibration Operation

The forgery ($\mathcal{F}_{pdb}$) created after the third step (*i.e.*, TV-based deblocking) of the proposed scheme is able to fool most of the existing forensic detectors except the calibration-based

detector K_L. Actually, the value of this calibration-based feature K_L is also decreased considerably after the third step of the proposed scheme. However, the value of this feature is considerably reduced in an interval of very small values. The further reduction of this value along with good image quality is difficult with the application of deblocking operation. Therefore, decalibration process is employed by directly optimizing an energy function which is very similar to the definition of K_L. The subgradient method is used to solve the minimization problem expressed as follows [38]:

$$X^* = \arg\min_X \sum_{k=1}^{28} |var(D_k X) - var(D_k\, X_{cal})| \tag{4.1.27}$$

In this process, the calibrated feature value is directly minimized. Thus, very small values of K_L are obtained when converging to X^* in (4.1.27). The K_L values distribution is exploited for uncompressed images to consider a random threshold for each image to misguide the forensic detector. The iteration continues till the value of K_L drops below this threshold. The final JPEG forgery is acquired after the application of decalibration process.

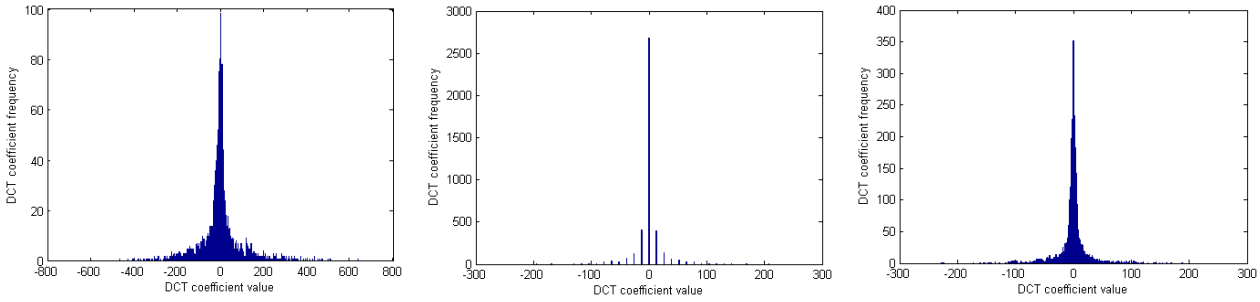
4.2 Experiment Results

In this section, the adequacy of the presented JPEG anti-forensic approach is confirmed by conducting several tests by considering standard UCID. The dataset of single and double compressed images is developed by compressing the UCID dataset images with different quality factors ranging from 50 to 95. The original uncompressed image ***I*** is JPEG compressed to yield an image $\mathcal{T}$ and various types of anti-forensically processed images are generated from this compressed version. All the 1338 images of UCID dataset and their equivalent JPEG (anti-forensic) images are considered for the evaluation purpose. The training dataset is created by selecting the 560 images from UCID dataset and remaining 778 images are used for testing purpose. The proposed JPEG anti-forensic techniques are represented as follows:

- $\mathcal{AF}_1$, represents the proposed anti-forensic technique with an improved TV-based deblocking operation and suggested denoising algorithm based on TV-based energy minimization problem.

- $\mathcal{AF}_2$, represents proposed anti-forensic technique with an improved TV-based deblocking operation and suggested denoising algorithm based on the normalized weighted function.

The concept of the JPEG compression anti-forensics can be visualized by creating the DCT coefficients histogram of a particular sub-band for the original, JPEG compressed and anti-forensically processed images. Figure 4.5 represents the histogram of the DCT coefficients for the (3, 3) sub-band of an uncompressed classical Lena image, a histogram of JPEG compressed Lena image with quality factor 50, and the histogram of the (3, 3) sub-band after the proposed anti-forensic technique. It is evident from Figure 4.5 (c) that the periodic gaps left during the JPEG compression are properly filled by the proposed anti-forensic technique $\mathcal{AF}_2$ without any grainy noise.



(a) (b) (c)

Figure 4.5: DCT coefficients histogram of (3, 3) sub-band of (a) uncompressed image, (b) JPEG image with quality factor 50 and (c) after suggested anti-forensic approach $\mathcal{AF}_2$.

4.2.1 Comparing Anti-Forensic Dithering Methods

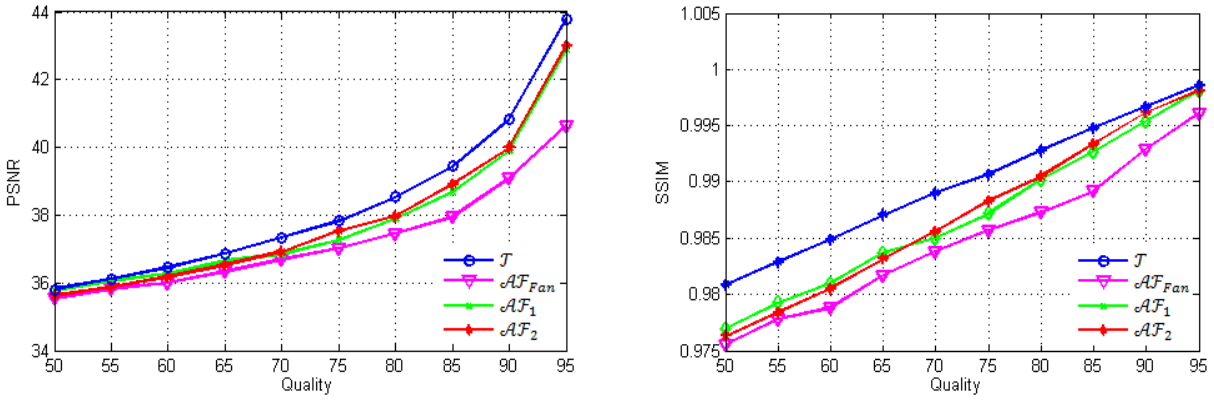
The presented anti-forensic algorithms are evaluated in this section by performing a comparative analysis with the existing anti-forensic dithering techniques. The effectiveness of the proposed anti-forensic techniques $\mathcal{AF}_1$ and $\mathcal{AF}_2$ is evident from Figure 4.6. The computation of PSNR and SSIM values is done by conducting a test on the classical Lena image with original image as reference. It is observed that the Lena image compressed with quality factor 50 has PSNR (dB) and SSIM value equals to 35.8085 and 0.9809 respectively. The JPEG forgery $\mathcal{AF}_{Fan}$ [39] created from JPEG compressed Lena image provides PSNR (dB) and SSIM value equals to 35.5471 and 0.9753 respectively. But the proposed JPEG forgery $\mathcal{AF}_1$ has PSNR (dB) and SSIM value equals to **35.7736** and **0.9770** respectively. Similarly, the proposed JPEG forgery

$\mathcal{AF}_2$ provides PSNR (dB) and SSIM value equals to **35.7938** and **0.9778** respectively. Therefore, the proposed techniques $\mathcal{AF}_1$and $\mathcal{AF}_2$ outperforms the existing $\mathcal{AF}_{Fan}$ technique in terms of PSNR and SSIM values.

(a) (b) (c) (d)

Figure 4.6: (a) JPEG compressed Lena image with quality 50, (b) JPEG forgery $\mathcal{AF}_{Fan}$ [39], (c) Proposed JPEG forgery $\mathcal{AF}_1$, (d) Proposed JPEG forgery $\mathcal{AF}_2$.

Moreover, Figure 4.7 shows the PSNR and SSIM values of the final Lena image processed through the existing JPEG anti-forensic technique $\mathcal{AF}_{Fan}$ and the proposed anti-forensic techniques $\mathcal{AF}_1$ and $\mathcal{AF}_2$, when evaluation is performed by considering different quality factors. The results of existing anti-forensic techniques confirm that concealing of JPEG compression footprints with better image quality is a difficult task. Therefore, it is always required in anti-forensics to create a forgery with high image quality and forensic undetectability. By studying the trend of the curves in Figure 4.7, it is noticed that the suggested anti-forensic methods $\mathcal{AF}_1$ and $\mathcal{AF}_2$ show better results as compared to the existing anti-forensic technique $\mathcal{AF}_{Fan}$ in terms of PSNR and SSIM values.



(a) (b)

Figure 4.7: (a) PSNR (dB) and (b) SSIM value attained by $\mathcal{I}$, $\mathcal{AF}_{Fan}$ [39], $\mathcal{AF}_1$ and $\mathcal{AF}_2$.

The motivation behind the development of the proposed anti-forensic technique is that the PSNR and SSIM of the processed image should approach the PSNR and SSIM of the considered JPEG image. The average PSNR value for the proposed JPEG anti-forensic methods $\mathcal{AF}_1$ and $\mathcal{AF}_2$ is **35.91** dB and **35.93** dB respectively, when a large-scale test is conducted on the UCID dataset images. Similarly, the average SSIM value for the proposed JPEG anti-forensic methods $\mathcal{AF}_1$ and $\mathcal{AF}_2$ is **0.9884** and **0.9893** respectively as shown in Table 4.1. It demonstrates that the proposed anti-forensic methods $\mathcal{AF}_1$ and $\mathcal{AF}_2$, help to achieve higher image quality with better forensic undetectability in comparison to existing methods.

Table-4.1: Comparison of various JPEG anti-forensic methods in terms of average PSNR (dB) and SSIM values, with an uncompressed image as the reference.

Forgeries / Parameters	$\mathcal{I}$	$\mathcal{AF}_{S_q}$ [95]	$\mathcal{AF}_{S_qS_b}$ [96]	$\mathcal{AF}_V$ [37]	$\mathcal{AF}_{S_u}$ [101]	$\mathcal{AF}_F$ [38]	$\mathcal{AF}_{Fan}$ [39]	$\mathcal{AF}_1$ (Proposed scheme)	$\mathcal{AF}_2$ (Proposed scheme)
PSNR	37.10	33.14	30.11	32.12	30.36	34.92	35.24	**35.91**	**35.93**
SSIM	0.9902	0.9713	0.9424	0.9646	0.9627	0.9712	0.9783	**0.9884**	**0.9893**

Most of the JPEG compression forensic approaches examine the pixel value difference either explicitly or implicitly. Therefore, it is also important for the JPEG anti-forensics to recover the pixel value difference statistics along with the image quality and forensic undetectability. This can be quantitatively estimated by using the Kullback-Leibler (KL) [39] divergence of DCT histograms for 64 sub-bands between the original and processed image. KL divergence is used to compute the difference among the two probability distributions. Note that smaller the value of KL divergence, more is the similarity between the two considered images. The comparative analysis of results is shown in Tables 4.2 and 4.3 based on the KL divergence values difference obtained after the third step of the existing anti-forensic technique $\mathcal{AF}_{Fan}$ as well as the proposed anti-forensic techniques $\mathcal{AF}_1$and $\mathcal{AF}_2$. The presented denoising operations reduce the unnatural noises in the image which is processed through the perceptual histogram smoothing. Subsequently, the blocking artifacts of compression are removed to a great extent by applying improved TV-based deblocking procedure. Hence, it can be observed from Tables 4.2 and 4.3 that the third stage of proposed anti-forensic techniques $\mathcal{AF}_1$and $\mathcal{AF}_2$ provide better results as compared to the third stage of the existing $\mathcal{AF}_{Fan}$ technique by providing smaller KL-divergence values for most of the DCT coefficient sub-bands.

Table-4.2: KL divergence values difference between the successive result of the second round TV-deblocking operation of $\mathcal{AF}_{Fan}$ and third step of $\mathcal{AF}_1$ for all 64 DCT sub-bands.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	-0.0212	0.0505	0.1059	-0.0740	0.0635	0.2403	0.2927	0.4409
2	0.1072	0.0838	0.0716	0.0239	0.0555	0.2218	0.2085	0.3271
3	0.1089	0.0701	0.0638	-0.0238	0.2922	0.3485	0.4604	0.5154
4	0.0227	0.0392	-0.0121	0.0874	0.3361	0.4228	0.5292	0.4643
5	0.1582	0.1229	0.2998	0.3430	0.4140	0.5910	0.6108	0.6019
6	0.3177	0.2895	-0.3932	0.4883	0.5076	0.6550	0.6582	0.6515
7	0.4628	0.3911	0.4560	0.6762	0.5745	0.6832	0.7387	0.5628
8	0.7031	-0.5795	0.6481	0.6926	0.7137	0.6261	0.5982	0.2761

Table-4.3: KL divergence difference between the successive result of the second round TV-deblocking operation of $\mathcal{AF}_{Fan}$ and third step of $\mathcal{AF}_2$ for all 64 DCT sub-bands.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	-0.0129	0.0492	0.0736	-0.0627	0.0614	0.2485	0.3199	0.5170
2	0.0703	0.0639	0.0658	0.0345	0.0571	0.2337	0.2374	0.3260
3	0.0986	0.0755	0.0367	-0.0443	0.3068	0.3873	0.4706	0.5321
4	0.0232	0.0218	-0.0342	0.0666	0.3406	0.4388	0.5258	0.4660
5	0.1493	0.1153	0.2686	0.3452	0.4318	0.5846	0.5952	0.5818
6	0.3415	0.3143	-0.3974	0.4850	0.5279	0.6235	0.6496	0.6328
7	0.4762	0.4037	0.4514	0.6734	0.5662	0.6637	0.7325	0.5550
8	0.7765	-0.5692	0.6920	0.6893	0.7118	0.6079	0.5918	0.3248

Table-4.4: KL divergence difference between the TV-deblocking operation proposed in $\mathcal{AF}_{Fan}$ and the proposed TV-deblocking operation for all 64 DCT sub-bands, when tested on classical Lena image.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	-0.0019	0.0519	0.0404	0.0358	0.0222	0.0629	0.2132	0.4080
2	0.0448	0.0827	0.0024	0.0148	0.0385	0.0994	0.1568	0.2933
3	0.0279	0.0137	0.0030	0.0294	0.0698	0.1647	0.3522	0.5435
4	0.0217	0.0131	0.0213	0.0798	0.1077	0.2371	0.3897	0.4608
5	0.0995	0.0351	0.0893	0.1075	0.1999	0.3479	0.4029	0.5066
6	0.1633	0.1158	0.1992	0.2483	0.3464	0.4633	0.3902	0.4939
7	0.4196	0.2632	0.3098	0.3948	0.3993	0.5070	0.4871	0.3086
8	0.7497	0.4837	0.5743	0.6294	0.6113	0.5274	0.3590	0.1035

To further confirm the efficacy of the proposed TV-based deblocking, the KL divergence values (with a reference uncompressed image) of existing TV-based deblocking in $\mathcal{AF}_{Fan}$ and

the proposed TV-based deblocking are evaluated. Table 4.4 depicts the difference between the KL divergence values of existing TV-based deblocking and the proposed TV-based deblocking. It can be inferred from Table 4.4 that except the DC sub-band, the proposed TV-deblocking operation outperforms the existing deblocking operation with small values of KL divergence.

4.2.2 Against JPEG Forensic Detectors

The JPEG forensic detectors are used as attacks to validate the capability of suggested anti-forensic techniques in this subsection. The proposed anti-forensic techniques $\mathcal{AF}_1$and $\mathcal{AF}_2$ are evaluated based on the various existing forensic detectors including $K_L, K_F, K_U^1, K_U^2,\ K_F^q$ with different kind of images compressed with quality factor 50. In this analysis, the PSNR and SSIM values are also provided along with the values of various forensic detectors for more clarity. It can be seen from Table 4.5 that the proposed anti-forensic techniques $\mathcal{AF}_1$and $\mathcal{AF}_2$ outperform the existing $\mathcal{AF}_{Fan}$ technique by providing smaller values for all the forensic detector parameters and larger PSNR and SSIM values for all the considered images.

Table-4.5: Performance of various JPEG forgeries $\mathcal{T}$, $\mathcal{AF}_{Fan}$, $\mathcal{AF}_1$ and $\mathcal{AF}_2$ based on different parameters by considering different kinds of JPEG images with quality factor 50.

Parameters / JPEG forgeries	PSNR (dB)	SSIM	K_L [98]	K_F [63]	K_U^1 [38]	K_U^2 [38]	K_F^q [63]
Lena $\mathcal{T}$	35.8085	0.9809	67.3822	1.0350	8.4993	349.4780	38.0000
Lena $\mathcal{AF}_{Fan}$ [39]	35.5471	0.9753	0.0470	0.0816	0.1061	3.8860	0.0000
Lena $\mathcal{AF}_1$	**35.7736**	**0.9770**	**0.0298**	**0.0756**	**0.0899**	**1.3455**	**0.0000**
Lena $\mathcal{AF}_2$	**35.7938**	**0.9778**	**0.0276**	**0.0456**	**0.0795**	**2.0702**	**0.0000**
Peppers $\mathcal{T}$	34.7507	0.9791	43.5405	1.1595	8.4391	298.8035	41.0000
Peppers $\mathcal{AF}_{Fan}$ [39]	34.5238	0.9738	0.0403	0.1947	0.7018	18.8809	1.0000
Peppers $\mathcal{AF}_1$	**34.6758**	**0.9747**	**0.0305**	**0.1036**	**0.2783**	**7.0140**	**0.0000**
Peppers $\mathcal{AF}_2$	**34.6921**	**0.9743**	**0.0363**	**0.0749**	**0.1818**	**5.7105**	**0.0000**
Barbara $\mathcal{T}$	32.8856	0.9821	88.4474	0.8188	10.4921	633.8459	48.0000
Barbara $\mathcal{AF}_{Fan}$ [39]	31.6186	0.9709	0.0517	0.2109	0.5684	118.4605	0.0000
Barbara $\mathcal{AF}_1$	**32.4339**	**0.9774**	**0.0375**	**0.1930**	**0.4032**	**1.3633**	**0.0000**
Barbara $\mathcal{AF}_2$	**32.6269**	**0.9766**	**0.0339**	**0.1040**	**0.1035**	**1.1039**	**0.0000**
Baboon $\mathcal{T}$	28.2279	0.9803	44.3233	0.5921	17.3929	1845.2121	60.0000
Baboon $\mathcal{AF}_{Fan}$ [39]	27.0367	0.9713	0.0506	0.2184	0.8060	224.1467	0.0000
Baboon $\mathcal{AF}_1$	**28.0614**	**0.9761**	**0.0378**	**0.1782**	**0.6896**	**185.0503**	**0.0000**
Baboon $\mathcal{AF}_2$	**28.8236**	**0.9758**	**0.0323**	**0.1983**	**0.4151**	**124.3153**	**0.0000**

Table-4.6: Different parameter values attained on Lena image after the denoising operation based on TV-based energy minimization problem $\mathcal{F}_{pd}$ of proposed anti-forensic technique based on different quality factors.

Parameters / Quality	PSNR (dB)	SSIM	K_L [98]	K_F [63]	K_U^1 [38]	K_U^2 [38]	K_F^q [63]
50	33.9269	0.9666	0.9758	0.2696	1.0713	41.5550	38.0000
55	34.0321	0.9679	0.9013	0.1950	0.9654	36.4526	38.0000
60	34.1316	0.9687	0.8020	0.2212	0.8387	30.5214	38.0000
65	34.2330	0.9698	0.7124	0.1678	0.7537	25.1501	37.0000
70	34.3444	0.9707	0.6084	0.2101	0.6362	18.3118	36.0000
75	34.4604	0.9715	0.5256	0.1930	0.5723	17.9463	35.0000
80	34.5672	0.9724	0.4139	0.2041	0.4611	13.0580	36.0000
85	34.6862	0.9730	0.2819	0.1744	0.3870	10.7470	33.0000
90	34.8094	0.9736	0.1948	0.1895	0.3044	5.3094	31.0000
95	34.8890	0.9739	0.1411	0.1784	0.2322	5.8981	26.0000

Table-4.7: Different parameter values attained on Lena image after the denoising operation based on normalized weighted function $\mathcal{F}_{pd}$ of proposed anti-forensic technique based on different quality factors.

Parameters / Quality	PSNR (dB)	SSIM	K_L [98]	K_F [63]	K_U^1 [38]	K_U^2 [38]	K_F^q [63]
50	35.1292	0.9637	0.4854	0.0579	0.4675	34.9369	34.0000
55	35.3078	0.9646	0.4119	0.0428	0.3978	32.2444	34.0000
60	35.4509	0.9651	0.2951	0.0670	0.2267	13.5201	34.0000
65	35.6113	0.9658	0.2686	0.0579	0.1675	4.3651	34.0000
70	35.7422	0.9662	0.2288	0.0443	0.1242	0.7861	33.0000
75	35.9065	0.9668	0.2033	0.0726	0.0702	1.4872	32.0000
80	36.0984	0.9675	0.1774	0.0942	0.0209	5.6279	33.0000
85	36.2536	0.9677	0.1316	0.0842	0.0039	5.7050	32.0000
90	36.3805	0.9679	0.1015	0.0595	0.0143	9.4677	33.0000
95	36.4411	0.9680	0.0982	0.0574	0.0206	4.8654	32.0000

Different parameter values are shown in Tables 4.6 and 4.7 which includes PSNR, SSIM, and the forensic detectors corresponding to the different quality factors after the denoising stage ($\mathcal{F}_{pd}$) of the proposed anti-forensic techniques $\mathcal{AF}_1$and $\mathcal{AF}_2$. Tables 4.6 and 4.7 depict that the denoising algorithm based on the normalized weighted function provides better results as compared to the algorithm based on minimization problem of total variation of energy by providing high PSNR with a small loss in SSIM values, and lower values for the forensic

detection parameters. This may happen because of the consideration of all the pixel values of the image for the evaluation of the new pixel value at the particular position in the case of algorithm based on the normalized weighted function.

To confirm the efficacy of the proposed TV-based deblocking, the performance analysis is carried out by considering the deblocking operation only. The performance of the improved TV-based deblocking is analyzed by evaluating various forensic detector parameters along with the existing TV-based deblocking as shown in Table 4.8. The improved TV-based deblocking provides better results for all the considered forensic detection parameters with a small effect on the image quality. It can be noticed from Table 4.8 that the value of detection parameter K_U^2 decreases significantly from **21.6955** to **0.3579**. This is generally because of the proposed definition of TV term that considers the combined effect of TV of energy in horizontal, vertical and diagonal directions.

Table-4.8: Comparison of TV-deblocking operation of $\mathcal{AF}_{Fan}$ and proposed TV-deblocking operation based on different parameters evaluated on Lena image.

Parameters / Deblocking operations	PSNR (dB)	SSIM	K_L [98]	K_F [63]	K_U^1 [38]	K_U^2 [38]	K_F^q [63]
$\mathcal{T}$	35.8085	0.9809	67.3822	1.0350	8.4993	349.4780	38.0000
TV-deblocking [39]	**35.7489**	**0.9765**	0.6704	0.1169	0.4362	21.6955	0.0000
Proposed TV-deblocking	35.6977	0.9756	**0.2607**	**0.0937**	**0.4170**	**0.3579**	**0.0000**

Furthermore, the ROC curve of the JPEG forgery created by the proposed methods is closer to the diagonal (random guess) as compared to the existing JPEG anti-forensic approaches [39, 96] against various forensics detectors as shown in Figure 4.8. Therefore, the proposed anti-forensic techniques are much better in fooling the various forensic detectors as compared to the existing anti-forensic techniques.

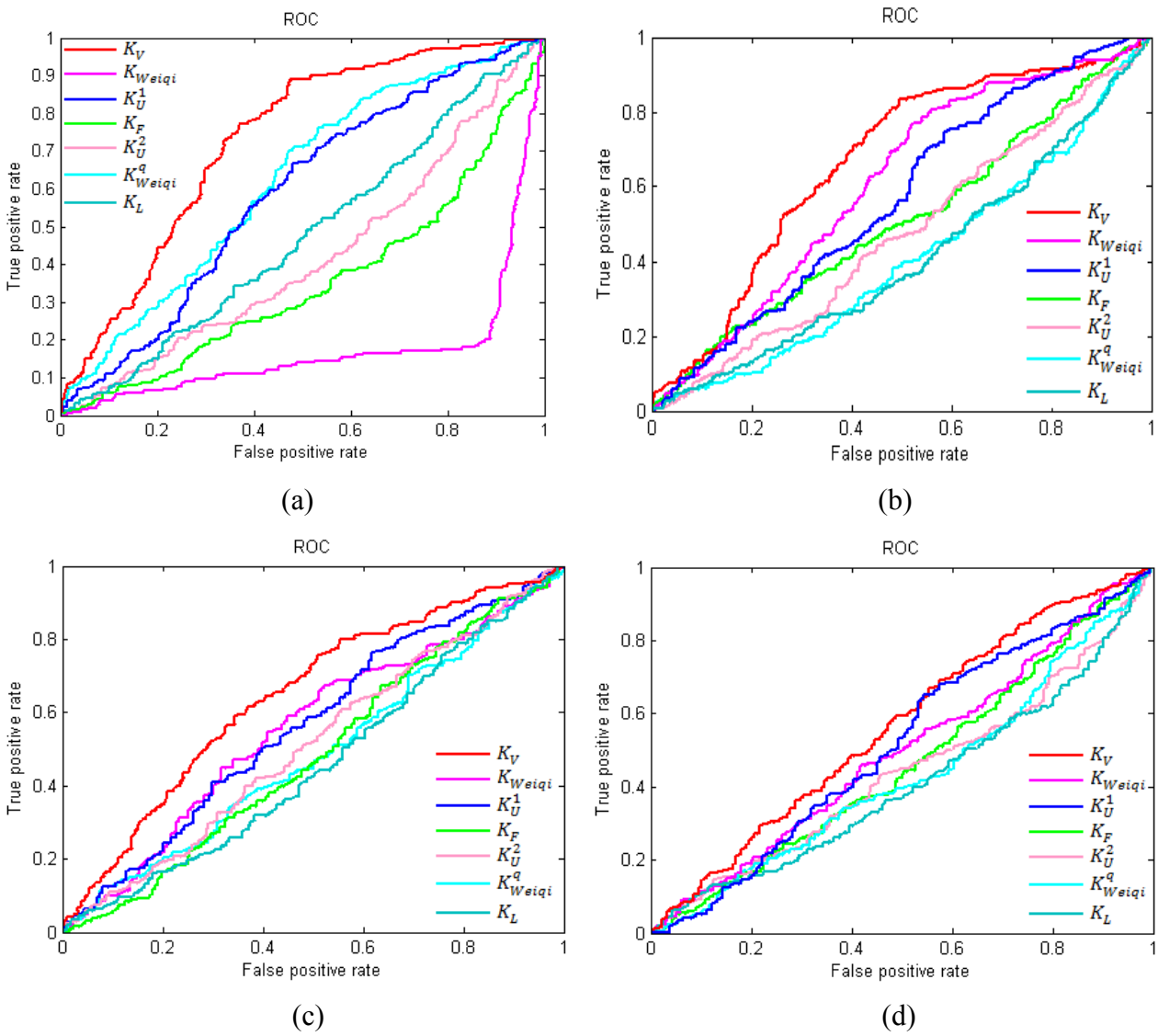


Figure 4.8: ROC curve of (a) $\mathcal{F}_{S_qS_b}$ [96], (b) $\mathcal{AF}_{Fan}$ [39], (c) $\mathcal{AF}_1$ and (d) $\mathcal{AF}_2$ against various forensic detectors. The detectors are fooled better, when the ROC curves approaches to the diagonal (random guess).

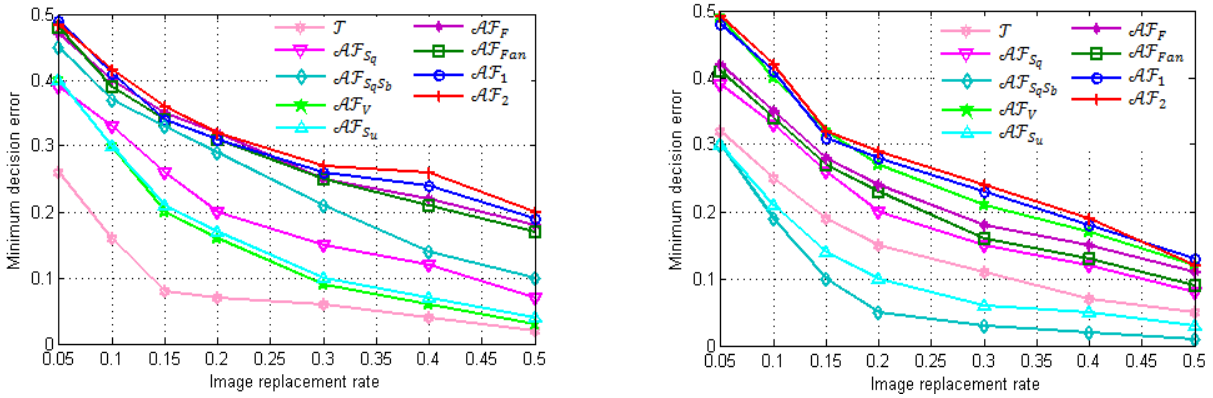
It is observed from Table 4.9 that the forensic detectors can detect the JPEG forgery created by the anti-forensic technique $\mathcal{AF}_{S_q}$. Moreover, the anti-forensic technique $\mathcal{AF}_V$ based on the perceptual dithering scheme achieves a high SSIM value but its forensic undetectability is comparable to the $\mathcal{AF}_{S_q}$technique. The JPEG forgery $\mathcal{AF}_{S_qS_b}$ uses the median filtering to improve the forensic undetectability against various detectors but with a loss of 6.9 dB in PSNR value. However, the proposed schemes are capable to fool the detectors, hence providing higher minimum decision error as compared to existing anti-forensic schemes as evident in Table 4.9.

Table-4.9: Minimum decision error for all the JPEG anti-forensic approaches against various forensic detectors.

Parameters / JPEG forgeries	K_F [63]	K_{Weiqi} [44]	K_{Weiqi}^{q} [44]	K_V [97]	K_L [98]	K_U^1 [38]	K_U^2 [38]
$\mathcal{T}$	0.0061	0	0.0043	0.0136	0.0295	0.0325	0.1687
$\mathcal{AF}_{S_q}$ [95]	0.1248	0.4159	0.2197	0.0168	0.0348	0.0723	0.1189
$\mathcal{AF}_{S_qS_b}$ [96]	0.3364	**0.4358**	0.3067	0.2176	0.4531	0.4048	0.4775
$\mathcal{AF}_V$ [37]	0.0469	0.4078	0.2164	0.0436	0.0235	0.0378	0.1439
$\mathcal{AF}_{S_u}$ [101]	0.1538	0.0724	0.0762	**0.4975**	0.0725	0.3457	**0.4924**
$\mathcal{AF}_F$ [38]	0.3465	0.3578	0.4697	0.3247	0.4825	0.3723	0.4421
$\mathcal{AF}_{Fan}$ [39]	0.3724	0.3726	0.4721	0.3854	0.4982	**0.4128**	0.4627
$\mathcal{AF}_1$ (Proposed scheme)	**0.4786**	0.3978	**0.4891**	0.4153	**0.5000**	0.0899	0.4795
$\mathcal{AF}_2$(Proposed scheme)	**0.4956**	0.4297	**0.4974**	0.4359	**0.5000**	0.0795	0.4831

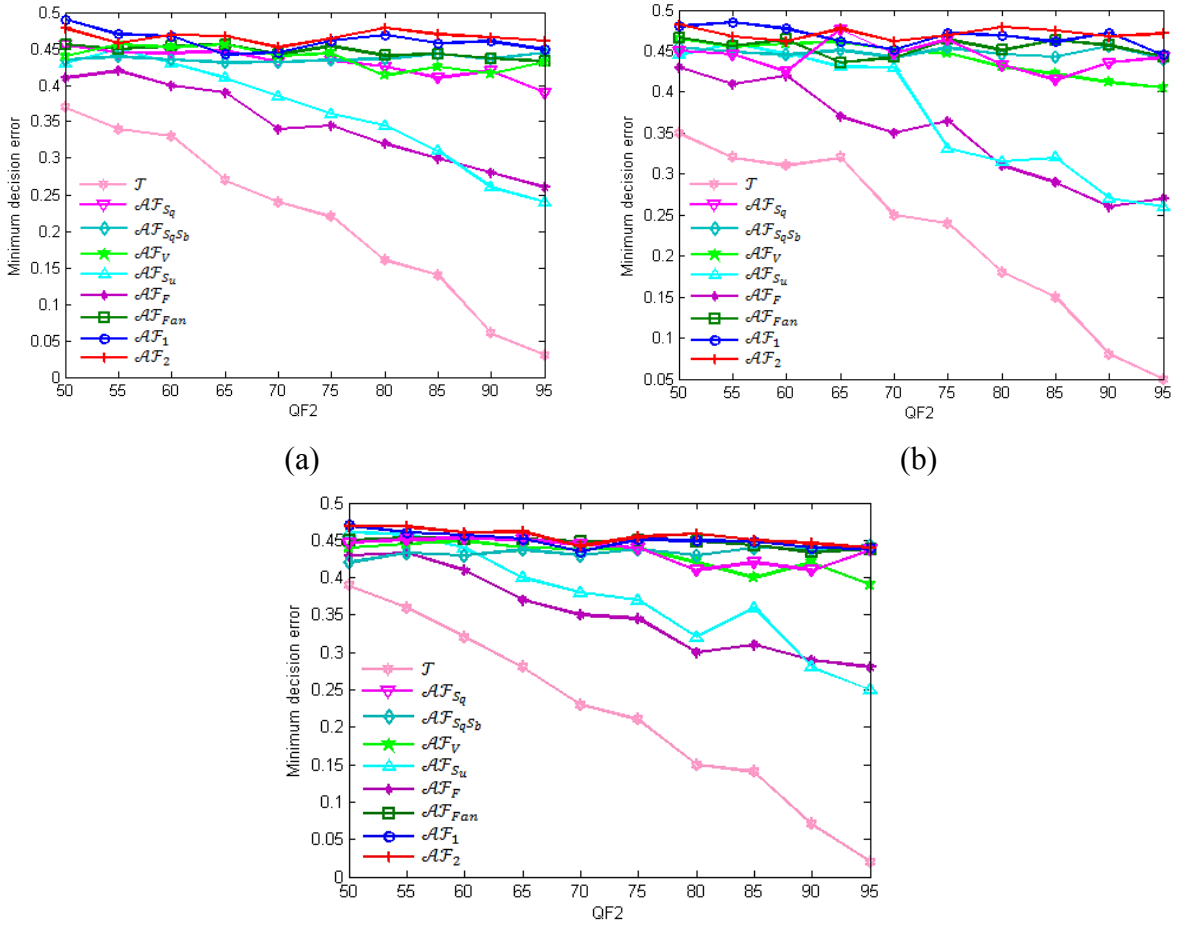
The proposed JPEG anti-forensic methods $\mathcal{AF}_1$ and $\mathcal{AF}_2$ have the capacity to fool even the advanced forensic detector K_V. This happens because of the minimization of proposed TV term in (4.1.20) which is responsible for the suppression of unnatural noises. Moreover, the decalibration operation is applied to defeat the calibration-based detector K_L. When considering the JPEG forgeries created by the proposed anti-forensic methods, 96.72% of the images can be classified as never JPEG compressed. Therefore, the presented JPEG anti-forensics performs better in comparison to the exiting techniques by providing enhanced forensic undetectability with good image quality.

The performance of proposed JPEG anti-forensic schemes is further confirmed by considering the SVM-based forensic detectors $K_{Li}^{S100}$and K_P^{S162} based on the JPEG forgeries created by using the experimental setup of steganography work [112]. The central part of a given uncompressed image is substituted by anti-forensically processed image by considering the image replacement rate that varies from 0.05 to 0.5. Figure 4.9 shows the minimum decision error on the basis of different image replacement rates. The proposed forgery techniques outperform the existing anti-forensic techniques by providing higher minimum decision error when tested against the forensic detectors $K_{Li}^{S100}$and K_P^{S162} as exposed in Figure 4.9.



(a) (b)

Figure 4.9: Minimum decision error based on different values of image replacement rate against SVM-based forensic detectors (a) K_{Li}^{S100} [99], (b) K_P^{S162} [28].



(a) (b)

(c)

Figure 4.10: Minimum decision error as the function of quality factor ($QF2$) for double compressed images against various forensic detectors proposed in (a) [87], (b) [36] and (c) [75].

4.3 Hiding Traces of DJPG Compression Artifacts

To further confirm the performance of the proposed anti-forensic techniques, the test is then conducted on the DJPG compressed images by considering the double compression artifacts detectors [36, 75, 87]. The considered images are JPEG compressed with quality factor QF_1 and then resultant images are compressed again with quality factor QF_2 results in DJPG compressed images. Afterwards, these images are processed with different JPEG anti-forensic techniques in order to create the DJPG compressed forgeries for evaluation purposes. It is evident from the Figure 4.10 that presented anti-forensic techniques are superior than the existing techniques by providing higher minimum decision error, which approaches 0.5 for all the considered quality factors when tested against the forensic detectors [36, 75, 87]. Moreover, the proposed anti-forensic approaches provide higher image quality for DJPG compressed images in comparison to the existing techniques as shown in Table 4.10.

Table-4.10: Average PSNR (dB) and SSIM values for all considered JPEG anti-forensic approaches evaluated on DJPG compressed images.

Forgeries / Parameters	$\mathcal{T}$	$\mathcal{AF}_{S_q}$ [95]	$\mathcal{AF}_{S_qS_b}$ [96]	$\mathcal{AF}_V$ [37]	$\mathcal{AF}_{S_u}$ [101]	$\mathcal{AF}_F$ [38]	$\mathcal{AF}_{Fan}$ [39]	$\mathcal{AF}_1$ (Proposed scheme)	$\mathcal{AF}_2$ (Proposed scheme)
PSNR	34.32	31.68	29.15	32.65	30.31	33.62	33.75	**33.85**	**33.92**
SSIM	0.9415	0.8245	0.7958	0.8824	0.8674	0.9148	0.9254	**0.9324**	**0.9345**

4.4 Analysis of Forensic Detectability and Image Quality

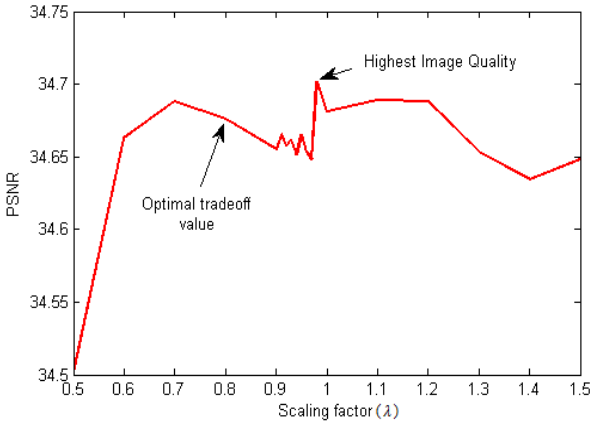
In this section, further research has been carried out to investigate the nature of tradeoff between forensic undetectability and image quality. In this analysis, highest image quality and forensic undetectability are achieved by varying the value of scaling factor (λ) in (4.1.9). It can be inferred from Table 4.11 that highest image quality is achieved at the cost of decrease in forensic undetectability. On the other hand, high forensic undetectability is attained with the loss in image quality.

Table-4.11: Different parameter values attained by the proposed anti-forensic scheme $\mathcal{AF}_1$ by varying the value of scaling factor λ in (4.1.9) based on different images.

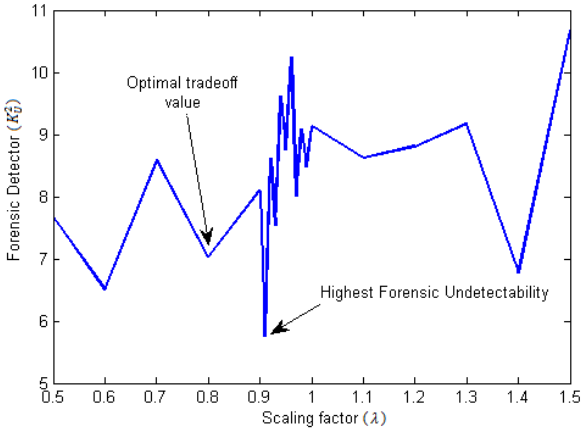
Parameters / Images	PSNR (dB)	SSIM	K_L [98]	K_F [63]	K_U^1 [38]	K_U^2 [38]	K_F^q [63]
Lena $\mathcal{T}$	35.80	0.9809	67.3822	1.0350	8.4993	349.4780	38.00
Lena (with better quality at $\lambda = 0.98$)	**35.79**	0.9782	0.0305	0.1880	0.6368	4.5646	0.00
Lena (with better Forensic Undetectability at $\lambda = 0.91$)	35.70	0.9766	**0.0102**	**0.0421**	**0.0373**	**0.4496**	**0.00**
Peppers $\mathcal{T}$	34.75	0.9791	43.5405	1.1595	8.4391	298.8035	41.00
Peppers (with better quality at $\lambda = 0.98$)	**34.70**	0.9749	0.3304	0.2854	0.3222	10.7726	0.00
Peppers (with better Forensic Undetectability at $\lambda = 0.91$)	34.58	0.9721	**0.0195**	**0.0954**	**0.1721**	**5.7495**	**0.00**
Barbara $\mathcal{T}$	32.88	0.9821	88.4474	0.8188	10.4921	633.8459	48.00
Barbara (with better quality at $\lambda = 0.99$)	**32.45**	0.9776	0.3300	0.2520	1.7230	14.4283	0.00
Barbara (with better Forensic Undetectability at $\lambda = 0.91$)	32.29	0.9719	**0.0214**	**0.1472**	**0.2357**	**0.9547**	**0.00**
Baboon $\mathcal{T}$	28.22	0.9803	44.3233	0.5921	17.3929	1845.2121	60.00
Baboon (with better quality at $\lambda = 0.97$)	**28.17**	0.9765	0.0705	0.2867	4.7869	187.5867	0.00
Baboon (with better Forensic Undetectability at $\lambda = 0.9$)	27.89	0.9712	**0.0215**	**0.0985**	**0.3145**	**112.2514**	**0.00**

Moreover, it can also be perceived from Figures 4.11 (a) and (b), that highest PSNR of 34.7015 dB is obtained at the value of scaling factor $\lambda = 0.98$ but with small forensic undetectability, whereas, highest forensic undetectability in terms of forensic parameter value $K_U^2 = 5.7495$ is obtained at the value of scaling factor $\lambda = 0.91$ but with smaller PSNR value, when tested on the peppers test image. The optimal tradeoff obtained by the proposed scheme $\mathcal{AF}_1$, is around the scaling factor value of 0.8, observed from Figures 4.11 (a) and (b). The values of PSNR and K_U^2 obtained at 0.8 are 34.6758 dB and 7.0140 respectively. Note that smaller the value of

forensic detector parameter K_U^2, more is the forensic undetectability. The forensic undetectability is considered in terms of parameter K_U^2 for the evaluation of the results in Figures 4.11 and 4.12. Similarly, evaluation can also be carried out by considering the other discussed forensic detectors. Figure 4.12 also demonstrates the nature of this tradeoff by considering the forensic parameter values (K_U^2). This is performed on the images obtained by compressing the same Peppers test image with different quality factors ranging from 50 to 90. It can be understood from Figure 4.12 that forensic undetectability decreases with the increase in the image quality based on the various values of scaling factor (λ). The forensic undetectability decreases significantly after the quality factor 70 as shown in Figure 4.12. The proposed JPEG anti-forensic techniques help to achieve better tradeoff between image quality and forensic undetectability.



(a)



(b)

Figure 4.11: (a) PSNR (dB) and (b) K_U^2 values obtained by the proposed anti-forensic scheme $\mathcal{AF}_1$ on Peppers image by considering the various values of scaling parameter (λ) in (4.1.9).

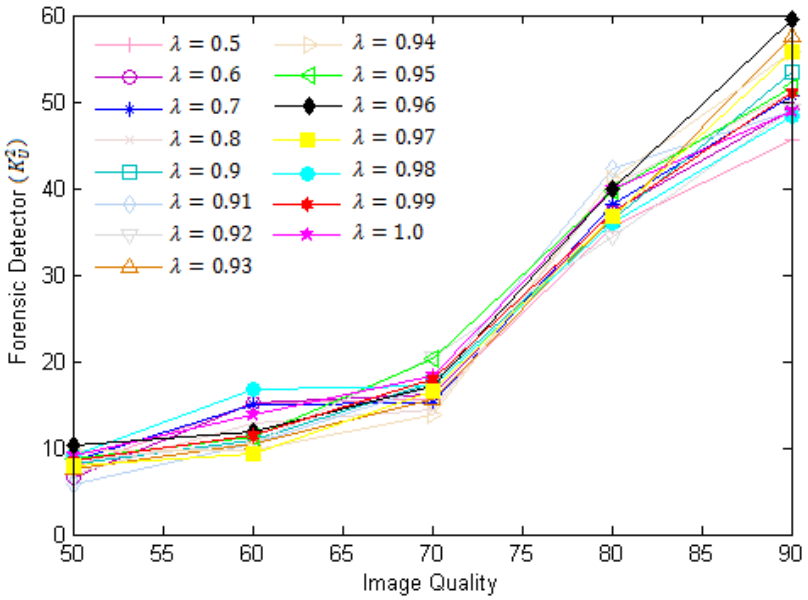


Figure 4.12: Forensic parameter (K_U^2) values obtained by the proposed anti-forensic scheme $\mathcal{AF}_1$ based on the different values of scaling parameter (λ) by considering the images obtained by compressing the same Peppers test image with different quality factors ranging from 50 to 90.

4.5 Computation Time

In this work, the anti-forensic techniques are created by using MATLAB R2016a software on a PC with 2.13 GHz CPU and 3 GB RAM. The execution time required to create the different JPEG forgeries by considering the images of different resolutions is revealed in Table 4.12. It is noticed from Table 4.12 that the time elapsed to create a JPEG forgery increases with the increase in the number of pixels in an image. The proposed anti-forensic techniques $\mathcal{AF}_1$ and $\mathcal{AF}_2$ require around 13.4 and 17.2 minutes respectively to create the JPEG forgery of size 512×512. The perceptual histogram smoothing is the reason behind the high computation cost of presented anti-forensic techniques. The proposed anti-forensic techniques are computationally intensive when compared with existing approaches. Nevertheless, proposed methods of anti-forensics provide a better tradeoff between forensic undetectability and image quality. Moreover, the counterfeiter does not require to produce a large number of forgeries. Therefore, it is reasonable to create a JPEG forgery in around 13 minutes.

Table-4.12: Time elapsed (sec) to create different types of JPEG forgeries based on the images of different resolutions.

Forgeries / Images	$\mathcal{AF}_{S_q}$ [95]	$\mathcal{AF}_{S_qS_b}$ [96]	$\mathcal{AF}_V$ [37]	$\mathcal{AF}_{S_u}$ [101]	$\mathcal{AF}_F$ [38]	$\mathcal{AF}_{Fan}$ [39]	$\mathcal{AF}_1$ (Proposed scheme)	$\mathcal{AF}_2$ (Proposed scheme)
Cameraman [135] (256×256)	0.039	0.051	0.225	0.245	4.502	58.978	**210.587**	**255.347**
Table [117] (512×384)	0.075	0.125	0.562	0.625	14.203	145.548	**525.147**	**863.254**
Boat [135] (512×512)	0.158	0.247	0.924	1.024	18.245	232.247	**840.214**	**1020.254**
Cat [135] (490×733)	0.151	0.260	1.011	1.231	23.128	305.254	**1190.258**	**1448.214**
Building [123] (768×512)	0.192	0.312	1.234	1.420	24.325	350.012	**1260.325**	**1575.232**

4.6 Summary

This chapter presents a JPEG anti-forensic framework to disguise the various forensic detectors by concealing the JPEG artifacts in spatial and DCT domains. Two different denoising algorithms are suggested for the removal of grainy noise left during the dithering operation to enhance the image quality. Moreover, the blocking artifacts are reduced competently by employing the enhanced TV-based deblocking method which results in better forensic undetectability. The presented JPEG anti-forensic scheme provides better results in terms of image quality and forensic undetectability as compared to the existing anti-forensic techniques. The presented improved JPEG compression anti-forensic framework raised questions on the capability of the existing forensic algorithms. Therefore, in the next chapter, further work is dedicated to design a counter JPEG anti-forensic scheme to expose the JPEG compression even in the presence of anti-forensic attacks.

CHAPTER 5

COUNTERING JPEG COMPRESSION ANTI-FORENSICS

The JPEG compression anti-forensic framework designed in the last chapter is capable of misleading the most of existing forensic detectors. Therefore, there is a need to extend the research work towards countering the anti-forensic techniques. A counter JPEG anti-forensic technique is presented in this chapter on the basis of second-order statistical analysis by revealing the artifacts introduced during the JPEG anti-forensics. Actually, the existing forensic work on JPEG compression detection is solely dedicated to the first-order statistical feature components analysis. These first-order traces can be effortlessly concealed by adopting some anti-forensic methods. A higher-order statistical analysis is desired to resolve this problem. Therefore, in this chapter, a second-order statistical analysis based on CM is carried out for countering the JPEG anti-forensics. The dependence or correlation between the neighboring image pixels or coefficients usually gets disturbed or become inconsistent when an image is forged or doctored. Thus, the statistical feature CM is modified due to the inconsistencies. The proposed forensic technique includes the selection of target difference image, evaluation of CMs, and generation of second-order statistical feature based on CMs. The simulation results confirm the efficacy of presented counter JPEG anti-forensic scheme in comparison to the existing techniques.

5.1 Proposed Counter JPEG Anti-Forensic Approach

A counter JPEG anti-forensic technique is suggested based on the second-order statistical analysis of the footprints left during the JPEG anti-forensic methods as shown in Figure 5.1. The second order statistical analysis is carried out based on the CMs to generate a detection feature even in the presence of an anti-forensic attack. The JPEG compressed image is anti-forensically processed by applying the dithering operation in which noise signal is injected in the pixel domain. Therefore, the analysis of distortion in the DCT domain shows that the distortion depends on the original transform coefficients as well as on the quantization matrix. Thus, it is concluded that the anti-forensic dithering energy is concentrated in the middle DCT frequencies which results in the unnatural noise in the spatial domain. Moreover, the neighboring correlation

of DCT coefficients changes after the JPEG anti-forensics. Thus, the second-order statistical analysis is performed to analyze the effects of grainy noise in DCT domain.

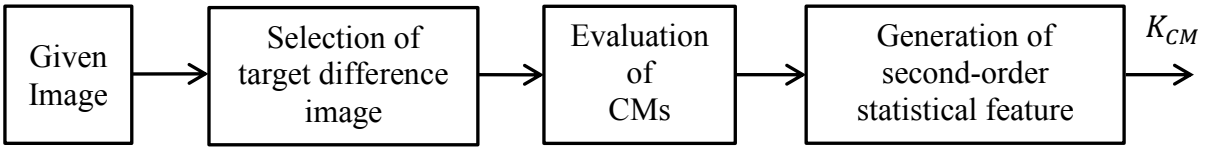


Figure 5.1: Proposed counter JPEG anti-forensic scheme.

5.1.1 Selection of Target Difference Image

The original image pixel values are modified inevitably due to the application of anti-forensic techniques and other image processing operations. Thus, it is difficult to preserve the inherent statistics such as correlation between the adjacent pixels. The local pixels properties within the image are analyzed in the difference domain rather than spatial domain in order to detect these modifications because difference domain is less dependent on the image contents. The considered image is re-compressed by several quality factors ranging from 50 to 95. This range is usually used because the quality factor 100 provides a much larger image as compared to the quality factor 95 with small increase in image quality. On the contrary, the quality factor less than 50 degrades image quality significantly as stated in [122]. Then, the difference between the given image and re-compressed version is computed from pixel values. The difference images corresponding to the different quality factors are high pass filtered to remove the low-frequency information and to enhance the variations due to the unnatural or grainy noise added during JPEG anti-forensics. This can be done by convolving the difference image $I_{diff}(x, y)$ with highpass operator $h(x, y) = [0, 1, 0; 1, -4, 1; 0, 1, 0]$ which results in $I_{filter}(x, y)$ [136]. The selection of the highpass operator has been made in such a way that it aids in the detection of modification of variance characteristics due to grainy noise added during the dithering operation.

Now, after the highpass filtering, each pixel of the filtered image $I_{filter}(x, y)$ is supposed to be drawn from a normal distribution with a certain variance. The MLE is used to evaluate the statistical variance of the pixel values along each diagonal. We observed that the resultant feature is more dominant in the diagonal direction as compared to the horizontal/vertical directions. This may happen because the TV-based deblocking minimization operations of most of the JPEG anti-forensic methods are based on the horizontal and vertical directions. Therefore, the anti-

forensic artifacts (unnatural or grainy noise) are more dominant in the diagonal directions. To reduce the computation complexity, mean of the absolute values of each diagonal in the image is considered instead of variance. Now, the image becomes a single dimensional signal and the normalized estimate of variance corresponding to the d^{th} diagonal is denoted by $E_{var}(d)$ [136].

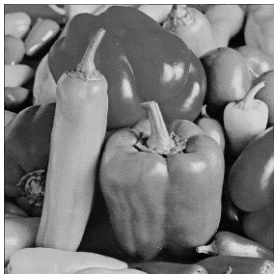
$$E_{var}(d) = \frac{\sum_{x+y=d} \left| I_{filter}(x, y) \right|}{N_d} \tag{5.1.1}$$

where, N_d represents the total number of pixels along the d^{th} diagonal. The variations in $E_{var}(d)$ can be examined by considering the Fourier transform of the estimated variance for all the difference images. The peak magnitude of the frequency spectrum can be estimated as [136]:

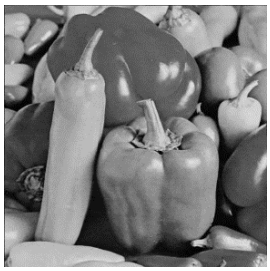
$$Peak = max\left(abs\left(fft\left(E_{var}(d)\right)\right)/M_s\right) \tag{5.1.2}$$

where, M_s denotes the median value of spectrum but it does not include the DC value. Here, normalizing by M_s factor helps to differentiate between the uncompressed image and the images containing unwanted noise signals. To highlight the artifacts of grainy noise due to JPEG anti-forensics, the difference image corresponding to the highest peak is selected. The variations in the estimated variance $E_{var}(d)$ can be observed from the second row of Figures 5.2 and 5.3. The signal $E_{var}(d)$ becomes more symmetric in the case of anti-forensically JPEG processed images by $\mathcal{AF}_{Fan}$ as compared to the uncompressed images. This is due to the perceptual histogram smoothing of JPEG anti-forensic scheme $\mathcal{AF}_{Fan}$. Also, the signal peak magnitude decreases to less than half in the case of JPEG forgeries. Similarly, the energy peak magnitude also decreases significantly in the frequency spectrum of the estimated variance $E_{var}(d)$ for the anti-forensically processed images as shown in the third row of Figures 5.2 and 5.3. The fourth row of Figures 5.2 and 5.3 reports the frequency spectrum peak magnitude of all the difference images based on different quality factors for uncompressed and anti-forensically processed images. The difference images with highest peak are selected corresponding to quality factor 61 and 71 for Peppers uncompressed image and JPEG forgery respectively. For the Lena uncompressed and its JPEG forgery, difference images corresponding to the quality factor 84 and 51 respectively are selected for further processing. The highlighted artifacts at this stage are further explored by second-order statistical feature based on CM.

(I)

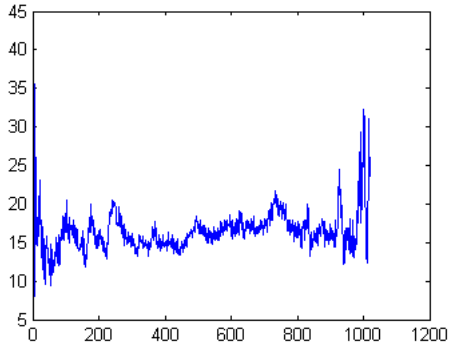


Uncompressed Peppers image

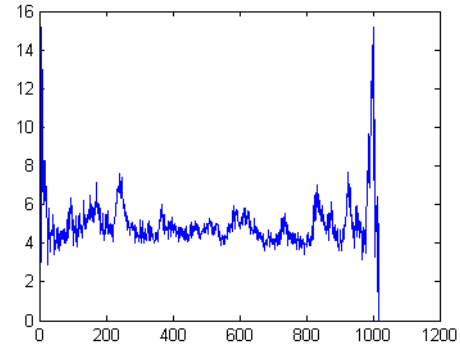


JPEG forgery ($\mathcal{AF}_{Fan}$) at 50 quality factor

(II)

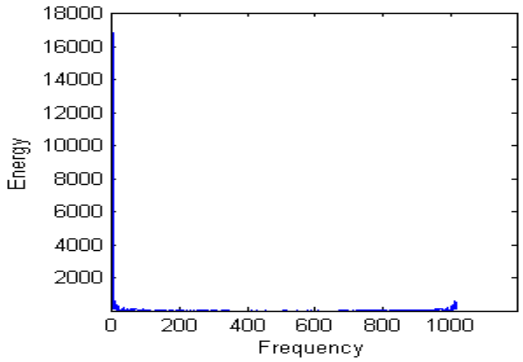


For uncompressed image

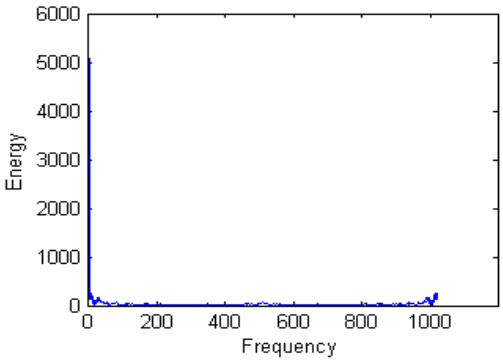


For JPEG forgery

(III)

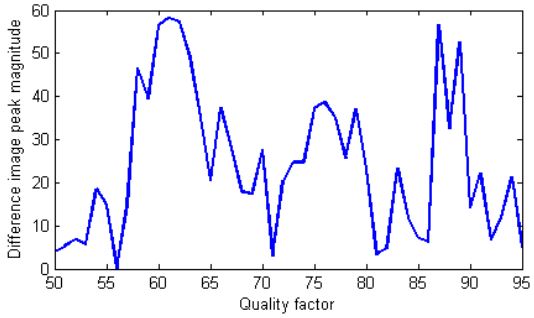


For uncompressed image

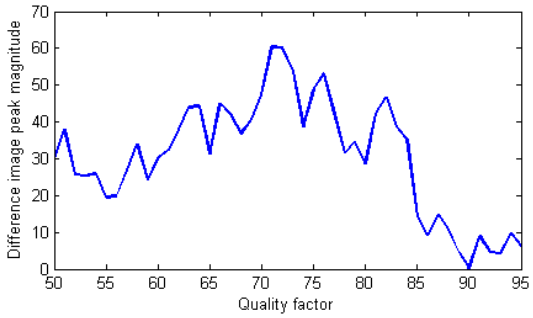


For JPEG forgery

(IV)



For uncompressed image



For JPEG forgery

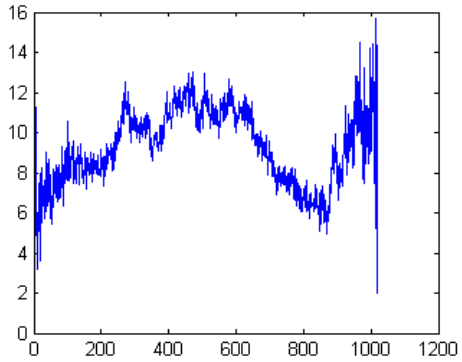
Figure 5.2: Row (I) uncompressed and anti-forensically ($\mathcal{AF}_{Fan}$) processed versions of Peppers image, (II) Variance $E_{var}(d)$, (III) Frequency spectrum of $E_{var}(d)$, and (IV) Peak magnitude of the spectrum of $E_{var}(d)$ for difference images based on various quality factors.

(I)

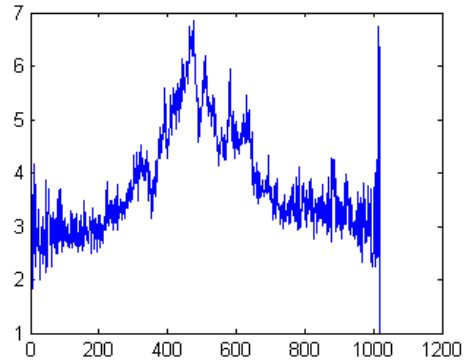
Uncompressed Lena image

JPEG forgery ($\mathcal{AF}_{Fan}$) at 50 quality factor

(II)

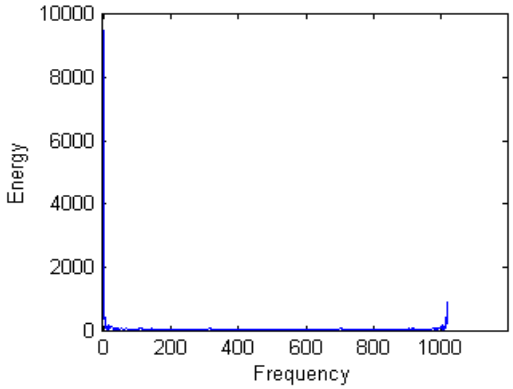


For uncompressed image

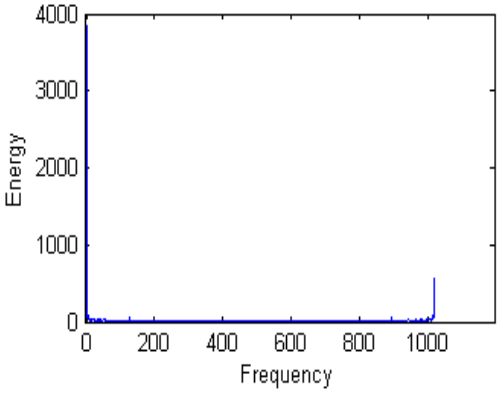


For JPEG forgery

(III)

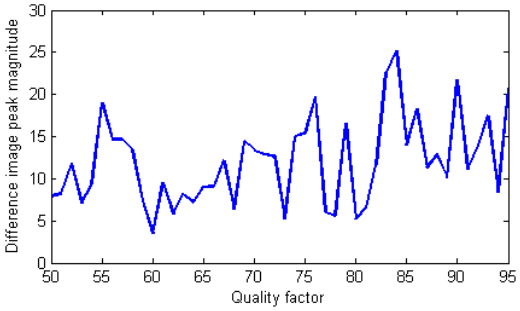


For uncompressed image

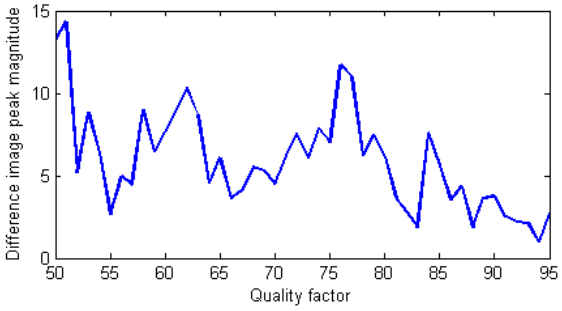


For JPEG forgery

(IV)



For uncompressed image



For JPEG forgery

Figure 5.3: Row (I) uncompressed and anti-forensically ($\mathcal{AF}_{Fan}$) processed versions of Lena image, (II) Variance $E_{var}(d)$, (III) Frequency spectrum of $E_{var}(d)$, and (IV) Peak magnitude of the spectrum of $E_{var}(d)$ for difference images based on various quality factors.

5.1.2 Evaluation of Co-Occurrence Matrices

The natural images have strong dependence or correlation between the neighboring DCT coefficients. The CM [137] exploits the distribution characteristics of the whole image data based on the joint distribution probability of adjoining data and can clearly reveal the correlation between the neighboring image data. In JPEG images, the neighboring DCT coefficients have strong correlation both in intra and inter-block of DCT domain. Suppose $M \times N$ is the size of the DCT coefficients matrix D of the considered image and $D_{m,n}(e,f)$ represents the value of the DCT coefficient in location (e,f) corresponding to m-th row and n-th column block. The CMs for the horizontal and vertical neighboring coefficients in intra and inter-block of DCT domain can be evaluated by using (5.1.3) to (5.1.6) [137].

$$\boldsymbol{CM}_{intra,h}(u,v) = \boldsymbol{\mathcal{P}}\big(D_{m,n}(e,f) = v, D_{m,n}(e,f+1) = u\big) = \frac{\sum_{m=1}^{M/8}\sum_{n=1}^{N/8}\sum_{e=1}^{8}\sum_{f=1}^{7}\partial\left(v, D_{m,n}(e,f)\right)\partial\left(u, D_{m,n}(e,f+1)\right)}{56 \times (M/8) \times (N/8)} \quad (5.1.3)$$

$$\boldsymbol{CM}_{intra,v}(u,v) = \boldsymbol{\mathcal{P}}\big(D_{m,n}(e,f) = v, D_{m,n}(e+1,f) = u\big) = \frac{\sum_{m=1}^{M/8}\sum_{n=1}^{N/8}\sum_{e=1}^{7}\sum_{f=1}^{8}\partial\left(v, D_{m,n}(e,f)\right)\partial\left(u, D_{m,n}(e+1,f)\right)}{56 \times (M/8) \times (N/8)} \quad (5.1.4)$$

$$\boldsymbol{CM}_{inter,h}(u,v) = \boldsymbol{\mathcal{P}}\big(D_{m,n}(e,f) = v, D_{m,n+1}(e,f) = u\big) = \frac{\sum_{m=1}^{M/8}\sum_{n=1}^{N/8-1}\sum_{e=1}^{8}\sum_{f=1}^{8}\partial\left(v, D_{m,n}(e,f)\right)\partial\left(u, D_{m,n+1}(e,f)\right)}{64 \times (M/8) \times (N/8-1)} \quad (5.1.5)$$

$$\boldsymbol{CM}_{inter,v}(u,v) = \boldsymbol{\mathcal{P}}\big(D_{m,n}(e,f) = v, D_{m+1,n}(e,f) = u\big) = \frac{\sum_{m=1}^{M/8-1}\sum_{n=1}^{N/8}\sum_{e=1}^{8}\sum_{f=1}^{8}\partial\left(v, D_{m,n}(e,f)\right)\partial\left(u, D_{m+1,n}(e,f)\right)}{64 \times (M/8-1) \times (N/8)} \quad (5.1.6)$$

Here, $\boldsymbol{CM}_{intra,h}$ and $\boldsymbol{CM}_{inter,h}$ represent the co-occurrence features components for the horizontal direction with joint distribution probabilities $\boldsymbol{\mathcal{P}}\big(D_{m,n}(e,f) = v, D_{m,n}(e,f+1) = u\big)$ and $\boldsymbol{\mathcal{P}}\big(D_{m,n}(e,f) = v, D_{m,n+1}(e,f) = u\big)$, respectively for the coefficients pair (v,u). Similarly, the joint distribution probabilities can be defined for the main and minor diagonal arrays for the

intra and inter-block of the DCT domain. Thus, the JPEG compression detection feature is based on the combination of CMs in horizontal, vertical and diagonal directions. Each CM contains $(H-G+1)^2$ number of elements, where $[G,H]$ is the range of u and v. The matrix containing $(H-G+1)^2$ number of feature components can be calculated by applying (5.1.7) [137].

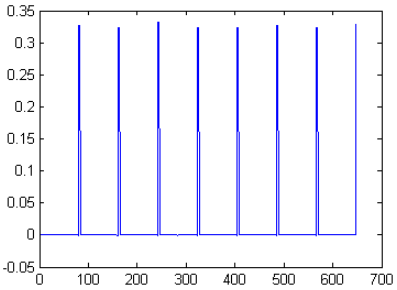
$$\boldsymbol{CM} = \begin{bmatrix} \boldsymbol{\mathcal{P}}(G,G) & \boldsymbol{\mathcal{P}}(G,G+1) & \cdots & \boldsymbol{\mathcal{P}}(G,H) \\ \boldsymbol{\mathcal{P}}(G+1,G) & \boldsymbol{\mathcal{P}}(G+1,G+1) & \cdots & \boldsymbol{\mathcal{P}}(G+1,H) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{\mathcal{P}}(H,G) & \boldsymbol{\mathcal{P}}(H,G+1) & \dots & \boldsymbol{\mathcal{P}}(H,H) \end{bmatrix} \tag{5.1.7}$$

The CM exploiting the correlation between the neighboring DCT coefficients is symmetric about (0,0). Consequently, the absolute value of the DCT coefficients can also be utilized for the evaluation of probability distribution based on CM. The CM generally has a sharp peak at (0,0) and then falls off rapidly because the majority of the high-frequency DCT coefficients are zero. The deviations induced due to the compression spread by some small value around (0,0). The dimension of the CM feature increases by the second power of range $(H-G)$ as shown in (5.1.7). Therefore, coefficients statistical range is defined in proper range to extract the features in controlled dimension. Most of the variations occur near the origin, therefore, the range of u and v is set to $[-4,4]$ providing 81 feature components for each CM [137]. Therefore, in total, we get 648 feature components from all inter and intra-block CMs along horizontal, vertical, main diagonal and minor diagonal directions. These feature components are further processed in the following subsection to further highlight the dithering artifacts (*i.e.*, unwanted grainy noise added during anti-forensics) explored by the CMs. This results in the generation of an optimal second-order statistical feature.

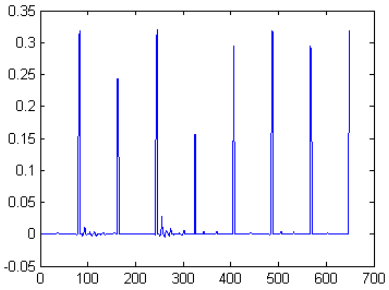
5.1.3 CM-based Second-Order Statistical Feature

In this section, efforts have been made to analyze the effect of anti-forensic approaches on CMs. Most of the anti-forensic techniques are based on the optimization problem with an objective of finding an optimal mapping to get back the original uncompressed image statistics. In this process, pixels are transferred from one to another bin based on a maximal pixel distortion. The mapping is performed by selecting pixels in such a way that it reduces the perceptual effect [39]. These anti-forensic attacks can completely remove the gaps in the histogram of JPEG compressed images. The histograms of uncompressed and anti-forensically processed images are

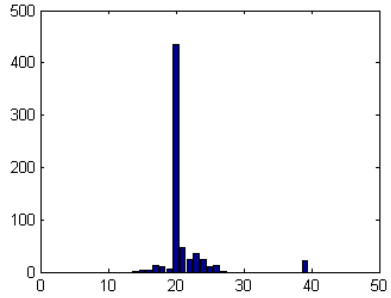
identical but there are still noticeable footprints in the CM. We are looking for a second-order statistical feature derived from CM that can discriminate the uncompressed and anti-forensically processed images competently.



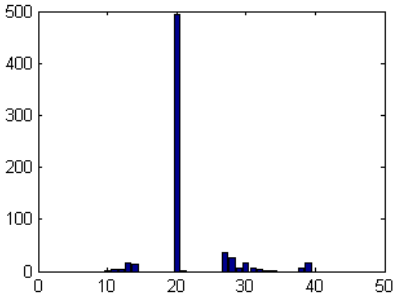
(a) $\varphi(n)$ for uncompressed image



(b) $\varphi(n)$ for JPEG forgery ($\mathcal{AF}_{Fan}$)



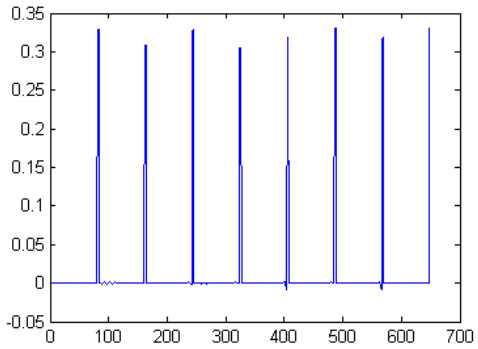
(c) Histogram for uncompressed image



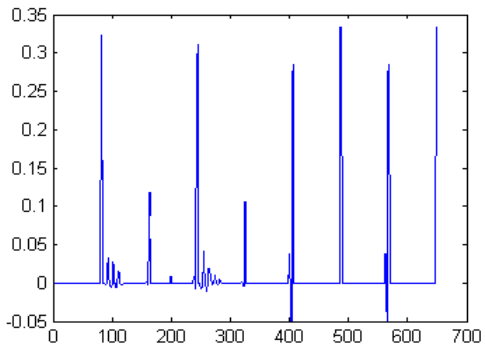
(d) Histogram for JPEG forgery ($\mathcal{AF}_{Fan}$)

Figure 5.4: Resultant signal $\varphi_{diff}(n)$ for (a) uncompressed and (b) anti-forensically processed Peppers images. Histogram of $\varphi_{diff}(n)$ for (c) uncompressed and (d) anti-forensically processed Peppers images.

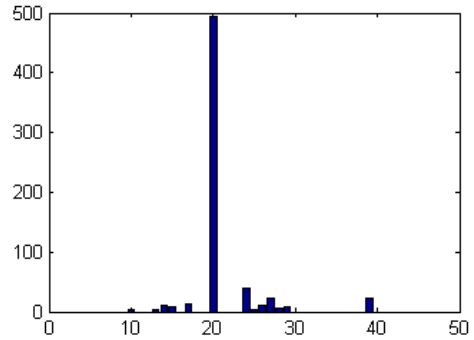
By observing different characteristics based on CM of the considered image, a mono-dimensional signal is derived by concatenating the rows of all inter and intra-block CMs highlighting the presence of dithering artifacts introduced during the image anti-forensics. Let $\varphi(n)$ denotes a mono-dimensional signal of size (1, 648) based on CMs. The analysis of signal $\varphi(n)$ illustrates that an uncompressed image exhibits a smooth behavior whereas the JPEG compressed image processed through anti-forensics shows an oscillating behavior as shown in Figures 5.4 and 5.5. The signal $\varphi(n)$ is processed to detect this behavior by applying the mean filtering which results in $\varphi_{Mean}(n)$. Then, the median filtering is applied to the signal $\varphi_{Mean}(n)$ which provides the signal $\varphi_{Median}(n)$. The oscillatory behavior of the signal $\varphi(n)$ is highlighted by computing the following normalized equation as [138]:



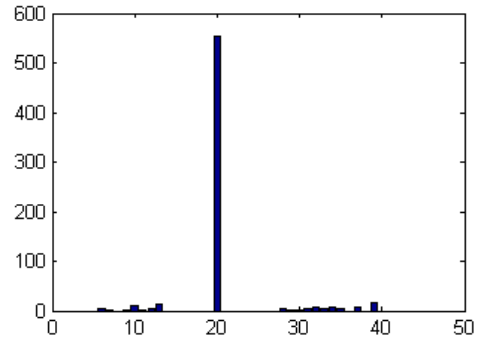
(a) $\varphi(n)$ for uncompressed image



(b) $\varphi(n)$ for JPEG forgery ($\mathcal{AF}_{Fan}$)



(c) Histogram for uncompressed image



(d) Histogram for JPEG forgery ($\mathcal{AF}_{Fan}$)

Figure 5.5: Resultant signal $\varphi_{diff}(n)$ for (a) uncompressed and (b) anti-forensically processed Lena images. Histogram of $\varphi_{diff}(n)$ for (c) uncompressed and (d) anti-forensically processed Lena images.

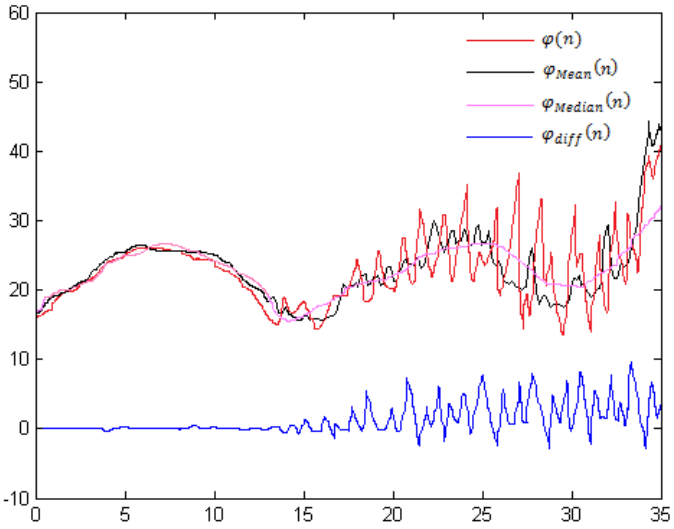


Figure 5.6: Variations in the signal $\varphi_{diff}(n)$ occurred due to the application of filtering operations on the original signal $\varphi(n)$.

$$\varphi_{diff}(n) = \frac{\tilde{\varphi}_{diff}(n)}{max\left(\tilde{\varphi}_{diff}(n)\right) - min\left(\tilde{\varphi}_{diff}(n)\right)} \tag{5.1.8}$$

where, $\tilde{\varphi}_{diff}(n)$ can be represented as:

$$\tilde{\varphi}_{diff}(n) = \varphi_{Median}(n) - \varphi_{Mean}(n) \tag{5.1.9}$$

The low pass component of the signal $\varphi(n)$ is eliminated while keeping the high frequency oscillations, when processed through the (5.1.8) and (5.1.9). In the first case, when the signal $\varphi(n)$ has a low pass behavior, then the signals $\varphi_{Mean}(n)$ and $\varphi_{Median}(n)$ follow it so that the resulting signal $\varphi_{diff}(n)$ becomes uniform as shown in Figure 5.6. Secondly, if the signal $\varphi(n)$ has an oscillating behavior, then the signals $\varphi_{Mean}(n)$ and $\varphi_{Median}(n)$ are well distinct and thus the resulting signal $\varphi_{diff}(n)$ becomes oscillating in nature. The artifacts in the CM of the anti-forensically processed JPEG compressed image is related to the large number of small deviations from zero in the $\varphi_{diff}(n)$ signal. On the contrary, the isolated deviations in the signal $\varphi_{diff}(n)$ having large amplitude occur due to the filtering process as shown in Figure 5.6. The histogram of $\varphi_{diff}(n)$ signal is generated as shown in Figures 5.4 and 5.5 to capture the amount of small deviations. We are giving special attention to small values by creating a symmetric histogram having $2N_{bin}$ bins, represented as $\{H_{-N_{bin}}, \dots, H_{-1}, H_1 \dots H_{N_{bin}}\}$ with logarithmically distributed width between $10^{\mathbb{i}}$ and $10^{\mathbb{j}}$. Here, for evaluation purpose, we consider N_{bin}= 20, $\mathbb{i} = -3$ and $\mathbb{j} = 1$ to investigate the small deviations. If we properly define a parameter $\Delta = (\mathbb{i} - \mathbb{j})/(N_{bin} - 1)$, then the i-th bin is centered on the value as follows [138]:

$$H_i = \begin{cases} 10^{(\mathbb{i}+(i-1)\Delta)} \times N_{bin}^{-1} & for\ i \in \{1, 2, 3, \dots, N_{bin}\} \\ -H_{-i} & for\ i \in \{-N_{bin}, \dots, -1\} \end{cases} \tag{5.1.10}$$

Figures 5.4 and 5.5 show that the $\varphi_{diff}(n)$ based histogram has more bins present nearby the central bin for uncompressed Peppers and Lena images. However, in the case of Peppers and Lena JPEG forgeries, bins move away from the central bin. The magnitude of the central bin for JPEG forgeries increases due to the movement of neighbor bins elements to the center bin. This normalized histogram feature vector is fed to SVM to classify the signals generated from uncompressed and anti-forensically processed JPEG compressed images.

Algorithm for the proposed Counter JPEG anti-forensic technique:

***Input*:**

I_{input}: Anti-forensically processed JPEG image.

***Output*:**

H_{final}: Histogram feature vector based on $\varphi_{diff}(n)$.

***Parameters*:**

QF: Quality factor

$I_{recompressed}$: Re-compressed image

I_{diff}: Difference image

h: High pass filtering operator

I_{filter}: Image obtained after the high pass filtering

N_d: Number of pixels along the d^{th} diagonal

$F_{spectrum}$: Frequency spectrum of estimated variance (E_{var})

M_s: Median value of the frequency spectrum

$Peak$: Peak magnitude in the frequency spectrum

begin

$[x, y] = size(I_{input})$;

$QF = 50{:}\,1{:}\,95$; $W_{size} = 7$; $l' = 3$; $\mathbb{i} = -3$; $\mathbb{j} = 1$; $N_{bin} = 20$;

$N_{QF} = length(QF)$; $Peak = zeros(1, N_{QF})$;

$I_{difference} = zeros(x, y, length(QF))$; Initialize $count = 1$;

for $i = QF$ ***do***

$I_{recompressed} = recompress(I_{input}, i)$; % Recompression with different quality factors

$I_{diff}(:,:,c) = I_{input}(:,:) - I_{recompressed}(:,:)$; $h = [0\ 1\ 0; 1\ -4\ 1;\ 0\ 1\ 0]$;

$I_{filter} = conv2\ (I_{diff}, h, 'valid')$; % High pass filtering is applied to remove the low frequency information

$I_{filter} = fliplr\ (I_{filter})$; % Flip matrix left to right

$E_{var} = [\,]$;

for $d = (\ size\ (I_{filter}, 2) - 1) : -1 : (-size\ (I_{filter}, 1) + 1)$

$E_{var}(\ size\ (I_{filter}, 2) - d) = mean\ (abs(\ diag\ (I_{filter}, d)\ ))$; % Compute variance diagonally

end

$F_{spectrum}(:,:,c) = abs(fft(E_{var}))$; % Frequency spectrum of estimated variance

$M_s = median\ (F_{spectrum}(2{:}\,end))$;

$M_{spectrum}(c) = F_{spectrum}(\ floor\ (\ size\ (F_{spectrum}, 2)\ /2) + 1)$;

$Peak = M_{spectrum}/M_s$; $count = count + 1$;

end

$[value, index] = max(M_{spectrum})$;

$I_{selected} = I_{diff}(:,:,index)$; % Difference image is selected corresponding to the highest peak

$I_{dct} = abs(dct(I_{selected}))$;

$f1 = CM_{intra,h}(I_{dct})$; $f2 = CM_{inter,h}(I_{dct})$; $f3 = CM_{intra,v}(I_{dct})$; $f4 = CM_{inter,v}(I_{dct})$;

$f5 = CM_{intra,d'}(I_{dct})$; $f6 = CM_{inter,d'}(I_{dct})$; $f7 = CM_{intra,d''}(I_{dct})$; $f8 = CM_{inter,d''}(I_{dct})$; % CMs based on intra and inter-block of DCT domain for Horizontal, Vertical, Main and Minor diagonal directions

$f = [f1;\ f2;\ f3;\ f4;\ f5;\ f6; f7; f8]$;

$Coef_{vector} = ones(1, l')/l'$;

$\varphi_{Mean} = filter(Coef_{vector}, 1, f)$;

$\varphi_{Median} = medfilt1(\varphi_{Mean}, W_{size})$;

$\tilde{\varphi}_{diff} = \varphi_{Median} - \varphi_{Mean}$;

$X_{min} = \min(\tilde{\varphi}_{diff})$;

$X_{max} = max(\tilde{\varphi}_{diff})$;

$\varphi_{diff} = \tilde{\varphi}_{diff}(n)/(X_{max} - X_{min})$;

$ls = logspace(\mathbb{i}, \mathbb{j}, N_{bin})/N_{bin}$;

$Bin = [-ls(end{:}-1{:}\,1)\ ls]$;

$H_{final} = hist(\varphi_{diff}, BIN)$; % Compute the resultant histogram feature vector based on $\varphi_{diff}(n)$

end

5.2 Experiment Results

In this section, the proposed counter JPEG anti-forensic technique is evaluated to confirm its capability in detecting JPEG compression footprints even after the application of anti-forensics by performing several tests on standard UCID and BOSSBase database. The images from both the datasets are compressed with different quality factors in the range $\{50, 51, 52, \ldots, 95\}$. Afterward, these compressed images are processed with different JPEG anti-forensic methods in order to create the corresponding JPEG forgery datasets. The image datasets created for the evaluation purpose are discussed in detail in Section 2.3 of Chapter 2. The evaluation is performed by considering the various SVM-based forensic detectors.

5.2.1 Comparing SVM-based Forensic Detectors

Anti-forensic techniques are used to fill the periodic gaps that are left during the JPEG compression. But the dithering operation of the anti-forensic approach introduces an unnatural or grainy noise in the spatial domain. The presented forensic technique aims to reveal the JPEG compression footprints even after the application of JPEG anti-forensic techniques. By exploring the statistical property of DCT coefficients, it is observed that the DCT coefficients are modified by the JPEG anti-forensic approaches. This modification of DCT coefficients changes the correlation of neighboring DCT coefficients. The Markov transition probabilities are affected because dithering operation of JPEG anti-forensic schemes changes the neighboring joint distribution or CM. It is also analyzed that the variation of the Markov transition probability cannot entirely reflect the change of the neighboring joint density. Hence, the proposed counter JPEG anti-forensic technique K_{CM} is much better in detecting the artifacts left during the JPEG anti-forensics in comparison to the existing SVM-based forensic detectors.

It is important to note that the conventional SRM-34,671 can hardly be utilized in SVM due to its high feature dimensionality as mentioned in [29]. SRM-714 suggested in [29] is an advanced version of SRM-34,671 that provides almost similar performance as that of the SRM-34,671 along with the huge reduction in feature dimensionality. Therefore, to make the comparison feasible we have compared our scheme with SRM-714.

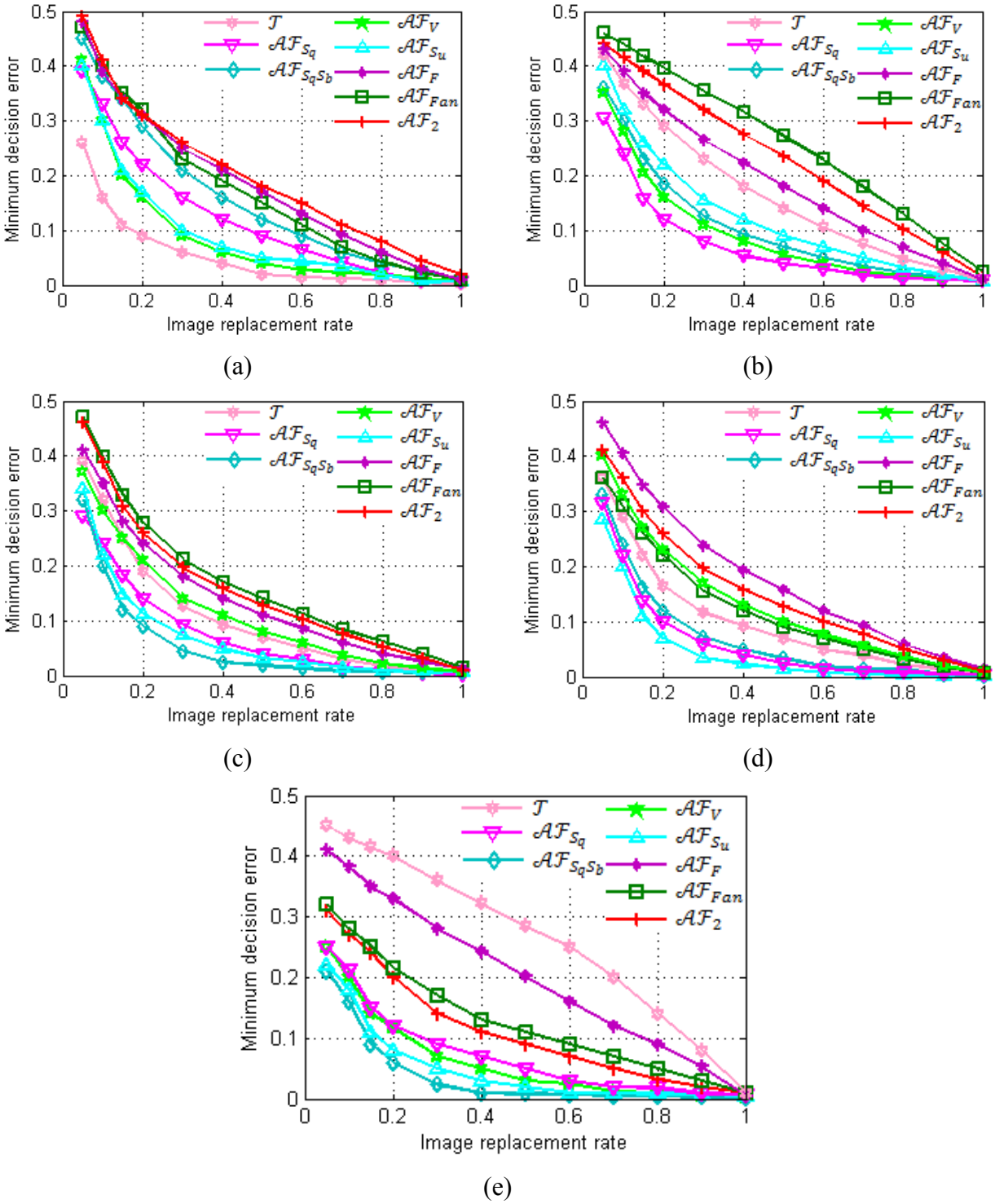


Figure 5.7: Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors on UCID dataset, under worst-case scenario (a) K_{Li}^{S100} [99], (b) K_{AR}^{S10} [104], (c) K_{SPAM}^{S686} [28], (d) K_{SRM}^{S714} [29], (e) K_{CM} (Proposed scheme).

Figure 5.7 shows the minimum decision error on the basis of image replacement rate against various anti-forensic techniques, under worst-case scenario. The proposed approach K_{CM} outperforms the existing forensic detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} by giving smaller minimum decision error values against various anti-forensic techniques shown in Figure 5.7. It is worth noting that the proposed technique is not very convincing in the case of original JPEG decompressed images. This may be due to the fact that the proposed scheme is designed in order to target the anti-forensically processed JPEG images by considering the weaknesses of the various anti-forensic schemes. For instance, most of the JPEG anti-forensic approaches apply TV-based minimization operation based on horizontal and vertical directions. Therefore, the diagonal variance is analyzed in the first stage of the proposed scheme to highlight the unwanted grainy noise effects. The motive of the proposed scheme is to detect the anti-forensically processed images and in that case the proposed scheme works efficiently. The JPEG forgery created by $\mathcal{AF}_F$ outperforms the anti-forensic schemes $\mathcal{AF}_{Fan}$ and $\mathcal{AF}_2$ in terms of forensic undetectability. This happens because the JPEG anti-forensic techniques $\mathcal{AF}_{Fan}$ and $\mathcal{AF}_2$ employ explicit DCT histogram smoothing to create JPEG forgeries. This smoothing leads to further modification in the image statistics. In the case of existing SVM-based detectors, the anti-forensic scheme $\mathcal{AF}_{Fan}$ provides high minimum decision error at the replacement rate of 0.10. Therefore, one can securely create a forgery by replacing 112×160 block in the UCID dataset images of size 384×512. Numerous kinds of forgeries can be created by replacing the block of size 112×160, for instance, the forger can easily replace the head of one person in the image. Although, it is a very difficult task for the anti-forensic techniques to fool the machine learning detectors when trying to disguise the complete JPEG image as uncompressed. The JPEG anti-forensics still remarkably applied in numerous situations such as image splicing and hiding DJPG compression traces. However, the efficacy of the suggested counter JPEG anti-forensic scheme is enhanced by providing relatively small minimum decision error against all the anti-forensic methods except $\mathcal{AF}_F$ at all the replacement rates including 0.10 as revealed in Figure 5.7 (e). In the case of projected forensic technique, the anti-forensic approach $\mathcal{AF}_F$ provides higher minimum decision error values as compared to the advanced $\mathcal{AF}_{Fan}$ and $\mathcal{AF}_2$ techniques. This is due to the employment of explicit histogram smoothing in $\mathcal{AF}_{Fan}$ and $\mathcal{AF}_2$.

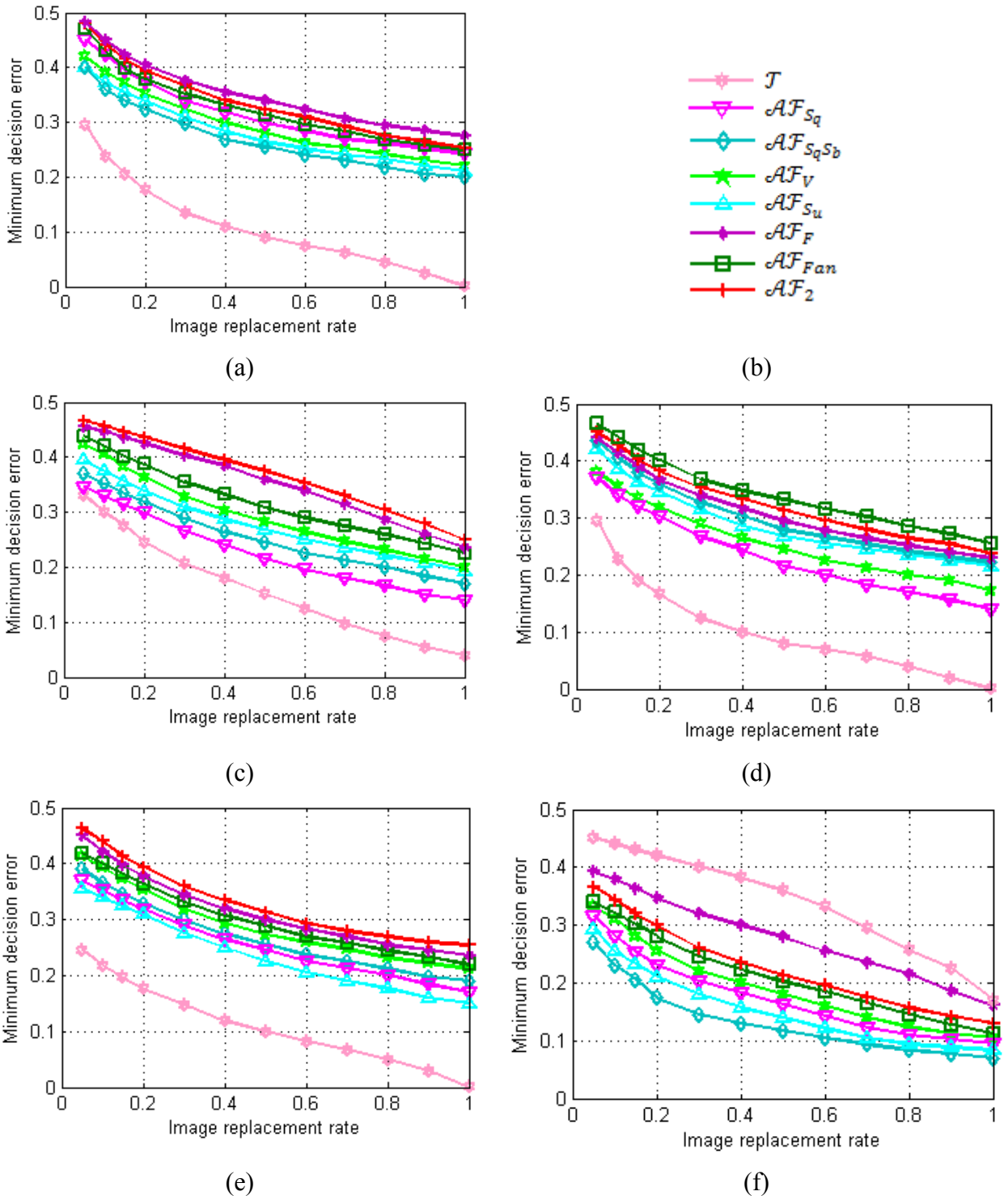


Figure 5.8: Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors on UCID dataset, under optimistic scenario (a) K_{Li}^{S100} [99], (b) Legends (Note that legends are provided separately due to lack of space), (c) K_{AR}^{S10} [104], (d) K_{SPAM}^{S686} [28], (e) K_{SRM}^{S714} [29], (f) K_{CM} (Proposed scheme).

The further analysis is performed based on the optimistic testing scenario. Figure 5.8 illustrates the minimum decision error on the basis of image replacement rate by considering various anti-forensic approaches against various SVM-based forensic detectors. Figure 5.8 shows that the recommended counter JPEG anti-forensic scheme performs better in comparison to the existing schemes by providing small minimum decision error values for the different values of image replacement rate against various anti-forensic techniques except for the JPEG forgery $\mathcal{AF}_F$. The proposed counter anti-forensic method has the capacity to detect even the advanced anti-forensic approaches $\mathcal{AF}_{Fan}$ and $\mathcal{AF}_2$ as shown in Figures 5.7 and 5.8. This happens because of the proposed higher-order statistical analysis of the DCT coefficients based on CM which is responsible for the detection of JPEG anti-forensics artifacts. Thus, the proposed method outperforms the existing schemes in terms of forensic detectability. Note that the detection of errors for JPEG compressed images and JPEG forgeries in Figures 5.7 and 5.8 are different due to the different training settings in the worst-case and optimistic scenarios. Furthermore, Table 5.1 provides the comparative analysis of various SVM-based forensic detectors in terms of average percentage accuracies achieved against various JPEG anti-forensic techniques. The training and testing process is repeated 10 times to obtain the average percentage accuracies. It is observed that the proposed scheme provides better percentage accuracies against all the considered anti-forensic schemes except $\mathcal{AF}_F$.

Table-5.1: Comparison of different SVM-based forensic detectors in terms of average percentage accuracy against various JPEG anti-forensic techniques.

Forgeries / Detectors	$\mathcal{AF}_{S_q}$ [95]	$\mathcal{AF}_{S_qS_b}$ [96]	$\mathcal{AF}_V$ [37]	$\mathcal{AF}_{S_u}$ [101]	$\mathcal{AF}_F$ [38]	$\mathcal{AF}_{Fan}$ [39]	$\mathcal{AF}_2$ (Proposed scheme)
K_{Li}^{S100} [99]	71.74	66.85	81.35	78.54	54.97	51.53	50.24
K_{AR}^{S10} [104]	78.74	77.35	79.80	68.54	58.07	53.83	59.66
K_{GLF}^{S56} [139]	60.53	58.54	59.36	54.21	67.49	52.37	50.28
K_{LTP}^{S220} [140]	58.15	53.18	64.04	50.76	62.11	50.29	52.97
K_{MFRAR}^{S10} [141]	61.34	57.85	59.34	56.85	51.34	50.53	51.22
K_{SPAM}^{S686} [28]	84.33	81.45	82.53	83.48	78.59	77.84	76.15
K_{SRM}^{S714} [29]	91.53	87.45	92.25	90.79	**92.34**	91.28	89.24
K_{CM} (Proposed scheme)	**95.21**	**93.82**	**94.53**	**94.20**	91.03	**93.69**	**92.96**

5.2.2 Countering DJPG Anti-Forensics

In this section, the ability of suggested counter anti-forensic technique is further authenticated by conducting the test on anti-forensically processed DJPG compressed images. The various existing anti-forensic schemes are considered to compute the efficiency of the presented forensic approach and the existing state-of-the-art DJPG compression forensic detectors [75] and [36]. JPEG compression with quality factor QF_2 is employed in single compressed images, whereas DJPG compressed images are initially compressed with QF_1 and then again compressed with QF_2. Image cropping and alteration of content can happen between two compressions. The JPEG image compressed with QF_1 is processed by the existing anti-forensic techniques. The resultant JPEG forgery is either untouched, or undergoes cropping with a random grid shift, in accordance with the various testing situations. Lastly, the anti-forensic DJPG compressed image is created by compressing the forgery again with quality factor QF_2.

5.2.2.1 Countering Non-Aligned DJPG Compression Anti-Forensics

The presented counter anti-forensic scheme is further explored to counter the NA-DJPG compression anti-forensics. The DJPG compression with a non-aligned 8×8 grid results in the statistical modification in DCT coefficients of DC component [75]. An efficient threshold detector is suggested in [75] to measure the non-uniformity of integer periodicity map based on DC coefficients. The UCIDTest image is compressed with quality factor $QF_1$and then image cropping is performed by taking a random shift $(i, j) \neq (0, 0)$ with $0 \leq i, j \leq 7$. Afterwards, we again compress the cropped image with QF_2 providing NA-DJPG compressed image. The anti-forensic process is applied after the first compression with QF_1. Therefore, NA-DJPG dataset is created from the UCID images by selecting the first and second quality factor values such that QF_1 and $QF_2 \in \{50, 55, 60, 65, 70, 75, 80, 85, 90, 95\}$ for which different types of JPEG forgeries are created. Thus, NA-DJPG dataset is created by using the strategy of [75] from the UCIDTest dataset images. We consider approximately half of the UCIDTest dataset images by considering all the 100 combinations of (QF_1, QF_2) for forensic testing due to the high computation time required by anti-forensic scheme $\mathcal{AF}_2$.

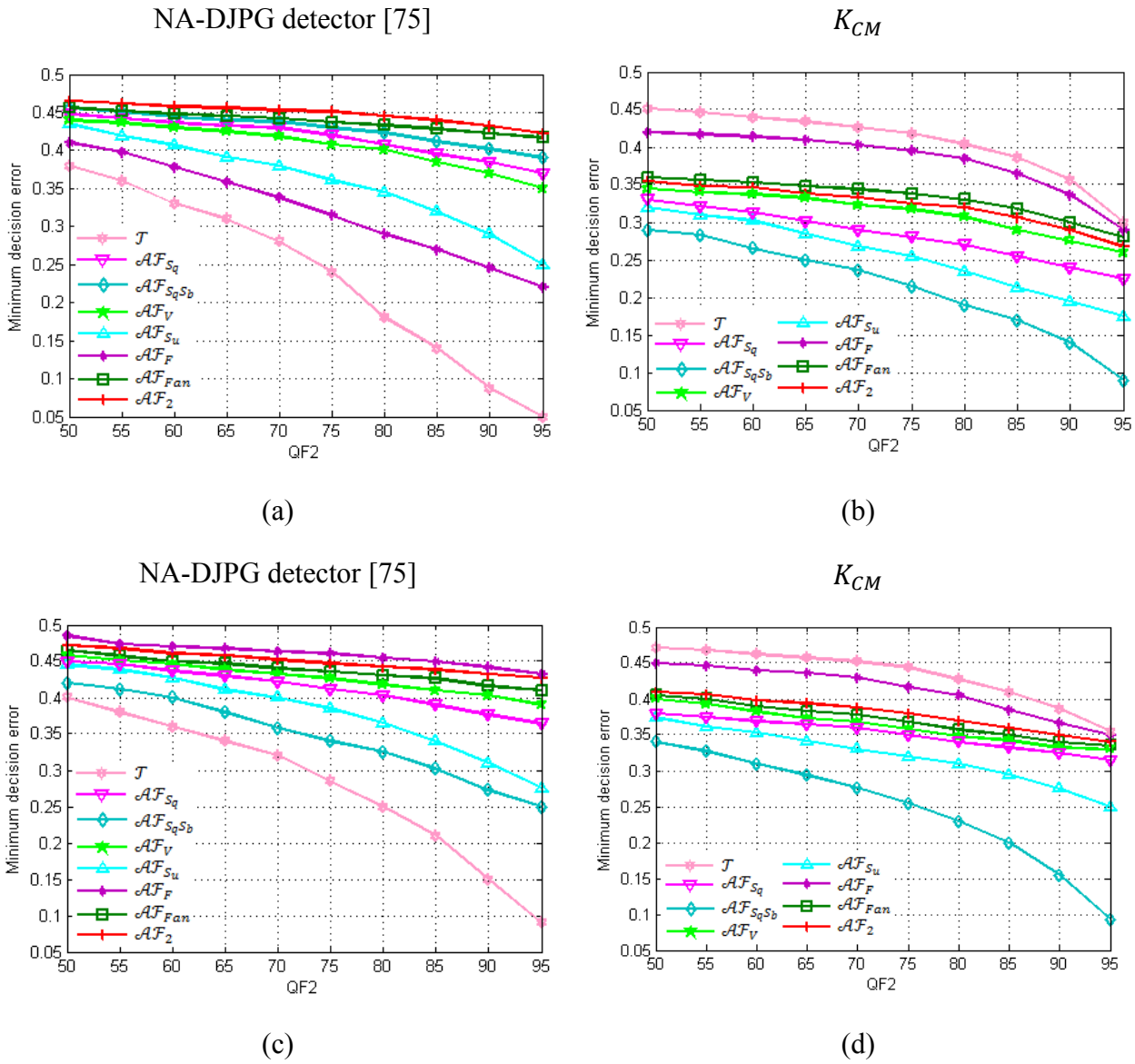


Figure 5.9: Comparison of NA-DJPG detector [75] and proposed scheme K_{CM} in terms of minimum decision error based on different QF_2 values against various types of forgeries, under worst (a), (b) and optimistic (c), (d) scenarios on UCIDTest dataset.

The testing of single JPEG compressed images and their equivalent (anti-forensic) DJPG compressed images is performed together by NA-DJPG detector [75] and proposed forensic detector. Afterward, the minimum decision error P_e is computed for different kinds of JPEG forgeries. The minimum decision error is averaged over the quality factor QF_1 under the fixed value of QF_2 as shown in Figure 5.9. It can be seen that the DCT histogram explicit smoothing of the anti- forensic schemes $\mathcal{AF}_{S_q}$ and $\mathcal{AF}_{S_qS_b}$ provides good forensic undetectability against the

NA-DJPG detector [75]. Many existing JPEG forensic detectors are successfully fooled by the JPEG anti-forensic technique [39]. The DJPG forgery created by $\mathcal{AF}_F$ can be exposed to certain amount by NA-DJPG detector [75]. The NA-DJPG detector [75] can be well fooled by the anti-forensic approach [39] with minimum decision error value closer to 0.5. This happens because NA-DJPG detector is unable to sense the integer periodicity. This proves the necessity of a second order statistical analysis for countering the JPEG anti-forensics. Moreover, the partially filled gaps in DCT domain might be exposed by the presented counter anti-forensic approach. The proposed forensic scheme K_{CM} outperforms the existing double compression forensic technique [75] against the various anti-forensic schemes in terms of small minimum decision error values for different values of QF_2, under the worst and optimistic scenarios as shown in Figure 5.9. However, the proposed counter JPEG anti-forensic scheme has less effect on the performance of anti-forensic method $\mathcal{AF}_F$ as shown in Figure 5.9.

5.2.2.2 Countering Aligned DJPG Compression Anti-Forensics

The detection of A-DJPG anti-forensics is also of great significance in forensic examination. Pevný and Fridrich [36] generated a 144-dimensional feature vector from low-frequency DCT histograms. This feature vector is fed to SVM for the categorization of single and DJPG compressed images. To construct the feature vector, Penvy and Fridrich consider 9 low-frequency AC sub-bands and then they compute a 16-bin histogram for each of the considered low-frequency sub-band. The UCIDTrain images are compressed with QF_1 and then compressed second time with quality factor QF_2, where $QF_2 \neq QF_1$ to create the dataset of A-DJPG compressed images. Therefore, in this case there are 90 combinations for which various kinds of JPEG forgeries are created by considering half of the UCIDTest dataset images. Figure 5.10 demonstrates that the presented counter JPEG anti-forensic approach provides better minimum decision error values as compared to the A-DJPG forensic detector [36] against most of the existing anti-forensic schemes, when tests are conducted under the worst and optimistic scenarios.

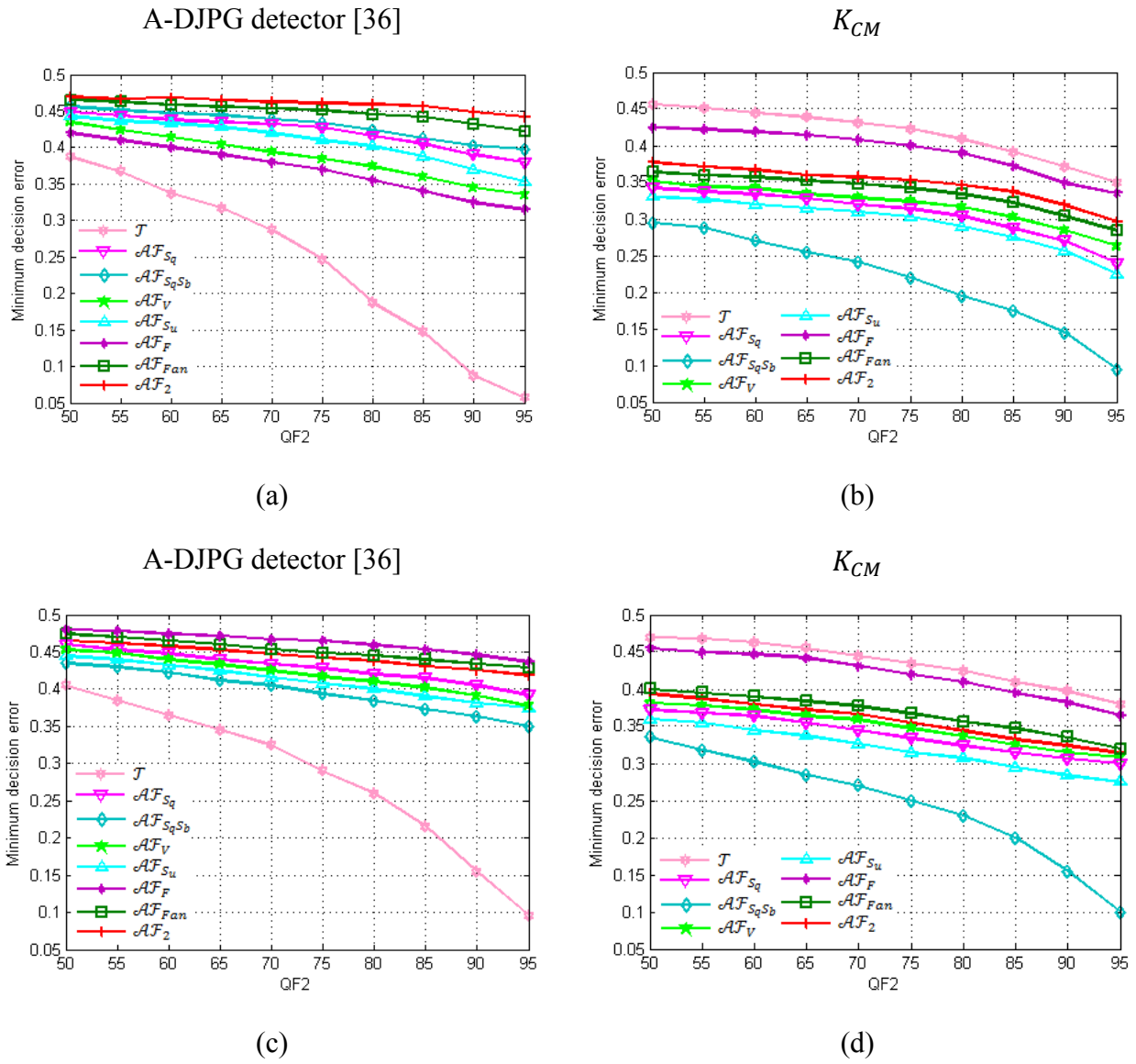


Figure 5.10: Comparison of A-DJPG detector [36] and proposed scheme K_{CM} in terms of minimum decision error based on different QF_2 values against various types of forgeries, under the worst (a), (b) and optimistic (c), (d) scenarios on UCIDTest dataset.

5.2.3 Experiment Results Obtained on Bossbase Dataset

The effectiveness of suggested counter anti-forensic technique is further confirmed by performing a test on BOSSBase image dataset. Figures 5.11 and 5.12 show the minimum decision error values under worst and optimistic scenarios respectively for different kinds of JPEG forgeries created from BOSSBase dataset at various image replacement rates against SVM-based detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686}, K_{SRM}^{S714}, and K_{CM}.

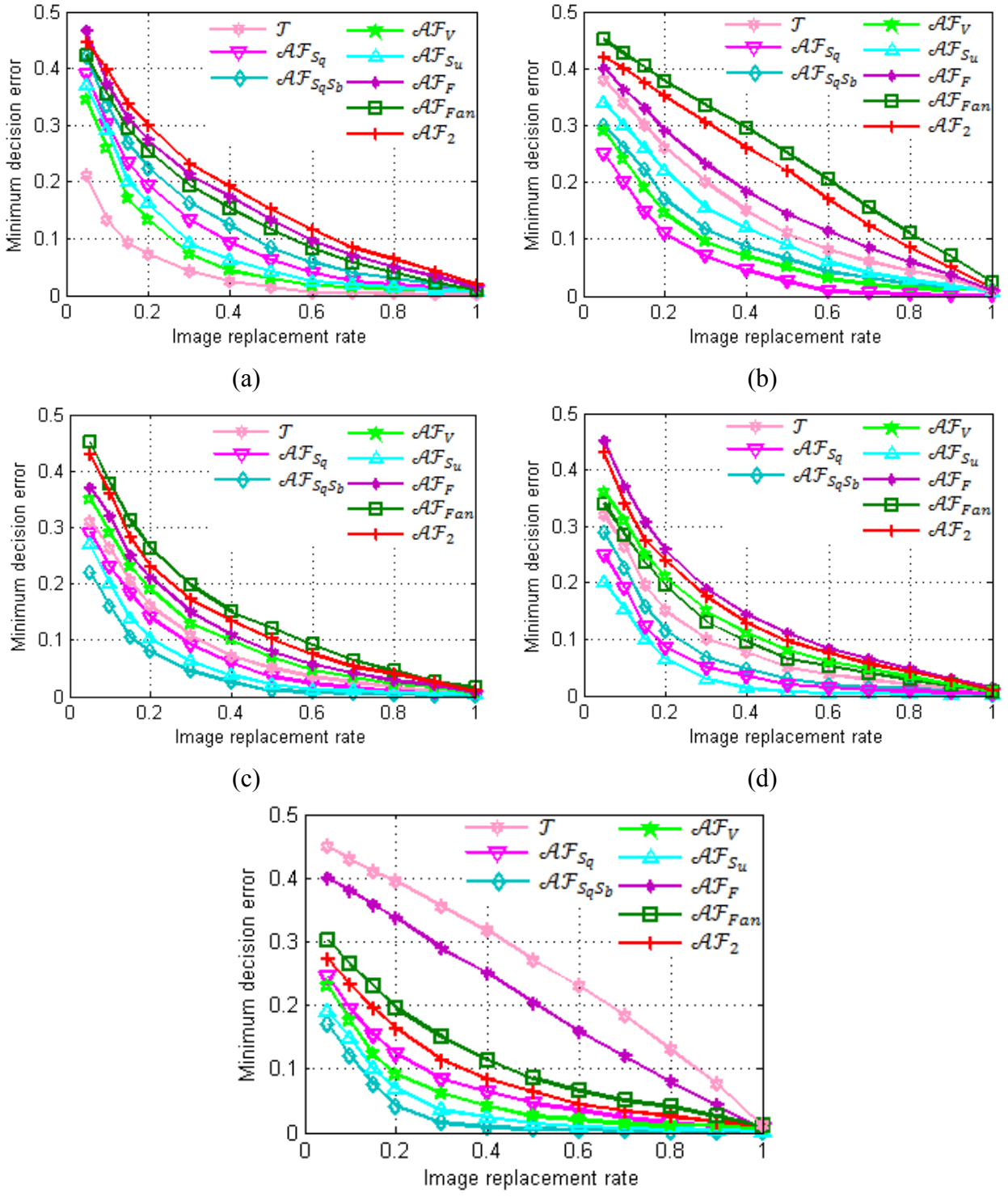


Figure 5.11: Performance of different SVM-based detectors based on minimum decision error as a function of image replacement rate against different forgeries on BOSSBase dataset, under worst-case scenario (a) K_{Li}^{S100} [99], (b) K_{AR}^{S10} [104], (c) K_{SPAM}^{S686} [28], (d) K_{SRM}^{S714} [29], (e) K_{CM} (Proposed scheme).

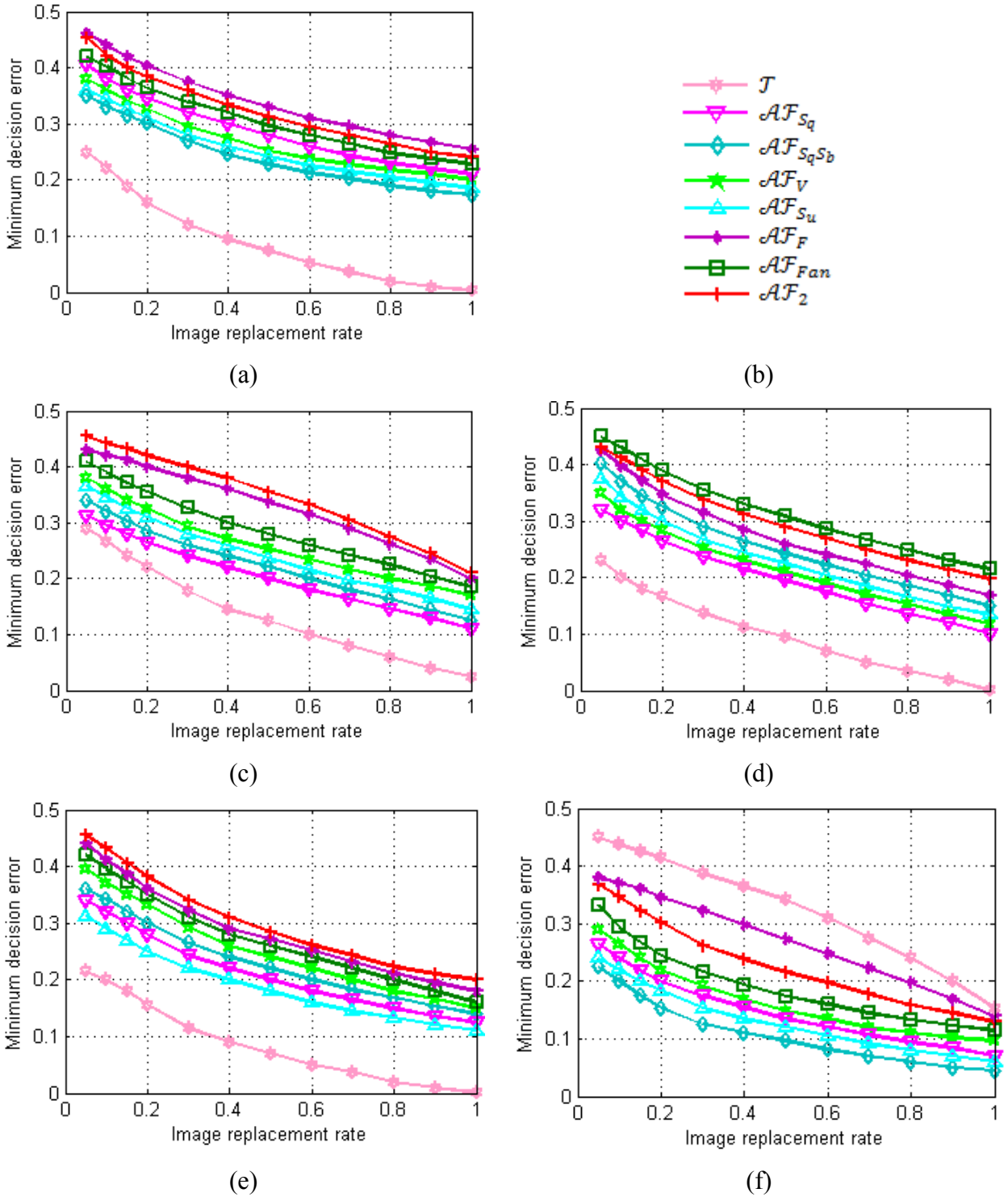


Figure 5.12: Performance of different SVM-based detectors based on minimum decision error as a function of image replacement rate against different forgeries on BOSSBase dataset, under optimistic scenario (a) K_{Li}^{S100} [99], (b) Legends (Note that legends are provided separately due to lack of space), (c) K_{AR}^{S10} [104], (d) K_{SPAM}^{S686} [28], (e) K_{SRM}^{S714} [29], (f) K_{CM} (Proposed scheme).

The experiment results of Figures 5.11 and 5.12 are similar to a great extent with the results obtained on UCID dataset. Our proposed detector K_{CM} outperforms the existing forensic detectors by successfully detecting all considered JPEG forgeries except $\mathcal{AF}_F$ forgery. Moreover, the SVM classifier is less sensitive to the problem of the curse of dimensionality [142]. Therefore, the number of dataset images has smaller effect on the efficiency of SVM classifier. The stable performance of proposed scheme is confirmed by the fact that minimum decision error values attained by the BOSSBase dataset under worst and optimistic scenarios are almost at the same level as that of the UCID dataset images.

5.3 Summary

In this chapter, a counter JPEG anti-forensic scheme is presented by considering the second-order statistical analysis based on CMs. The proposed scheme is based on the fact that dithering operation of JPEG anti-forensic techniques introduces unnatural noise in the resultant image. This unnatural noise produces variance inconsistencies. The CM-based second-order statistical feature captures these inconsistencies efficiently. The experiment results confirm that the presented approach outperforms the existing schemes in countering various JPEG anti-forensic approaches by providing smaller values of minimum decision error. In the next chapter, the presented counter JPEG anti-forensic technique is further investigated to discover its applications for other image processing operations.

CHAPTER 6

MULTI-PURPOSE COUNTER JPEG ANTI-FORENSICS

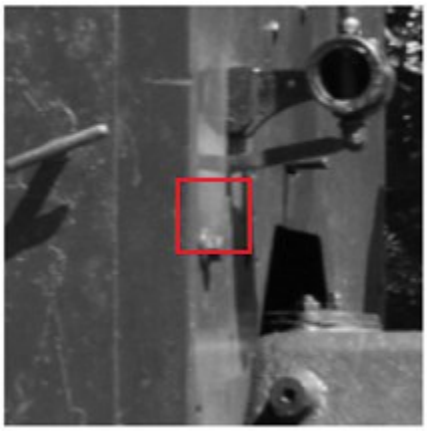
In this chapter, the counter JPEG anti-forensic technique presented in the last chapter is further examined to find its applications in the detection of various anti-forensic techniques of Median filtering and CE. The multi-purpose nature of the proposed method is confirmed from the extensive experimental results under both worst-case and optimistic scenarios. The proposed counter JPEG anti-forensic scheme provides better results as compared to the existing techniques against the anti-forensic schemes based on Median filtering and CE. Moreover, the proposed counter JPEG anti-forensic scheme outperforms the existing techniques by providing improved average percentage accuracies against various image processing operations such as Mean filtering, Gaussian filtering, Wiener filtering, Scaling, and Rotation.

6.1 Analysis of Image Processing and Anti-Forensic Operations

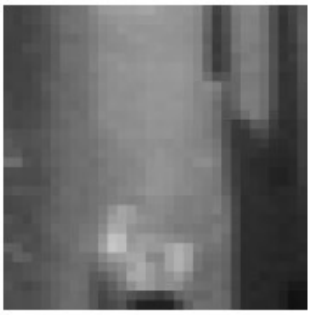
The various image processing operations are explored in this section to analyze the introduced artifacts in the resultant image. The multi-purpose nature of the proposed counter JPEG anti-forensic technique based on the second-order statistical analysis of CMs is revealed from the fact that it is capable of detecting these footprints competently.

6.1.1 Pixel Modification based on Different Image Processing Operations

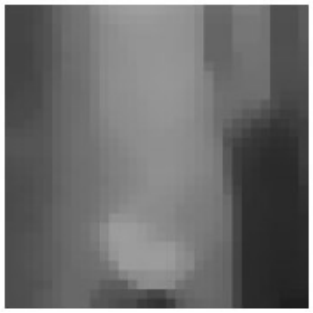
A universal forensic approach is desired in order to detect the various image processing operations. This forensic approach should be alone capable of capturing the footprints left during the various image processing operations rather than the footprints related to a particular image operation. The application of various image processing operations results in the modification of several pixel values. The modification levels are high for some image operations and it is perceived from the analysis of these operations that more than 70% of the pixel values are changed [29]. The image visual quality of the resultant images obtained from these operations decreases significantly due to this pixel values modification. Figure 6.1 shows the patches processed with different image processing and anti-forensic operations. The inherent image statistics modification can be observed from these different patches.



(a) Original image



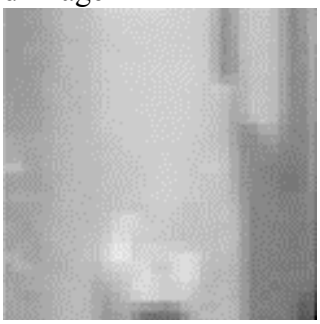
(b) Patch from the original image



(c) Median filtered image

(d) MF anti-forensically processed image

(e) CE image



(f) CE anti-forensically processed image

Figure 6.1: (a) Original image and (b) Patch extracted from the original image. Patches processed with different image processing operations such as (c) Median filtering, (d) Median filtering anti-forensics, (e) CE image, (f) CE anti-forensics.

In the original images, the neighboring pixel values and frequency coefficients are strongly correlated in nature. This correlation gets disturbed due to the modification of pixel or coefficient values introduced by the application of certain image processing operation. Therefore, it is a difficult task to preserve the inherent correlations after the modification of pixel values. It is also noted that different image processing operations alter the original image in different ways and strengths. The manipulated and original images can be distinguished easily through the proper measurement of these correlations in order to recognize the category of image processing operation.

6.2 Applications of Proposed Counter Anti-Forensic Technique

This section is devoted to evaluate the performance of suggested counter JPEG anti-forensic scheme against different types of anti-forensic schemes and image processing operations in order to validate its multi-purpose nature.

6.2.1 Countering Anti-Forensics of Median Filtering

Median filtering is often applied by the counterfeiters to cover the traces of JPEG compression. The traces initiated by the median filtering are further concealed by the median filtering anti-forensics. It is essential that the footprints removal effects of the filtering firstly employed should not be impaired by anti-forensics of median filtering. Now, we analyze the capability of our presented forensic approach against the anti-forensics of median filtering.

Chen *et al.* [139] proposed an efficient median filtering detection feature on the basis of statistical analysis of pixel value difference domain. The combination of global probability feature vector h^{GPF} and local correlation feature vector h^{LCF} results in Global and Local Feature (GLF) vector h^{GLF}. The global probability feature vector h^{GPF} is created on the basis of the fact that empirical cumulative distribution in the pixel value difference domain varies noticeably among original, average filtered and Median Filtered (MF) images. MF image has a relatively different intrinsic characteristic for the adjoining difference pair correlation. This observation is the motivation behind the construction of h^{LCF}. Later, the median filter residual is analyzed based on the autoregressive model and the extracted coefficients constitute the Median Filter Residual Autoregressive Feature (MFRAR) [141]. This MFRAR feature provides better results with low dimensionality. Furthermore, the median filtering is examined by Zhang *et al.* [140] by

considering the angle of micro-texture structure based on the local ternary and derivative pattern. The kernel PCA process is engaged to decrease the dimensionality of Median Filter Local Ternary Patterns (MFLTP) feature. Also, this dimensionality reduction does not affect the efficiency of the forensic detector.

In this analysis, the JPEG compressed image $\mathcal{T}$ obtained from the UCID dataset is median filtered with most commonly used square window of size 3×3, which results in $\mathcal{M}_{\mathcal{T}}$ image. Afterward, different MF forgeries $\mathcal{AF}_{Wu}$ [27], $\mathcal{AF}_{Dang}$ [143], and $\mathcal{AF}'_{Fan}$ [119] are obtained from the $\mathcal{M}_{\mathcal{T}}$ image. The anti-forensic technique $\mathcal{AF}_{Wu}$ is based on the modification of pixel difference distribution using anti-forensic noise. Another median filtering anti-forensic technique $\mathcal{AF}_{Dang}$ is based on the addition of noise signal to disguise the median filtering forensic detectors. In this method, the image is initially distributed into non-overlapping blocks. Afterward, the moderately complex blocks with variances larger than a particular threshold are exposed to a major noise attack. The complex block is dithered with random noise equally dispersed in $[-7,-3] \cup [3,7]$. Finally, the random noise equally dispersed in [0, 1] is used to attack the entire image. The anti-forensic technique $\mathcal{AF}'_{Fan}$ is based on the TV energy minimization problem. This method is analogous to the JPEG anti-forensic scheme suggested in [39]. Inspired by [144], this approach is based on an image variational deconvolution problem. The training and testing datasets of MF anti-forensic images are generated from the UCID dataset by using the similar strategy as used in the case of JPEG forgeries. The various median filtering forensic detectors are denoted as follows:

- K_{GLF}^{S56}, represents the detector based on the statistical analysis of pixel value difference domain [139].
- K_{MFRAR}^{S10}, autoregressive feature based forensic detector [141].
- K_{LTP}^{S220}, denotes the detector based on MFLTP feature [140].

Figures 6.2 and 6.3 show that the proposed counter anti-forensic approach provides better minimum decision error values as compared to the existing median filtering forensic detectors against most of the existing anti-forensic schemes, in both worst and optimistic scenarios. Note that the capability of suggested scheme is superior in detecting the MF images $\mathcal{M}_{\mathcal{T}}$ as compared to the JPEG decompressed images $\mathcal{T}$ due to the application of median filtering in the case of $\mathcal{M}_{\mathcal{T}}$.

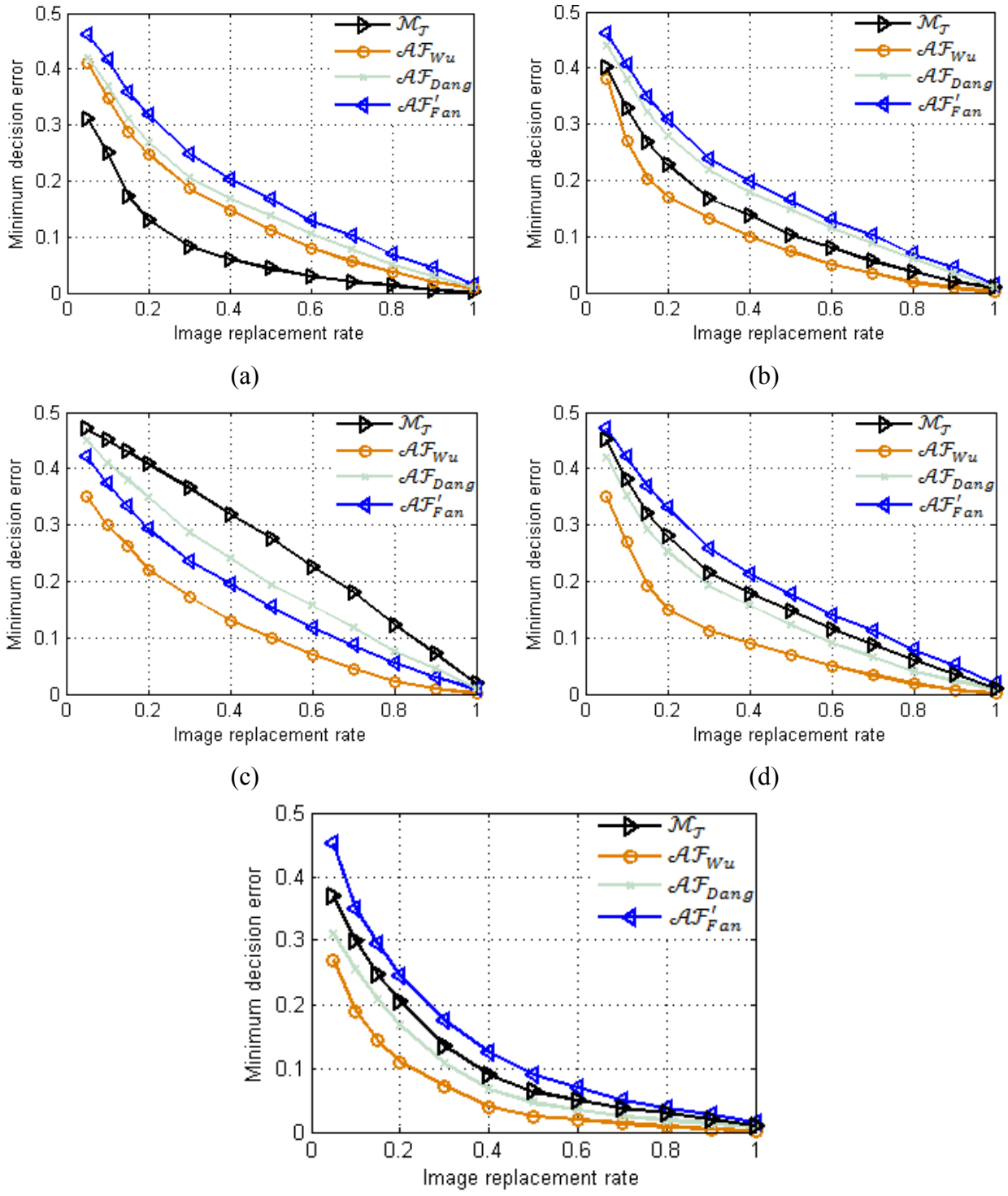


Figure 6.2: Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors on UCID dataset, under worst-case scenario (a) K_{SPAM}^{S686} [28], (b) K_{GLF}^{S56} [139], (c) K_{MFRAR}^{S10} [141], (d) K_{LTP}^{S220} [140], (e) K_{CM} (Proposed scheme).

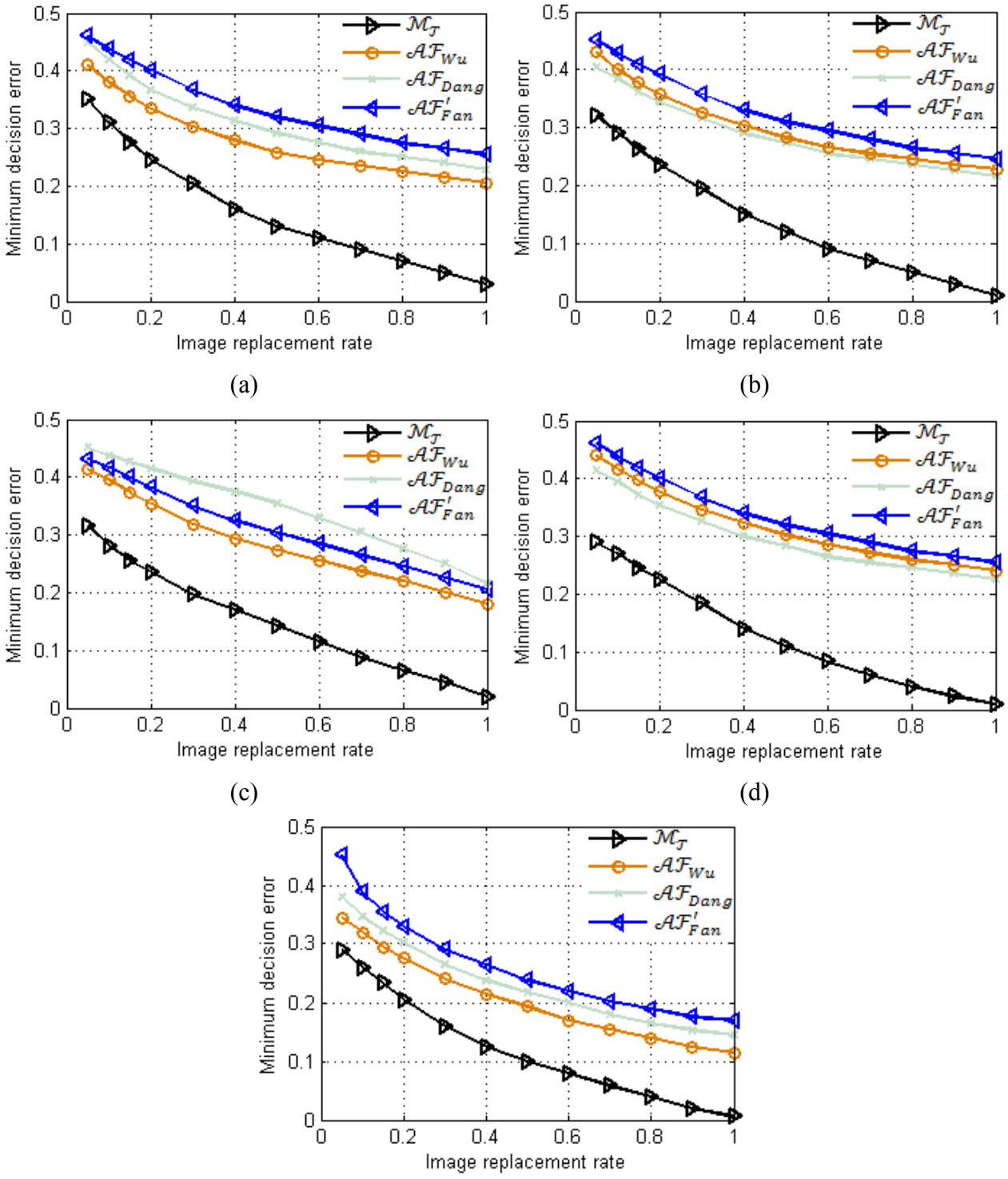


Figure 6.3: Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors on UCID dataset, under optimistic scenario (a) K_{SPAM}^{S686} [28], (b) K_{GLF}^{S56} [139], (c) K_{MFRAR}^{S10} [141], (d) K_{LTP}^{S220} [140], (e) K_{CM} (Proposed scheme).

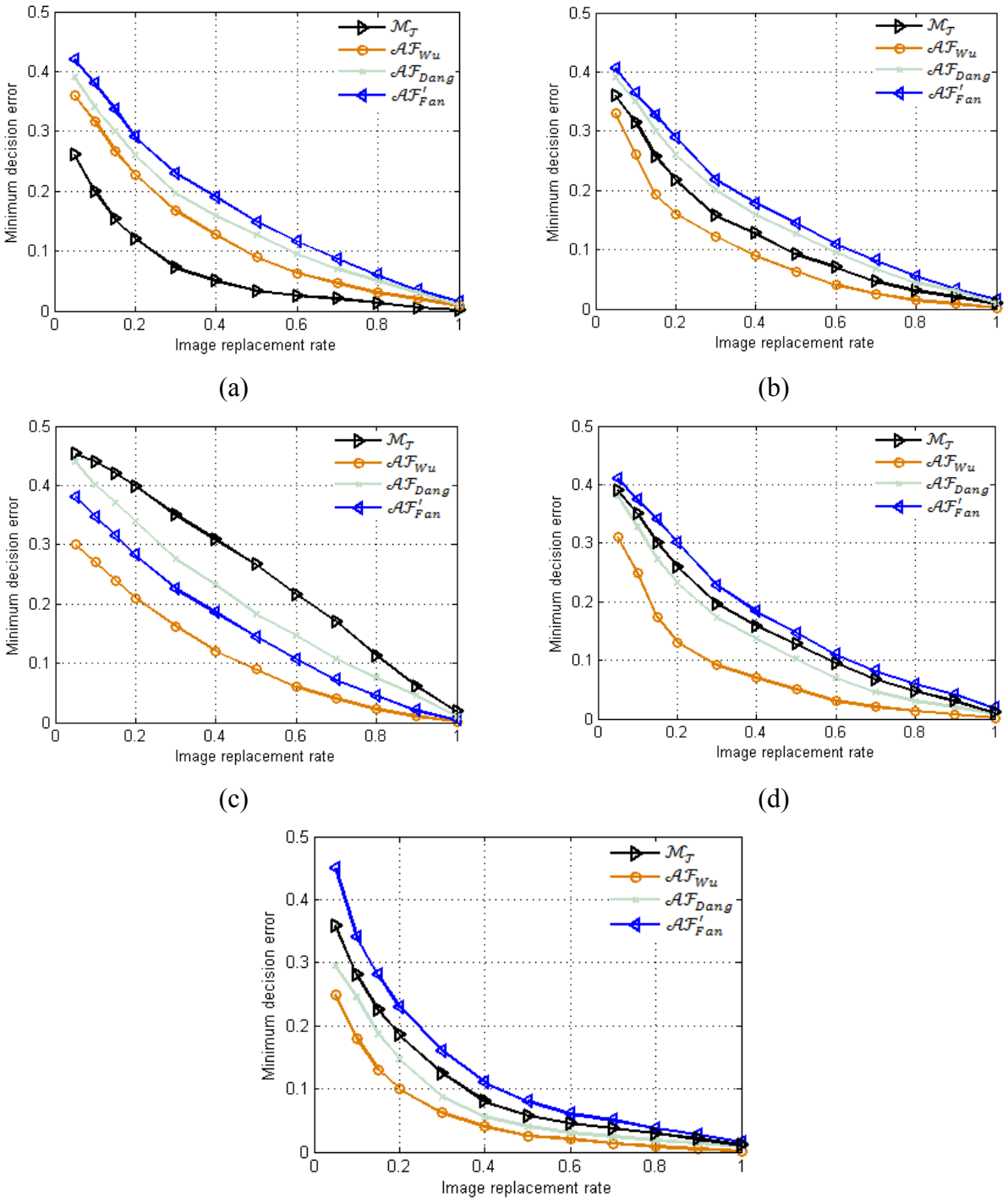


Figure 6.4: Comparison of different SVM-based detectors based on minimum decision error as a function of image replacement rate against different forgeries on BOSSBase dataset, under worst-case scenario (a) K_{SPAM}^{S686} [28], (b) K_{GLF}^{S56} [139], (c) K_{MFRAR}^{S10} [141], (d) K_{LTP}^{S220} [140], (e) K_{CM} (Proposed scheme).

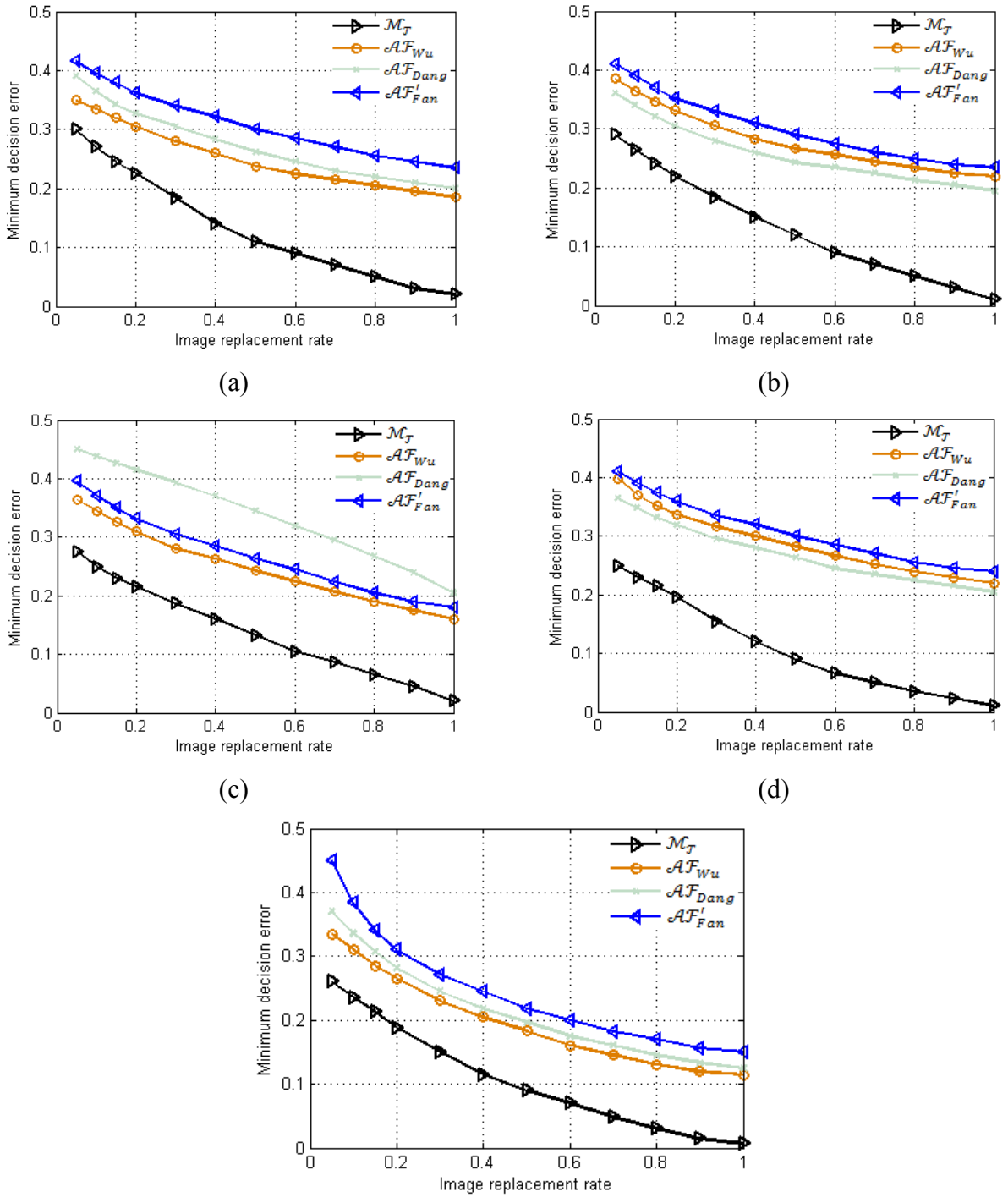


Figure 6.5: Comparison of different SVM-based detectors based on minimum decision error as a function of image replacement rate against different forgeries on BOSSBase dataset, under optimistic scenario (a) K_{SPAM}^{S686} [28], (b) K_{GLF}^{S56} [139], (c) K_{MFRAR}^{S10} [141], (d) K_{LTP}^{S220} [140], (e) K_{CM} (Proposed scheme).

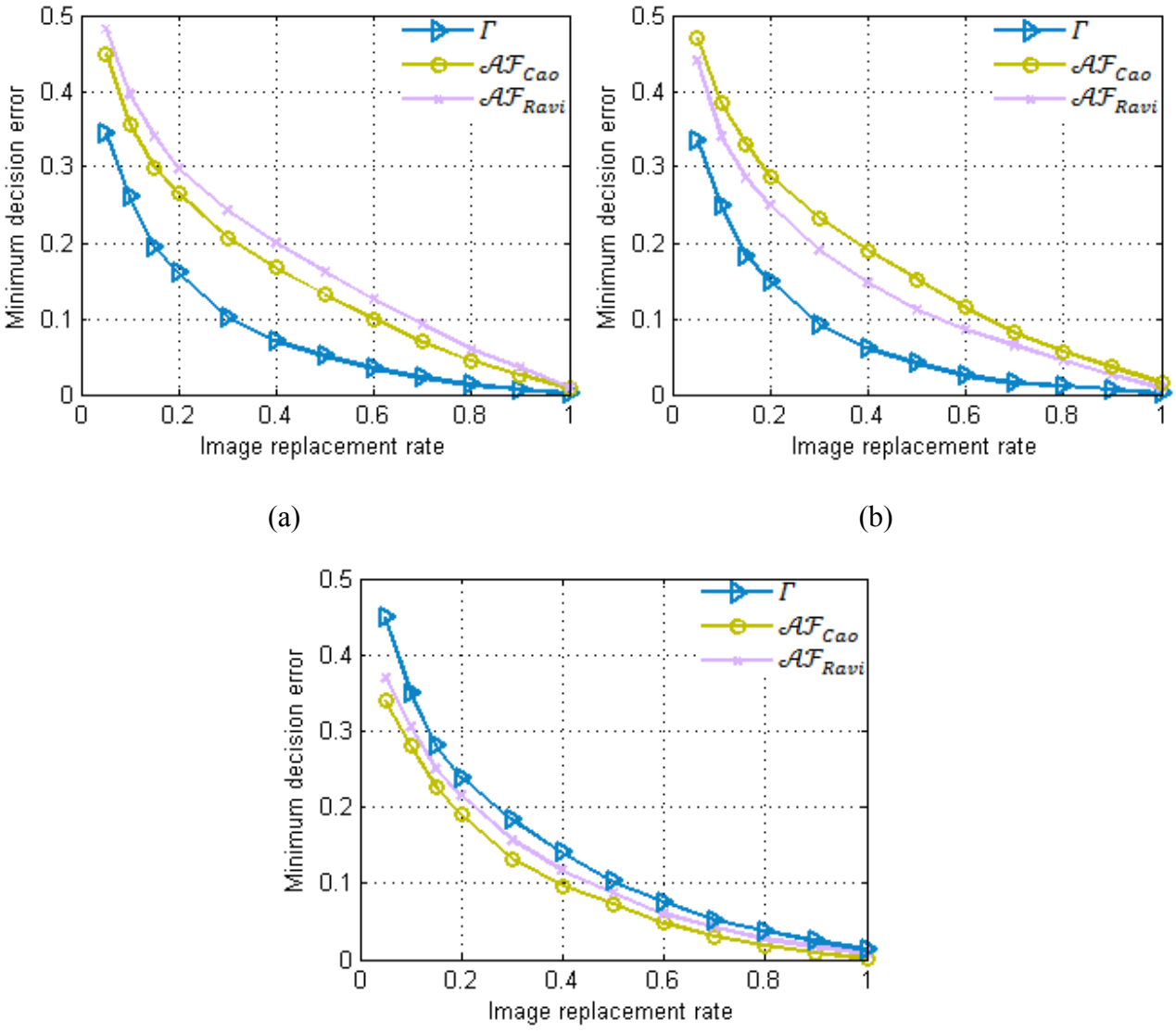
The proposed counter JPEG anti-forensic scheme is further evaluated by conducting tests on BOSSBase dataset images. Figures 6.4 and 6.5 provide the minimum decision error values under worst-case and optimistic scenario respectively for different MF forgeries against the SVM-based detectors K_{SPAM}^{S686}, K_{GLF}^{S56}, K_{MFRAR}^{S10}, K_{LTP}^{S220}, and K_{CM}, when test is performed on BOSSBase images. The proposed counter JPEG anti-forensic technique performs better as compared to the existing forensic schemes by providing smaller minimum decision error values against all the considered median filtering forgeries, when tested on BOSSBase dataset. Therefore, the proposed counter JPEG anti-forensic approach is also capable to counter the median filtering anti-forensic techniques by detecting the artifacts introduced during the median filtering anti-forensics. The experiment results shown in Figures 6.4 and 6.5 in terms of minimum decision error values on BOSSBase dataset are quite similar to the results obtained on UCID dataset. This is due to the reason that SVM classifier efficacy is not much affected by the number of dataset images. Moreover, the minimum decision error values obtained for BOSSBase and UCID datasets are almost at the same level under both worst-case and optimistic scenarios.

6.2.2 Countering CE Anti-Forensics

CE is a frequently used image enhancement operation by most of the photo editing softwares. The approaches related to CE forensics and anti-forensics have become popular in multimedia forensics. Now, the multi-purpose nature of the proposed scheme is further confirmed against the CE anti-forensic techniques.

The analysis provided in [29] reveals that it is a challenging task for any forensic detector to counter the CE anti-forensic techniques as compared to the JPEG compression and median filtering anti-forensic techniques. This is due to the direct modification of image histogram by the CE anti-forensic schemes. The CE operation with gamma value randomly selected from the set $\{0.6,\ 0.8,\ 1.2,\ 1.4\}$ is applied on UCID dataset images to create the contrast enhanced images represented by Γ. Afterward, these images are processed through CE anti-forensic techniques $\mathcal{AF}_{Cao}$ [145] and $\mathcal{AF}_{Ravi}$ [146] to create a dataset of CE anti-forensically processed images. The training and testing is realized by considering the UCID dataset in the similar manner as it is done in the case of JPEG and MF forgeries. The recommended counter anti-forensic scheme outperforms the forensic detection methods K_{SPAM}^{S686} and K_{SRM}^{S714} against various CE anti-forensic methods in terms of small minimum decision error values at most of the

considered replacement rates as shown in the Figures 6.6 and 6.7, under both worst-case and optimistic scenarios. It is worth noting that larger the value of minimum decision error, better the forensic detector is fooled by the anti-forensic technique [147]. Therefore, it is confirmed that the proposed counter anti-forensic scheme is efficient in revealing the CE artifacts even in the presence of an anti-forensic attack.



(a) (b)

(c)

Figure 6.6: Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors on UCID dataset, under worst-case scenario (a) K_{SPAM}^{S686} [28], (b) K_{SRM}^{S714} [29], (c) K_{CM} (Proposed scheme).

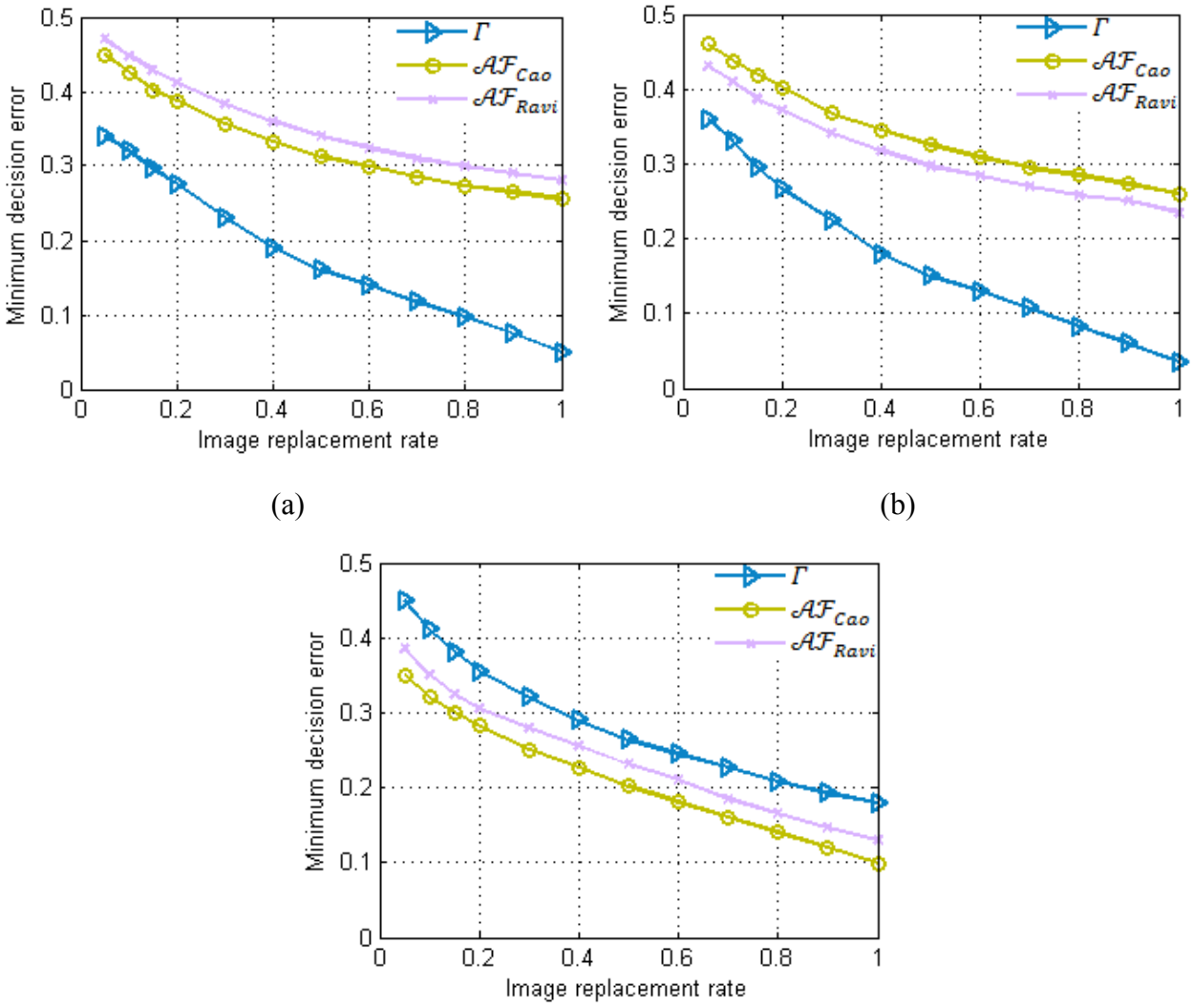


Figure 6.7: Minimum decision error based on various image replacement rates against different forgeries by considering SVM-based detectors on UCID dataset, under optimistic scenario (a) K_{SPAM}^{S686} [28], (b) K_{SRM}^{S714} [29], (c) K_{CM} (Proposed scheme).

The proposed approach is now evaluated based on the BOSSBase dataset images against various anti-forensic techniques of CE by considering various SVM-based forensic detectors K_{SPAM}^{S686}, K_{SRM}^{S714}, and K_{CM}. It is observed from Figures 6.8 and 6.9 that the proposed counter JPEG anti-forensic approach outperforms the existing techniques by providing smaller minimum decision error values based on different image replacement rates under both worst-case and optimistic scenarios. These small minimum decision error values obtained in the case of

proposed counter JPEG anti-forensic scheme signifies that the considered CE anti-forensic techniques are unable to properly hide the CE footprints. Moreover, the results obtained against CE anti-forensic techniques on BOSSBase dataset are comparable to the results obtained on UCID dataset, which is also the case with JPEG and MF forgeries. This is due to the fact that the performance of the SVM classifier is less affected by the number of images in the dataset.

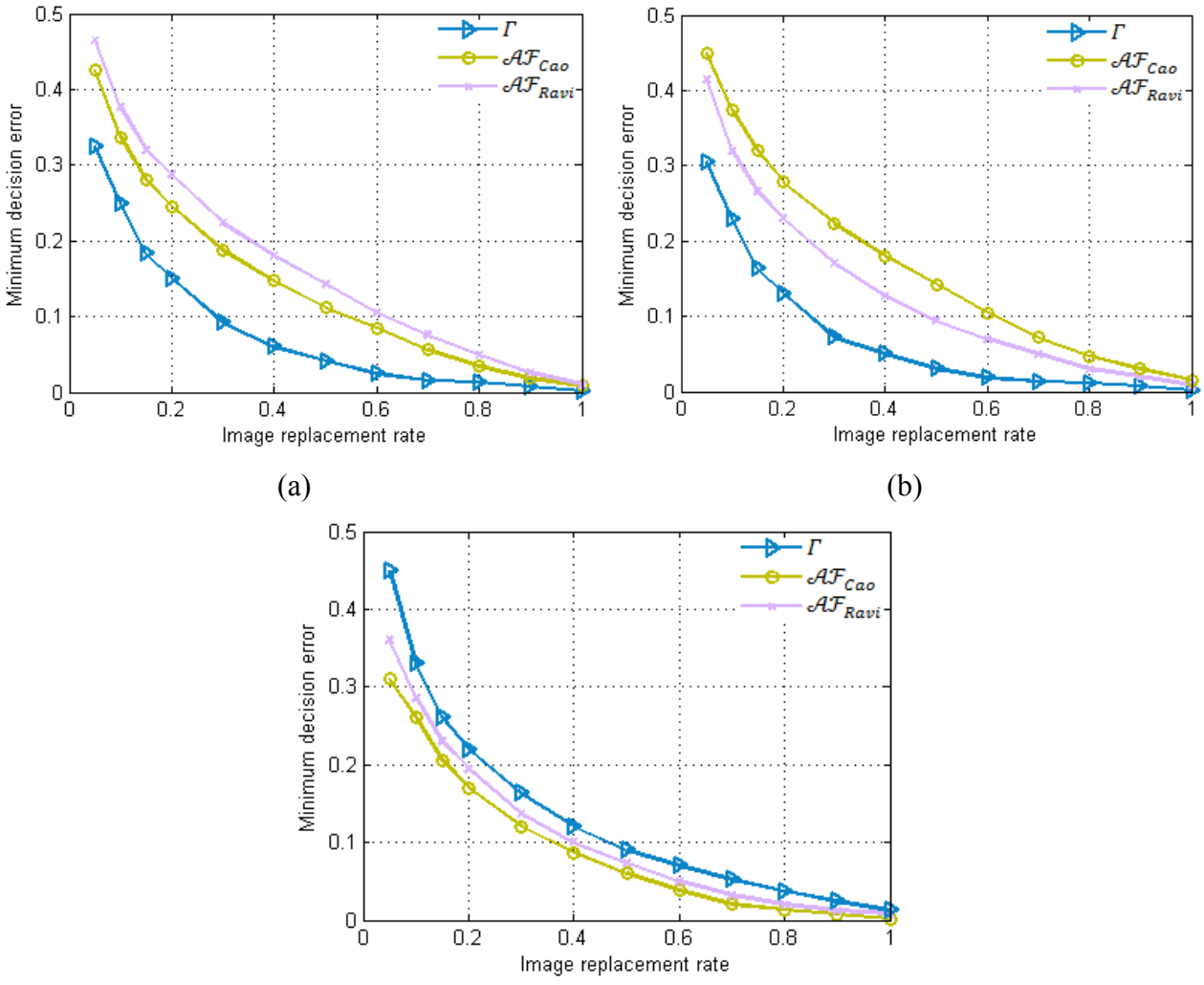


Figure 6.8: Performance of different SVM-based detectors based on minimum decision error as a function of image replacement rate against different forgeries on BOSSBase dataset, under worst-case scenario (a) K_{SPAM}^{S686} [28], (b) K_{SRM}^{S714} [29], (c) K_{CM} (Proposed scheme).

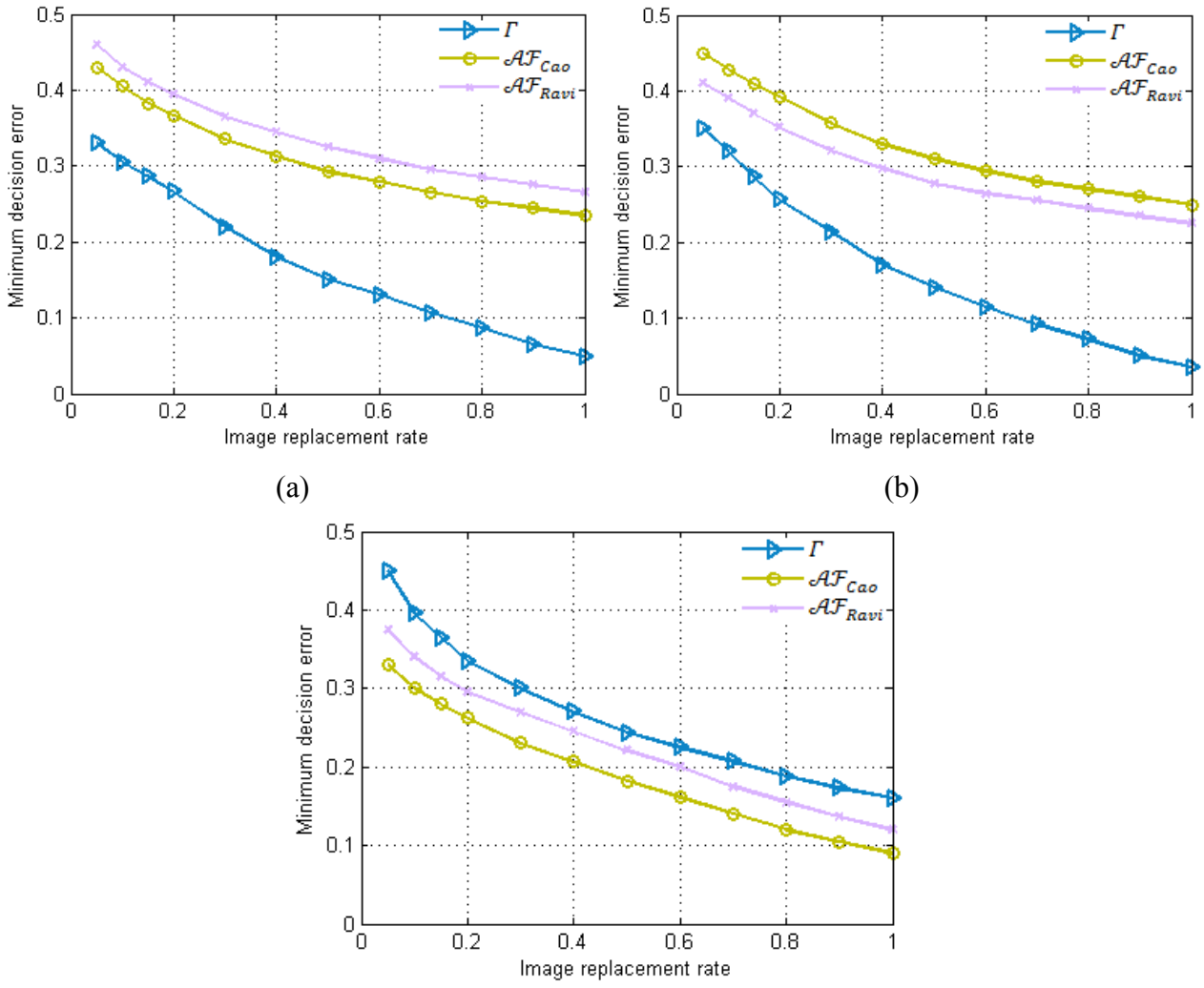


Figure 6.9: Performance of different SVM-based detectors based on minimum decision error as a function of image replacement rate against different forgeries on BOSSBase dataset, under optimistic scenario (a) K_{SPAM}^{S686} [28], (b) K_{SRM}^{S714} [29], (c) K_{CM} (Proposed scheme).

Table 6.1 provides the comparative analysis of the different SVM-based forensic methods in terms of average percentage accuracies against various anti-forensic techniques based on Median filtering and CE. The proposed counter JPEG anti-forensic technique also provides better average percentage accuracies as compared to the existing approaches against Median filtering and CE anti-forensics. The maximum average detection accuracy achieved by the proposed counter JPEG anti-forensic scheme is 94.27% against the median filtering anti-forensic scheme $\mathcal{AF}_{Wu}$ [27]. It can also be perceived from Table 6.1 that most of the existing forensic methods are designed by considering the special footprints of anti-forensic operations. Therefore, one

forensic method based on the particular type anti-forensic scheme may not be able to detect the other anti-forensic techniques.

Table-6.1: Comparison of different SVM-based forensic detectors in terms of average percentage accuracy against various anti-forensic techniques based on Median filtering and CE operations.

Forgeries / Detectors	Median filtering anti-forensics			CE anti-forensics	
	$\mathcal{AF}_{Wu}$ [27]	$\mathcal{AF}_{Dang}$ [143]	$\mathcal{AF}'_{Fan}$ [119]	$\mathcal{AF}_{Cao}$ [145]	$\mathcal{AF}_{Ravi}$ [146]
K_{Li}^{S100} [99]	58.08	55.17	53.95	52.84	50.88
K_{AR}^{S10} [104]	67.85	65.46	59.24	61.25	58.25
K_{GLF}^{S56} [139]	76.33	57.86	52.49	65.38	59.97
K_{LTP}^{S220} [140]	75.28	66.83	59.56	52.84	50.71
K_{MFRAR}^{S10} [141]	75.51	69.28	68.40	63.85	61.07
K_{SPAM}^{S686} [28]	80.49	79.36	76.08	75.93	73.05
K_{SRM}^{S714} [29]	91.65	90.25	87.95	86.14	82.25
K_{CM} (Proposed scheme)	**94.27**	**92.09**	**90.15**	**90.75**	**83.77**

6.2.3 Detection of Other Image Processing Operations

The proposed scheme has been further evaluated by considering the other image processing operations such as Mean filtering (MeanF), Gaussian filtering (GF), Wiener filtering (WF), Scaling (Sca), and Rotation (Rot). The SVM-based detectors are tested by performing the forensic testing on BOSSBaseTest dataset images and BOSSBaseTrain dataset images are used for training purposes. Different types of image processing operations are applied on these images in order to create the processed image datasets for evaluation.

6.2.3.1 Spatial Filtering Operations Detection

Mean, Gaussian, and Wiener filtering operations are the commonly used spatial filtering operations for the purpose of image enhancement. In many practical applications such as medical and satellite images, it is often required to boost the image visual quality by reducing the introduced noises. Therefore, in all these scenarios, spatial filtering operations have great importance.

Mean filtering is frequently employed for smoothing purposes *i.e.*, to reduce the noise in the considered image by decreasing the intensity variation between the one pixel and its subsequent. The idea behind the mean filtering is to substitute the particular pixel value with the average of its neighboring pixels falling inside the considered window.

Similarly, the Gaussian filter is also utilized to eliminate the unwanted noise in an image. This filter is also very much analogous to mean filter but works on different kernel. The standard deviation of the Gaussian determines the degree of smoothing. The Gaussian filtering operation for two-dimensional signal is represented as [148]:

$$G_{gaussian}(x', y') = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x'^2+y'^2}{2\sigma^2}} \tag{6.2.1}$$

where, σ denotes the standard deviation of the distribution.

Besides, the wiener filtering is exploited to reduce the overall mean square error in inverse filtering process and noise smoothing for the purpose of image restoration. It provides an optimum tradeoff among inverse filtering and noise smoothing and is defined as [149]:

$$W_{wiener}(f_1', f_2') = \frac{H^*_{filter}(f_1', f_2') S_{xx}(f_1', f_2')}{\left|H_{filter}(f_1', f_2')\right|^2 S_{xx}(f_1', f_2') + S_{\eta\eta}(f_1', f_2')} \tag{6.2.2}$$

where, $S_{xx}(f_1', f_2')$ and $S_{\eta\eta}(f_1', f_2')$ denote the power spectrum of original image and additive noise respectively. $H_{filter}(f_1', f_2')$ represents the blurring filter and its complex conjugate is denoted by $H^*_{filter}(f_1', f_2')$.

These various types of filtering operations are frequently used by the counterfeiters to disguise the forensic detectors by hiding the footprints or inconsistencies introduced during the image tampering. For evaluation purposes, the BOSSBase dataset images are processed with Mean, Gaussian, and Wiener filtering operations with a usually used window of sizes 3×3 and 5×5. Tables 6.2 and 6.3 show the average percentage accuracies obtained by the various considered forensic detectors against different spatial filtering operations based on different window sizes. The proposed counter JPEG anti-forensic approach provides enhanced average percentage accuracies as compared to the existing forensic techniques against different filtering operations.

It is also observed from Tables 6.2 and 6.3 that highest average percentage accuracies of 97.65% and 98.79% are obtained against the mean filtering operation by the proposed counter JPEG anti-forensic scheme. Moreover, the effectiveness of the proposed scheme increases in terms of average detection accuracies with the increase in window size as revealed from Tables 6.2 and 6.3. This happens because of the excess smoothing of processed images by these spatial filtering operations due to large window size.

Table-6.2: Average percentage accuracies in detecting different spatial filtering operations by considering the window of size 3×3.

Spatial filtering operations / Detectors	Mean Filtering (%)	Gaussian Filtering (%)	Wiener Filtering (%)
K_{Li}^{S100} [99]	64.57	80.57	79.24
K_{AR}^{S10} [104]	82.64	79.53	76.47
K_{GLF}^{S56} [139]	89.42	82.78	80.86
K_{LTP}^{S220} [140]	61.37	74.81	64.78
K_{MFRAR}^{S10} [141]	81.52	78.64	69.85
K_{SPAM}^{S686} [28]	88.26	86.67	88.17
K_{SRM}^{S714} [29]	93.75	92.07	91.79
K_{CM} (Proposed scheme)	**97.65**	**96.43**	**94.85**

Table-6.3: Average percentage accuracies in detecting different spatial filtering operations by considering the window of size 5×5.

Spatial filtering operations / Detectors	Mean Filtering (%)	Gaussian Filtering (%)	Wiener Filtering (%)
K_{Li}^{S100} [99]	66.28	83.64	83.56
K_{AR}^{S10} [104]	85.61	81.42	78.33
K_{GLF}^{S56} [139]	91.67	85.31	83.57
K_{LTP}^{S220} [140]	64.11	76.84	66.91
K_{MFRAR}^{S10} [141]	84.49	82.19	72.46
K_{SPAM}^{S686} [28]	92.56	90.75	92.81
K_{SRM}^{S714} [29]	95.83	94.18	94.58
K_{CM} (Proposed scheme)	**98.79**	**98.15**	**96.69**

6.2.3.2 Geometric Operations Detection

The image scaling and rotation are the geometric operations used to shrink or zoom and rotate respectively. These operations are used for geometric transformation of images based on the geometric coordinate transformations. Let $f'(w,z)$ represents the input image which is geometrically transformed to output image $g'(x,y)$ defined as [150]:

$$g'(x,y) = f'(T^{-1}\{(x,y)\}) \tag{6.2.3}$$

where, $T^{-1}\{.\}$ denotes the inverse transformation function. Therefore, these operations are considered as affine transformation which is defined as the mapping of image statistics from one vector space to another based on matrix multiplication/addition and translation.

The image scaling operation can be represented in the form of affine transformation with affine matrix (**T**) defined as [150]:

$$\mathbf{T} = \begin{bmatrix} s_x & 0 & 0 \\ 0 & s_y & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{6.2.4}$$

and equivalent coordinate equations are represented as:

$$x = s_x w \tag{6.2.5}$$

$$y = s_y z \tag{6.2.6}$$

Similarly, the affine matrix for image rotation operation is expressed as [150]:

$$\mathbf{T} = \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{6.2.7}$$

and corresponding coordinate equations are formulated as:

$$x = w\cos\theta - z\sin\theta \tag{6.2.8}$$

$$y = w\sin\theta + z\cos\theta \tag{6.2.9}$$

During the creation of image forgery, sometimes the image has gone through these scaling and rotation operations. Therefore, it is also important to investigate these geometric operations for the image authentication process. For the evaluation purposes, the scaling operation is performed on the BOSSBase dataset images which includes up and down-sampling in the range $\{1, 3, 5, 10, 20, 30, 40, 50, 60, 70, 80, 90\}$ (%) and $\{1, 3, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$ (%) respectively. Similarly, the rotation operation is performed on the BOSSBase images by considering the range $\{1, 3, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$ in degree as suggested in [29]. Table 6.4 provides the comparative analysis based on different geometric operations by considering the various detectors. The multi-purpose nature of the proposed scheme is confirmed by the fact that it also provides better average percentage accuracies in the detection of considered geometric operations. The proposed counter anti-forensic approach provides an average detection accuracy of 97.28% and 96.54% against the scaling and rotation operation respectively.

Table-6.4: Average percentage accuracies in detecting geometric operations.

Geometric operations / Detectors	Scaling (%)	Rotation (%)
K_{Li}^{S100} [99]	76.52	83.47
K_{AR}^{S10} [104]	68.72	72.68
K_{GLF}^{S56} [139]	77.69	82.17
K_{LTP}^{S220} [140]	76.28	65.46
K_{MFRAR}^{S10} [141]	67.59	74.41
K_{SPAM}^{S686} [28]	90.39	88.64
K_{SRM}^{S714} [29]	93.89	92.68
K_{CM} (Proposed scheme)	**97.28**	**96.54**

6.3 Summary

In this chapter, various applications of proposed counter JPEG anti-forensic technique are explored. Firstly, the various processed image datasets are generated by considering the anti-forensic techniques based on Median filtering and CE in order to evaluate the presented counter anti-forensic scheme. The multi-purpose nature of the proposed counter JPEG anti-forensic scheme is confirmed from the experiment results under both worst-case and optimistic scenarios,

when tested on UCID and BOSSBase datasets. The proposed scheme provides better detection as compared to the existing forensic techniques against various types of anti-forensic techniques and other image processing operations.

CHAPTER 7

CONCLUSIONS AND FUTURE SCOPE

This chapter provides conclusions based on the research work carried out in this thesis in the field of digital image forensics and anti-forensics. It also provides main highlights and future prospects of the research work.

7.1 Conclusions

The unethical use of digital images on the social networking sites inspires the researchers to work for the enhancement of forensic investigation techniques in order to find out the authenticity of digital images. Therefore, a technique is proposed to detect and analyze the partial doubly compressed JPEG image which leads to the estimation of the first quantization matrix. The proposed technique is based on the concept that to estimate the first quantization matrix from the partial double compressed image, it is desired to detect and isolate the double compressed region efficiently. The experimental results show that the first stage of the proposed scheme has satisfactory performances with an average percentage accuracy of 95.45% even when the detected double compressed regions are of a small size. The proposed filtering strategy increases the accuracy to estimate the first quantization matrix in the second stage. For the first 10 DCT coefficients, an error less than 1.5% has been recorded. The experiment results depict that the performance of the proposed approach is better as compared to the considered state-of-the-art techniques for the partial double compressed images based on the two different datasets. The evaluation is based on the partial double compressed images in which the recompression is performed with different quantization matrix.

A JPEG anti-forensic framework is presented to fool the existing forensic detectors by hiding the compression artifacts in both spatial and DCT domain. The suggested denoising algorithms improve the image quality by removing the unnatural noise left during the perceptual histogram smoothing. Furthermore, the suggested TV-based deblocking operation helps to attain better forensic undetectability by reducing the blocking artifacts. When this framework is evaluated on UCID dataset, 96.72% of the images are classified as never JPEG compressed. Image visual

quality is also one of the main goals of the presented JPEG anti-forensic technique along with the good forensic undetectability. The proposed JPEG anti-forensic scheme provides enhanced image visual quality as compared to the existing approaches with an average PSNR and SSIM values of 35.93 dB and 0.9893 respectively on UCID dataset. Moreover, a better tradeoff is obtained between image quality and forensic undetectability by the proposed JPEG anti-forensic techniques as compared to the state-of-the-art techniques. Though the proposed technique is better than the previous anti-forensic techniques, but in terms of computational complexity, it takes more execution time to generate a JPEG forgery.

The anti-forensic techniques can easily misguide the forensic detectors based on the first-order statistical analysis and hence making the use of first-order statistics irremediably insecure. When higher statistical analysis is carried out then such anti-forensic techniques do not guarantee forensic undetectability. Thus, a second-order statistical analysis is conducted derived from the CM for detecting the footprints left during the JPEG anti-forensic schemes. The analysis performed in this thesis proves that it is difficult to remove the footprints of JPEG compression completely. Moreover, the proposed forensic technique particularly targets the JPEG anti-forensic dithering which is not the case in the existing counter JPEG anti-forensic approaches. Thus, the proposed forensic method is less prone to produce false positives when the image has been corrupted by other nonmalicious noise. The proposed scheme provides an average accuracy of 93.63%, when tested by considering various JPEG anti-forensic techniques. The experiment results confirm the multi-purpose nature of the proposed scheme by providing better detection in comparison to the existing forensic techniques against various types of anti-forensic attacks and other image processing operations. The proposed counter JPEG anti-forensic technique provides an average detection accuracy of 92.17% and 96.31% against different median filtering anti-forensic schemes and spatial filtering operations respectively.

Some beneficial observations are provided in this research work for the forensic detectives and counterfeiters. For the forensic detectives, the proposed counter anti-forensic scheme works efficiently in the detection of various types of anti-forensic techniques and other image processing operations without considering the specific artifacts of particular image operation. On the contrary, inherent original image statistics must be considered very precisely by forgers in order to create a robust image forgery or anti-forensic process.

7.2 Main Highlights of the Research Work

The following are the main highlights of the presented research work in the field of digital image forensics and anti-forensics:

- A forensic technique is developed for DJPG compression to detect the double compressed region along with the estimation of first quantization matrix.
- An anti-forensic framework for JPEG compression (single and double) is proposed to disguise the existing scalar and SVM-based forensic detectors. When this framework is evaluated on UCID dataset, 96.72% of the images are classified as never JPEG compressed.
- A counter JPEG anti-forensic approach is designed based on the second-order statistical analysis.
- The proposed counter JPEG anti-forensic is further explored to find its applications in the detection of Median filtering and CE anti-forensics. The proposed forensic scheme provides better results in the detection of these anti-forensic schemes and other image processing operations.

The novelty of the proposed JPEG anti-forensics is that it provides better image visual quality and robust against various scalar and SVM-based forensic detectors. Moreover, the proposed work on countering JPEG anti-forensics will be very useful for the forensic community to investigate the fake digital evidences.

7.3 Future Scope

The presented research work can be extended in the following directions for further improvements in digital image forensics:

- The work can be extended to create a detection methodology for the partial double compressed images, where recompression is performed with same quantization matrix.
- The presented work on JPEG anti-forensics is further stretched to make a universal framework for anti-forensics by achieving a better restoration of DCT coefficients histogram.
- The proposed JPEG anti-forensic work can also be extended to color images.

- Future research can be dedicated to create a universal detection scheme to detect different image manipulations such as locating regions that have been tampered within an image.
- The future work can be dedicated to use the CNN in order to improve the forensic and anti-forensic techniques.
- Moreover, a comparative analysis can also be performed between the SVM and CNN-based forensic detectors.

REFERENCES

[1] H. Farid. (2012). *Digital image forensics* [Online]. Available: https://farid.berkeley.edu/downloads/tutorials/digitalimageforensics.pdf [Accessed On: 10 Jun. 2019].

[2] G. Singh. (2019). *Top 33 Photo editing apps-Best photo apps of 2019* [Online]. Available: https://www.pixpa.com/blog/photo-apps [Accessed On: 27 Oct. 2019].

[3] A. Brock, T. Lim, J. M. Ritchie, and N. Weston, "Neural photo editing with introspective adversarial networks," in *Proc. Int. Conf. Learning Representations*, Apr. 2017, pp. 1–11.

[4] J. A. Redi, W. Taktak, and J. L. Dugelay, "Digital image forensics: A booklet for beginners," *Multimed. Tools Appl.*, vol. 51, no. 1, pp. 133–162, 2011.

[5] R. Saracco. (2018). *IEEE future directions* [Online]. Available: https://cmte.ieee.org/futuredirections/2018/08/23/6953 [Accessed On: 12 Jan. 2019].

[6] M. Garber. (2012). *Oprah's head, Ann-Margaret's body: A brief history of pre-photoshop fakery* [Online]. Available: https://www.theatlantic.com/technology/archive/2012/06/oprahs-head-ann-margarets-body-a-brief-history-of-pre-photoshop-fakery/258369 [Accessed On: 27 Apr. 2019].

[7] M. Nizza and P. J. Lyons. (2008). *In an Iranian image, a missile too many* [Online]. Available: https://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many [Accessed On: 12 Jan. 2018].

[8] B. Arogundade. (2016). *OJ Simpson's 1994 Mugshot for 'Time' & 'Newsweek' magazine covers: 'Time' deliberately blackened picture* [Online]. Available: http://www.arogundade.com/oj-simpson-murder-trial-case-time-and-newsweek-magazine-cover-controversy-1994-oj-simpson-photo-manipulation.html [Accessed On: 12 Jan. 2018].

[9] Snopes.com. (2000). *University of Wisconsin booklet photoshopped to add black student* [Online]. Available: https://www.snopes.com/fact-check/photo-finish-2 [Accessed On: 27 Apr. 2019].

[10] Indianexpress.com. (2015). *Chennai Floods: PIB removes PM Modi's photo from website after proven fake* [Online]. Available: https://indianexpress.com/article/india/india-news-india/pib-removes-pm-modis-chennai-photo-from-website-after-proven-fake [Accessed On: 21 Mar. 2016].

[11] Indianexpress.com. (2016). *Photos of Dhaka streets are going viral again! Well, they're photoshopped* [Online]. Available: https://indianexpress.com/article/trending/trending-in-india/photos-of-normal-dhaka-streets-are-going-viral-again-well-theyre-photoshopped-3036034 [Accessed On: 20 May 2017].

[12] T. Nicholson. (2019). *Is Donald Trump doctoring photos to make his tiny little fingers look longer?* [Online]. Available: https://www.esquire.com/uk/latest-news/a25986516/is-donald-trump-doctoring-photos-to-make-his-tiny-little-fingers-look-longer [Accessed On: 19 May 2019].

[13] S. Battiato, O. Giudice, and A. Paratore, "Multimedia forensics: Discovering the history of multimedia contents," in *Proc. Int. Conf. Comput. Syst. Technology*, Jun. 2016, pp. 5–16.

[14] C. Pasquini, G. Boato, and R. Bohme, "Teaching digital signal processing with a challenge on image forensics," *IEEE Signal Process. Mag.*, vol. 36, no. 2, pp. 101–109, 2019.

[15] A. K. Jaiswal and R. Srivastava, "Copy-move forgery detection using shift-invariant SWT and block division mean features," in *Lecture Notes in Electrical Engineering*, vol. 524, pp. 289–299, 2019.

[16] R. Montasari and R. Hill, "Next-generation digital forensics: Challenges and future paradigms," in *Proc. Int. Conf. Global Security, Safety and Sustainability*, Jan. 2019, pp. 1–8.

[17] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *AEU - Int. J. Electron. Commun.*, vol. 65, no. 10, pp. 840–847, 2011.

[18] V. Conotter, *Active and passive multimedia forensics*. PhD thesis, University of Trento, Italy, 2011.

[19] G. L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image," *IEEE Trans. Consum. Electron.*, vol. 39, no. 4, pp. 905–910, 1993.

[20] Tech.sina.com.cn. *Huaqi: the secret to self-innovation in the market* [Online]. Available: http://tech.sina.com.cn/%0Ait/2005-12-21/1432798682.shtml [Accessed On: 18 Oct. 2017].

[21] H. Farid, "A survey of image forgery detection," *IEEE Signal Process. Mag.*, vol. 2, no. 26, pp. 16–25, 2009.

[22] H. Farid, *Digital image ballistics from JPEG quantization*. Tech. rep. TR2006-583, Department of Computer Science, Dartmouth College, USA, 2006.

[23] R. Böhme and M. Kirchner, "Counter-forensics: Attacking image forensics," in *Digital Image Forensics*, New York, USA: Springer-Verlag, 2013, pp. 327–366.

[24] M. Barni and F. Perez-Gonzalez, "Coping with the enemy: Advances in adversary-aware signal processing," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2013, pp. 8682–8686.

[25] M. Kirchner and R. Böhme, "Tamper hiding: defeating image forensics," in *Proc. Int. Conf. Inf. Hiding*, Jun. 2007, pp. 326–341.

[26] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1050–1065, 2011.

[27] Z.-H. Wu, M. C. Stamm, and K. J. R. Liu, "Anti-forensics of median filtering," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2013, pp. 3043–3047.

[28] T. Pevny, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, 2010.

[29] H. Li, W. Luo, X. Qiu, and J. Huang, "Identification of various image operations using residual-based features," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 1, pp. 31–45, 2018.

[30] M. Kirchner and R. Röhme, "Hiding traces of resampling in digital images," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 582–592, 2008.

[31] W3techs.com. (2019) *Usage of image file formats for websites* [Online]. Available: http://w3techs.com/technologies/overview/image_format/all [Accessed On: 12 Jan. 2019].

[32] H. Farid, "Exposing digital forgeries from JPEG ghosts," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 154–160, 2009.

[33] G. Puglisi, A. R. Bruna, F. Galvan, and S. Battiato, "First JPEG quantization matrix estimation based on histogram analysis," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2013, pp. 4502–4506.

[34] F. Galvan, G. Puglisi, A. R. Bruna, and S. Battiato, "First quantization matrix estimation from double compressed JPEG images," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1299–1310, 2014.

[35] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," in *Proc. Security, Steganography, Watermarking of Multimedia Contents IX*, Feb. 2007, pp. 1–11.

[36] T. Pevny and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 247–258, 2008.

[37] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "The cost of JPEG compression anti-forensics," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2011, pp. 1884–1887.

[38] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "A variational approach to JPEG anti-forensics," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2013, pp. 3058–3062.

[39] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1211–1226, 2014.

[40] G. Hudson, A. Léger, B. Niss, I. Sebestyén, and J. Vaaben, "JPEG-1 standard 25 years: past, present, and future reasons for a success," *J. Electron. Imag.*, vol. 27, no. 4, pp. 1–19, 2018.

[41] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Trans. Consum. Electron.*, vol. 38, no. 1, pp. 18–34, 1992.

[42] P.-Y. Lin. (2009). *Basic image compression algorithm and introduction to JPEG standard* [Online]. Available: http://disp.ee.ntu.edu.tw/meeting [Accessed On: 13 Sep. 2016].

[43] W. B. Pennebaker and J. L. Mitchell, *JPEG still image data compression standard*. Springer US, 1993.

[44] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 480–491, 2010.

[45] M. A. Robertson and R. L. Stevenson, "DCT quantization noise in compressed images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 1, pp. 27–38, 2005.

[46] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 101–117, 2008.

[47] P. Korus, "Digital image integrity – a survey of protection and verification techniques," *Digital Signal Processing*, vol. 71, pp. 1–26, 2017.

[48] E. Kee, M. K. Johnson, and H. Farid, "Digital image authentication from JPEG headers," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1066–1075, 2011.

[49] A. Piva, "An overview on image forensics," *ISRN Signal Process.*, vol. 2013, pp. 1–22, 2012.

[50] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," *IEEE Access*, vol. 1, pp. 167–200, 2013.

[51] S. Battiato and G. Messina, "Digital forgery estimation into DCT domain: A critical analysis," in *Proc. ACM Workshop Multimedia Forensics*, Oct. 2009, pp. 37–42.

[52] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proc. Int. Workshop Inf. Hiding*, May 2004, pp. 128–147.

[53] C. Chen, Y. Q. Shi, and W. Su, "A machine learning based scheme for double JPEG compression detection," in *Proc. Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1–4.

[54] V. L. L. Thing, Y. Chen, and C. Cheh, "An improved double compression detection method for JPEG image forensics," in *Proc. IEEE Int. Symp. Multimedia*, Dec. 2012, pp. 290–297.

[55] F. Huang, J. Huang, and Y. Q. Shi, "Detecting double JPEG compression with the same quantization matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 848–856, 2010.

[56] F. Shi, B. Kang, H. Li, and Y. Zhu, "A new method for detecting JEPG doubly compression images by using estimated primary quantization step," in *Proc. Int. Conf. Syst. Informatics*, May 2012, pp. 1810–1814.

[57] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y. Q. Shi, "An effective method for detecting double JPEG compression with the same quantization matrix," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1933–1942, 2014.

[58] D. Y. Huang, C. N. Huang, W. C. Hu, and C. H. Chou, "Robustness of copy-move forgery detection under high JPEG compression artifacts," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1509–1530, 2017.

[59] Y. Li and J. Zhou, "Fast and effective image copy-move forgery detection via hierarchical feature point matching," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1307–1322, 2019.

[60] K. Khuspe and V. Mane, “Robust image forgery localization and recognition in copy-move using bag of features and SVM,” in *Proc. IEEE Int. Conf. Comm. Inf. and Computing Technology*, Jan. 2015, pp. 1–5.

[61] Q. Zhao, D. Grace, A. Vilhar, and T. Javornik, “Using K-means clustering with transfer and Q learning for spectrum, load and energy optimization in opportunistic mobile broadband networks,” in *Proc. IEEE Int. Symp. Wireless Comm. Syst.*, Aug. 2015, pp. 1–5.

[62] Q. Liu, “Detection of misaligned cropping and recompression with the same quantization matrix and relevant forgery,” in *Proc. 3rd Int. ACM Workshop Multimedia Forensics Intell.*, Nov. 2011, pp. 25–30.

[63] Z. Fan and R. L. De Queiroz, “Identification of bitmap compression history: JPEG detection and quantizer estimation,” *IEEE Trans. Image Process.*, vol. 12, no. 2, pp. 230–235, 2003.

[64] Z. Wang, A. C. Bovik, and B. L. Evan, “Blind measurement of blocking artifacts in images,” in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2000, pp. 981–984.

[65] B. Mahdian and S. Saic, “Detecting double compressed JPEG images,” in *Proc. Int. Conf. Image Crime Detection Prevention*, Dec. 2009, pp. 1–6.

[66] X. Feng and G. Doërr, “JPEG recompression detection,” in *Proc. Media Forensics Security II*, Jan. 2010, pp. 1–12.

[67] J. He, Z. Lin, L. Wang, and X. Tang, “Detecting doctored JPEG images via DCT coefficient analysis,” in *Proc. Eur. Conf. Comput. Vis.*, vol. 3953, May 2006, pp. 423–435.

[68] Y. Y. Chuang, B. Curless, D. H. Salesin, and R. Szeliski, “A Bayesian approach to digital matting,” in *Proc. IEEE Int. Conf. Comput. Vis. and Pattern Recognit.*, Dec. 2001, pp. 264–271.

[69] D. T. Trung, A. Beghdadi, and M. C. Larabi, “Blind inpainting forgery detection,” in *Proc. IEEE Int. Conf. Signal and Inf. Process.*, Dec. 2014, pp. 1019–1023.

[70] W. Luo, Z. Qu, J. Huango, and G. Qiu, “A novel method for detecting cropped and recompressed image block,” in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Apr. 2007, pp. 217–220.

[71] M. Barni, A. Costanzo, and L. Sabatini, “Identification of cut & paste tampering by means of double-JPEG detection and image segmentation,” in *Proc. IEEE Int. Symp. Circuits Syst.*, Jun. 2010, pp. 1687–1690.

[72] Y. L. Chen and C. T. Hsu, “Image tampering detection by blocking periodicity analysis in JPEG compressed images,” in *Proc. IEEE Workshop Multimedia Signal Process.*, Oct. 2008, pp. 803–808.

[73] Y. L. Chen and C. T. Hsu, “Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 396–406, 2011.

[74] X. Z. Meng, S. Z. Niu, and J. C. Zou, “Tamper detection for shifted double JPEG

compression," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2010, pp. 434–437.

[75] T. Bianchi and A. Piva, "Detection of nonaligned double JPEG compression based on integer periodicity maps," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 842–848, 2012.

[76] Z. Lin, J. He, X. Tang, and C. K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognit.*, vol. 42, no. 11, pp. 2492–2501, 2009.

[77] T. Bianchi, A. De Rosa, and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2011, pp. 2444–2447.

[78] R. Zhang and R. D. Wang, "In-camera JPEG compression detection for doubly compressed images," *Multimedia Tools Appl.*, vol. 74, no. 15, pp. 5557–5575, 2015.

[79] A. Taimori, F. Razzazi, A. Behrad, A. Ahmadi, and M. B. Zadeh, "A novel forensic image analysis tool for discovering double JPEG compression clues," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 7749–7783, 2017.

[80] W. Wang, J. Dong, and T. Tan, "Exploring DCT coefficient quantization effect for image tampering localization," in *Proc. IEEE Int. Workshop Inf. Forensics Security*, Dec. 2011, pp. 1–6.

[81] T. Pevný and J. Fridrich, "Estimation of primary quantization matrix for steganalysis of double-compressed JPEG images," in *Proc. Security, Forensics, Steganography, Watermarking of Multimedia Contents X*, Mar. 2008, pp. 1–13.

[82] Z. Fan and R. L. De Queiroz, "Maximum likelihood estimation of JPEG quantization table in the identification of bitmap compression history," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2000, pp. 948–951.

[83] J. Wang, B. H. Cha, S. H. Cho, and C. C. J. Kuo, "Understanding Benford's law and its vulnerability in image forensics," in *Proc. IEEE Int. Conf. Multimedia and Expo*, Jul. 2009, pp. 1568–1571.

[84] C. Pasquini, G. Boato, and F. Perez-Gonzalez, "Statistical detection of JPEG traces in digital images in uncompressed formats," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2890–2905, 2017.

[85] J. Lukas and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. Digit. Forensic Res. Workshop*, Aug. 2003, pp. 5–8.

[86] B. Li, Y. Q. Shi, and J. Huang, "Detecting doubly compressed JPEG images by using mode based first digit features," in *Proc. IEEE Workshop Multimedia Signal Process.*, Oct. 2008, pp. 730–735.

[87] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1003–1017, 2012.

[88] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2691–2706, 2018.

[89] V. Verma, N. Agarwal, and N. Khanna, "DCT-domain deep convolutional neural networks for multiple JPEG compression classification," *Signal Process.: Image Comm.*, vol. 67, pp. 22–33, 2018.

[90] M. Boroumand and J. J. Fridrich, "Deep learning for detecting processing history of images," in *Proc. Int. Symp.* Media Watermarking, Security, Forensics, Jan. 2018, pp. 1–9.

[91] X. Huang, S. Wang, and G. Liu, "Detecting double JPEG compression with same quantization matrix based on dense CNN feature," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2018, pp. 3813–3817.

[92] Q. Wang and R. Zhang, "Double JPEG compression forensics based on a convolutional neural network," *EURASIP J. Inf. Security*, pp. 1–12, 2016.

[93] J. Park, D. Cho, W. Ahn, and H. K. Lee, "Double JPEG detection in mixed JPEG quality factors using deep convolutional neural network," in *Proc. European Conf. Comput. Vision*, Sep. 2018, pp. 656–672.

[94] B. Bayar and M. C. Stamm, "Towards order of processing operations detection in JPEG compressed images with convolutional neural networks," in *Proc. Int. Symp. Media Watermarking, Security, Forensics*, Jan. 2018, pp. 1–9.

[95] M. Stamm, S. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Mar. 2010, pp. 1694–1697.

[96] M. Stamm, S. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 2109–2112.

[97] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, "Countering JPEG anti-forensics," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2011, pp. 1949–1952.

[98] S. Lai and R. Böhme, "Countering counter-forensics: The case of JPEG compression," in *Proc. Int. Conf. Inf. Hiding*, May 2011, pp. 285–298.

[99] H. Li, W. Luo, and J. Huang, "Countering anti-JPEG compression forensics," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2012, pp. 241–244.

[100] C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2008, pp. 3029–3032.

[101] P. Sutthiwan and Y. Q. Shi, "Anti-forensics of double JPEG compression detection," in *Proc. Int. Workshop Digital Forensics Watermarking*, Oct. 2011, pp. 411–424.

[102] P. Comesaña-Alfaro and F. Pérez-González, "Optimal counterforensics for histogram-based forensics," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Jun. 2013, pp. 3048–3052.

[103] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "Revealing the traces of JPEG compression anti-forensics," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 335–349, 2013.

[104] H. Zeng, X. Kang, and A. Peng, "A multi-purpose countermeasure against image anti-forensics using autoregressive model," *Neurocomputing*, vol. 189, pp. 117–122, 2016.

[105] M. Barni, Z. Chen, and B. Tondi, "Adversary-aware, data-driven detection of double JPEG compression: How to make counter-forensics harder," in *Proc. IEEE Int. Workshop Inf. Forensics Security*, Dec. 2016, pp. 1–6.

[106] Y. Chen, X. Kang, Z. J. Wang, and Q. Zhan, "Densely connected convolutional neural network for multi-purpose image forensics under anti-forensic attacks," in *Proc. ACM Workshop Inf. Hiding Multimedia Security*, Jun. 2018, pp. 91–96.

[107] B. Li, H. Zhang, H. Luo, and S. Tan, "Detecting double JPEG compression and its related anti-forensic operations with CNN," *Multimed. Tools Appl.*, pp. 1–25, 2019.

[108] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, 2006.

[109] T. Mapayi, S. Viriri, and J. R. Tapamo, "Adaptive thresholding technique for retinal vessel segmentation based on GLCM-Energy information," *Comput. Math. Methods Med.*, vol. 2015, pp. 1–12, 2015.

[110] M. Mishra. (2018). *Understanding ROC & AUC curve* [Online]. Available: https://medium.com/datadriveninvestor/understanding-roc-auc-curve-7b706fb710cb [Accessed On: 15 Jan. 2019].

[111] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, Jun. 2010, pp. 161–177.

[112] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. ACM Int. Workshop Inf. Hiding Multimedia Security*, Jun. 2013, pp. 59–68.

[113] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–39, 2011.

[114] S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in *Proc. IEEE Int. Conf. TENCON*, Nov. 2008, pp. 1–5.

[115] Z. Wang and A. C. Bovik, *Modern image quality assessment*. Morgan & Claypool, 2006.

[116] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, 2004.

[117] G. Schaefer and M. Stich, "UCID—An uncompressed colour image database," in *Proc. SPIE*, Mar. 2004, pp. 472–480.

[118] P. Bas, T. Filler, and T. Pevny, "Break our steganographic system: The ins and outs of organizing BOSS," in *Proc. Int. Conference Inf. Hiding*, May 2011, pp. 59-70.

[119] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "Median filtered image quality enhancement and anti-forensics via variational deconvolution," *IEEE Trans. Inf. Forensics Security,* vol. 10, no. 5, pp. 1076–1091, May 2015.

[120] F. Zach, C. Riess, and E. Angelopoulou, "Automated image forgery detection through classification of JPEG ghosts," in *Proc. Joint DAGM and OAGM Symp. Pattern Recognit.*, Aug. 2012, pp. 185–194.

[121] N. Jaiswal and Y. K. Meghrajani, "Saliency based automatic image cropping using support vector machine classifier," in *Proc. IEEE Int. Conf. Innovations in Inf., Embedded and Comm. Syst.*, Mar. 2015, pp. 1–5.

[122] Ijg.org. (2014). *Independent JPEG Group* [Online]. Available: http://www.ijg.org [Accessed On: 11 Dec. 2015].

[123] R0k.us. (2014). *Dataset Eastman Kodak* [Online]. Available: http://r0k.us/graphics/kodak [Accessed On: 11 Dec. 2015].

[124] T. Pevný and J. Fridrich, "Multiclass detector of current steganographic methods for JPEG format," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 635–650, 2008.

[125] A. T. S. Ho, S. Li, *Handbook of digital forensics of multimedia data and devices*. John Wiley & Sons, 2015.

[126] C. Ullerich and A. Westfeld, "Weaknesses of MB2," in *Proc. Int. Workshop Digital Watermarking*, Nov. 2008, pp. 127–142.

[127] A. Chambolle, "An algorithm for total variation minimization and applications," *J. Math. Imag. Vis.*, vol. 20, no. 1, pp. 89–97, 2004.

[128] T. Sharma and K. K. Sharma, "QRS complex detection in ECG signals using locally adaptive weighted total variation denoising," *Comput. Biol. Med.*, vol. 87, pp. 187–199, 2017.

[129] P. Getreuer, "Rudin-Osher-Fatemi total variation denoising using split bregman," *Image Process. Line*, vol. 2, pp. 74–95, 2012.

[130] L. I. Rudin, S. Osher, and E. Fatemi, "Nonlinear total variation based noise removal algorithms," *Phys. D Nonlinear Phenom.*, vol. 60, pp. 259–268, 1992.

[131] A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," in *Proc. IEEE Int. Conf. Comput. Vis.*, Sep. 1999, pp. 1–6.

[132] A. Buades, B. Coll, and J. M. Morel, "A non-local algorithm for image denoising," in *Proc. IEEE Int. Conf. Comput. Vis. and Pattern Recognit.*, Jun. 2005, pp. 1–6.

[133] F. Alter, S. Durand, and J. Froment, "Adapted total variation for artifact free decompression of JPEG images," *J. Math. Imag. Vis.*, vol. 23, no. 2, pp. 199–211, 2005.

[134] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[135] Homepages.cae.wisc.edu. *Public-domain test images for homeworks and projects* [Online]. Available: https://homepages.cae.wisc.edu/~ece533/images [Accessed On: 15 Dec. 2016].

[136] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in *Proc. IEEE Int. Conf. Comput. Vis. and Pattern Recognit.*, Jun. 2008, pp. 1–8.

[137] J. Lu, F. Liu, and X. Luo, "A study on JPEG steganalytic features: Co-occurrence matrix vs. Markov transition probability matrix," *Digit. Investig.*, vol. 12, pp. 1–14, 2015.

[138] A. De Rosa, M. Fontani, M. Massai, A. Piva, and M. Barni, "Second-order statistics analysis to cope with contrast enhancement counter-forensics," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1132–1136, 2015.

[139] C. Chen, J. Ni, and J. Huang, "Blind detection of median filtering in digital images: A difference domain based approach," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 4699–4710, 2013.

[140] Y. Zhang, S. Li, S. Wang, and Y. Q. Shi, "Revealing the traces of median filtering using high-order local ternary patterns," *IEEE Signal Process. Lett.*, vol. 21, no. 3, pp. 275–279, 2014.

[141] X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics using an autoregressive model," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1456–1468, 2013.

[142] V. Vapnik, *The nature of statistical learning theory*. New York, USA, Springer-Verlag, 2000.

[143] D. T. Dang-Nguyen, I. D. Gebru, V. Conotter, G. Boato, and F. G. B. De Natale, "Counter-forensics of median filtering," in *Proc. IEEE Int. Workshop Multimedia Signal Process.*, Sep./Oct. 2013, pp. 260–265.

[144] D. Krishnan and R. Fergus, "Fast image deconvolution using hyper-laplacian priors," *Adv. Neural Inf. Process. Syst.*, pp. 1–9, 2009.

[145] G. Cao, Y. Zhao, R. R. Ni, H. W. Tian, and L. F. Yu, "Attacking contrast enhancement forensics in digital images," *Sci. China Inf. Sci.*, vol. 57, no. 5, pp. 1–13, 2014.

[146] H. Ravi, A. V. Subramanyam, and S. Emmanuel, "ACE - An effective anti-forensic contrast enhancement technique," *IEEE Signal Process. Lett.*, vol. 23, no. 2, pp. 212–216, Feb. 2016.

[147] Y. Choi, D. Kang, J. J. Hwang, and K. H. Rhee, "JPEG compression detection based on edge-corner features using SVM," in *Proc. IEEE Int. Conf. Machine Learning and Data Science*, Dec. 2017, pp. 80–84.

[148] J. J. Hwang and K. H. Rhee, "Gaussian filtering detection based on features of residuals in image forensics," in *Proc. IEEE Int. Conf. Computing and Comm. Technologies, Research, Innovation, and Vision for the Future*, Nov. 2016, pp. 153–157.

[149] M. H. J. Gruber and M. H. Hayes, *Statistical digital signal processing and modeling*. John Wiley & Sons, 1997.

[150] R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital image processing using Matlab*. New Jersey, USA, Pearson Prentice-Hall, 2009.

ANNEXURE-A

LIST OF PUBLICATIONS

Published Journal Publications:

[P.1] G. Singh and K. Singh, "Forensics for partially double compressed doctored JPEG images," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 485–502, 2018. **(SCIE-Indexed, Impact factor: 1.541)**

[P.2] G. Singh and K. Singh, "Improved JPEG anti-forensics with better image visual quality and forensic undetectability," *Forensic Science International*, vol. 277, pp. 133–147, 2017. **(SCI-Indexed, Impact factor: 1.974)**

[P.3] G. Singh and K. Singh, "Counter JPEG anti-forensic approach based on the second-order statistical analysis," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1194–1209, 2019. **(SCI/SCIE-Indexed, Impact factor: 5.824)**

[P.4] K. Singh, A. Kansal, and G. Singh, "An improved median filtering anti-forensics with better image quality and forensic undetectability," *Multidimensional Systems and Signal Processing*, 2019, DOI: 10.1007/s11045-019-00637-8. **(SCI/SCIE-Indexed, Impact factor: 2.088)**

Communicated Journal Publications:

[C.1] G. Singh and K. Singh, "Digital image forensic approach based on the second-order statistical analysis of CFA artifacts," *Forensic Science International*. **(SCI-Indexed, Impact factor: 1.974)**

VITA

Gurinder Singh was born at Gurdaspur, Punjab, India, in 1988. He received his B.Tech. degree in Electronics and Communication Engineering from Lovely Professional University, Phagwara, Punjab, India, in 2012, and M.Tech. degree in Electronics and Communication Engineering from Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India, in 2014. He is currently working towards the Ph.D. degree in Electronics and Communication Engineering from Thapar Institute of Engineering and Technology, Patiala, Punjab, India. He was awarded with the prestigious Visvesvaraya PHD scheme for Electronics and IT fellowship, Ministry of Electronics and Information Technology, Government of India. His research interests include the field of digital image forensics and anti-forensics, image processing, and information security. He can be reached via email: singh.gurinder111@gmail.com and gurinder.singh@thapar.edu.