Improved Forensic and Anti-Forensic Techniques for JPEG Compressed Images

A thesis submitted

in fulfillment of the requirement for the award of degree

of

Doctor of Philosophy

Submitted by

Amit Kumar

Registration Number: 901606006

Under the Supervision of

Dr. Kulbir Singh
Professor, ECED

Dr. Ankush Kansal
Associate Professor, ECED

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

August 2021

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "**Improved Forensic and Anti–Forensic Techniques for JPEG Compressed Images**", 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 and Dr. Ankush Kansal, Associate 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.

Amit Kumar

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
TIET, Patiala, India

Dr. Ankush Kansal
Associate Professor, ECED
TIET, 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 and **Dr. Ankush Kansal**, Associate 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 five 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 am also grateful to my doctoral committee members **Dr. Vinay Kumar**, Associate Professor, **Dr. Neeru Jindal**, Assistant Professor in ECED, TIET, Patiala and **Dr. Sunil Singla**, Associate Professor in Electrical and Electronic Engineering Department, TIET, Patiala for their valuable suggestions during my entire research. I am also immensely thankful to Dr. S.P Singh (G.C.E.T) and my fellow researchers Dr. Gurinder Singh (I.I.T, Ropar), Kanwarpreet Kaur, Hari Shankar and Navneet Kaur 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.

Amit Kumar

ABSTRACT

Digital image forensics aims to evaluate the image authenticity by analyzing its processing history. This history relates to the origin, credibility and steps of processing that it has experienced and helps the detective to find the truth of an image. JPEG is a regularly utilized compression standard and it has been broadly utilized in cameras and image processing software's. Therefore, JPEG compression has become an important part of many image forgeries. Thus, the detection of JPEG compression can add a great value to evaluate the authenticity of digital images. Therefore, there is need of efficient forensic techniques to evaluate the authenticity and proficient anti-forensic techniques that challenge and help in the upgradation of forensic techniques are required.

The research work is directed to design an efficient JPEG anti-forensic technique that has the capability to mislead the forensic detectors by hiding the artifacts of compression in Discrete Cosine Transform (DCT) domain. In the first stage of the proposed scheme, shifted block DCT approach is employed on the considered JPEG compressed image to fill the gaps in the comb-like distribution of DCT coefficients. This shifted block DCT approach led to the addition of dithering noise itself without the need of any adaptive dithering model. The result of this shifted block DCT approach is further processed in the second stage by TV (Total variation)-based deblocking operation to remove the blocking artifacts left during the JPEG compression in the spatial domain. The experimental results illustrate that the presented approach has better performance in comparison to the existing techniques in terms of image visual quality and forensic undetectability with highly reduced computational cost.

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. Therefore, the technique which has the capability to deceive the scalar based and machine learning-based forensic detectors by hiding the artifacts of compression in DFrCT domain is proposed. The additional fractional parameter $'\alpha'$ in DFrCT gives more flexibility when designing a system, in contrast to DCT. The shifted block DFrCT approach efficiently hides the JPEG compression artifacts and disguises several JPEG forensic detectors. The proposed technique possesses the advantage of having an additional fractional parameter to increase its flexibility. TV-based deblocking is further used to reduce the blocking artifacts. Therefore, this technique possesses different variables for each considered image i.e. shifted block and fractional parameter for the optimization of proposed

JPEG anti-forensic approach. It is observed from the experimental results that the proposed approach provides improved performance in terms of image quality and forensic undetectability when compared to existing techniques.

The goal 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. Actually, the existing forensic work on JPEG compression detection is solely dedicated to the first-order statistical feature components analysis. The first order statistical analysis based forensic detectors can be easily misguided by applying some anti-forensic techniques. Therefore, higher order statistical analysis is required to counter these anti-forensic techniques. 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 Markov Transition Probability Matrices (MTPMs) in DCT and DFrCT domain. The proposed framework comprises of three stages: Selection of the target difference image, Evaluation of MTPMs, and Generation of second-order statistical feature based on MTPMs. In the first stage, we explore the effects of dithering operation of JPEG anti-forensics by analyzing the variance inconsistencies along the diagonals. Afterwards, MTPMs 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 MTPMs is very efficient even in the presence of anti-forensic attacks. Moreover, the multi-purpose nature of the proposed counter JPEG anti-forensic scheme is confirmed when evaluated on spliced images considering CASIA v1.0 and Columbia datasets provides better results in the detection of these image operations. The ability of the proposed forensic technique is authenticated from the extensive experimental analysis which provides better detection results against various anti-forensic techniques in terms of minimum decision error, when compared to the existing techniques. The further research work can be concentrated to design a multi-purpose forensic technique based on deep learning by considering Convolutional Neural Networks (CNN) in order to detect the different image processing operations.

LIST OF PUBLICATIONS

[P.1] A. Kumar, A. Kansal, and K. Singh, "An improved anti-forensic technique for JPEG compression," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 25427–25453, 2019. **(SCIE-Indexed, Impact factor: 2.757)**

[P.2] A. Kumar, A. Kansal, and K. Singh, "Anti-forensic approach for JPEG compressed images with enhanced image quality and forensic undetectability," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 8061–8084, 2020. **(SCIE-Indexed, Impact factor: 2.757)**

[P.3] A. Kumar, G. Singh, A. Kansal, and K. Singh, "Digital image forensic approach to counter the JPEG anti-forensic attacks," *IEEE Access*, vol. 9, pp. 4364–4375, 2021. **(SCIE-Indexed, Impact factor: 3.367).**

[P.4] A. Kumar, A. Kansal, and K. Singh, "Exposing JPEG compression footprints by using second-order statistical analysis," *ACM Transactions on Multimedia Computing, Communications, and Applications*. **(SCIE-Indexed, Impact factor: 3.144)**
(Communicated)

LIST OF ABBREVIATIONS

CCD	Charge Coupled Device
A-DJPG	Aligned Double JPEG
NA-DJPG	Non-Aligned Double JPEG
bpp	bits per pixel
HOG	Histogram of oriented gradients
CFA	Color Filter Array
SURF	Speeded-up robust features
LBP	Local binary patterns
CNN	Convolutional Neural Network
MIFT	Mirror Invariance Feature Transform
MTPM	Markov Transition Probability Matrix
dB	deciBel
CMOS	Complementary metal–oxide–semiconductor
DC	Direct Current
AC	Alternating Current
DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
DFrCT	Discrete Fractional Cosine Transform
IDCT	Inverse Discrete Cosine Transform
KL	Kullback-Leibler
DJPG	Double JPEG
FFT	Fast Fourier Transform
HVS	Human Visual System
BACM	Blocking Artifact Characteristics Matrix
PCA	Principal Component Analysis
FPR	False Positive Rate
TPR	True Positive Rate
JPEG	Joint Photographic Experts Group
MLE	Maximum-Likelihood Estimation
CITDE	CASIA image tampering detection evaluation dataset

PGM	Portable Gray Map
PSNR	Peak Signal-to-Noise Ratio
SSIM	Structural SIMilarity
ANOVA	Analysis of Variance
MSE	Mean Squared Error
QDCT	Quantized DCT
RAM	Random Access Memory
RGB	Red, Green, Blue
PGM	Portable Gray Map
TIFF	Tagged Image File Format
PPM	Portable Pixmap
BMP	Bitmap Image
ROC	Receiver Operating Characteristics
AUC	Area Under Curve
SVM	Support Vector Machine
CPU	Central Processing Unit
SPAM	Subtractive Pixel Adjacency Matrix
QF	Quality Factor
TV	Total Variation

LIST OF SYMBOLS

$\boldsymbol{I}$	Original uncompressed image
$\mathcal{T}$	JPEG image compressed from $\boldsymbol{I}$
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
S	Constraint image space
D_{matrix}	DCT block matrix
$q_{block}(.)$	Block DCT coefficient quantization operator
L_p	Laplacian parameter
Max_Y	Maximum value of pixel
$var(.)$	Variance function
$H(.)$	Normalized DCT histogram
μ	Mean intensity
σ	Contrast
$t_{i,j}$	Total variation alongside vertical and horizontal direction.
N_i	Added noise
$TV(.)$	Total variation term
P_e	Minimum Decision Error
D_k	Coefficients DCT matrix of k-th sub-band
B_{gr}^{p}	Gradient aware blockiness
l_p	Norm of weighted gradient
$T(X)$	Convex function
O_S	Projection operator
$C_{(\alpha,\gamma)}(.)$	Kernel matrix
α	Fractional Parameter
D_N	Diagonal matrix
I_{tar}	Target difference image
$T^{(mode)}(.)$	Mode coefficient is represented as as

$\delta(.)$	Mono-dimensional signal
$\mathbb{C}$	Convex set
t_{step}	Positive step size
φ	Regularization parameter
$\mathcal{FD}_{S_qS_b}$	refers to the dithering and deblocking operation based anti-forensic approach [115].
$\mathcal{FD}_V$	corresponds to perceptual anti-forensic dithering approach [150].
$\mathcal{FD}_{S_u}$	represents an anti-forensic technique with SAZ attack [125].
$\mathcal{FD}_F$	refers to anti-forensic scheme based on TV [143].
$\mathcal{FD}_{S_q}$	denotes anti-forensic technique based on DCT histogram smoothing [151].
$\mathcal{FD}_{Fan}$,	four-step adaptive dithering based anti-forensic scheme [47].
$\mathcal{FD}_{Gur}$,	corresponds to scheme based on denoising and dithering [152].
$\mathcal{FD}$	Proposed anti-forensic technique based on shifted block DCT approach.
$\mathcal{FD}_1$	Proposed approach when shifted DFrCT becomes shifted DCT (i.e. $'a'$ =1).
$\mathcal{FD}_2$	Proposed anti-forensic technique based on shifted DFrCT approach.
K_F	denotes the JPEG compression blocking artifacts based detector [96].
K_F^q	refers to detector based on the estimation of quantization table [96].
K_{Weiqi}^q	corresponds to the detector based on the estimation of quantization step [53].
K_{Weiqi}	refers to the detector that identifies JPEG [53].
K_L	denotes calibration feature based JPEG detector [141].
K_V	denotes total variation based JPEG forensic detector [142].
$K_U^1$and K_U^2	denotes JPEG blocking artifacts based detectors [143].
K_P^{S162}	refers to 162-D SPAM feature based detector [145].
K_{Li}^{S100}	100-D correlation detector using intra and inter block [122], [144].
K_{AR}^{S10}	auto regressive detector [128].
K_{SPAM}^{S686}	686-D SPAM detector [38].
K_{SRM}^{S714}	residual detector [130].
K_{MTPM}	Proposed MTPM based forensic approach.

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Most of the information that is being shared on internet with the assistance of varied social networking websites is in the form of digital data. Intentional alteration of digital documents might also be used to defame someone, by showing altered documents in the court [1]. Therefore, the analysis of digital proof can significantly speed up the forensic investigation process. The availability of doctored or tampered images on social media increases every day with the expansion of technology [2]. Therefore, the truthfulness of digital data is one among the main problems in information security. The digital image forensics branch refers to investigation of the digital image so one can examine its legitimacy. On the other hand, image anti-forensics intentions to make barriers inside the trail of forensic investigation [3]. Therefore, this chapter gives detailed information associated with digital image anti-forensics and forensics.

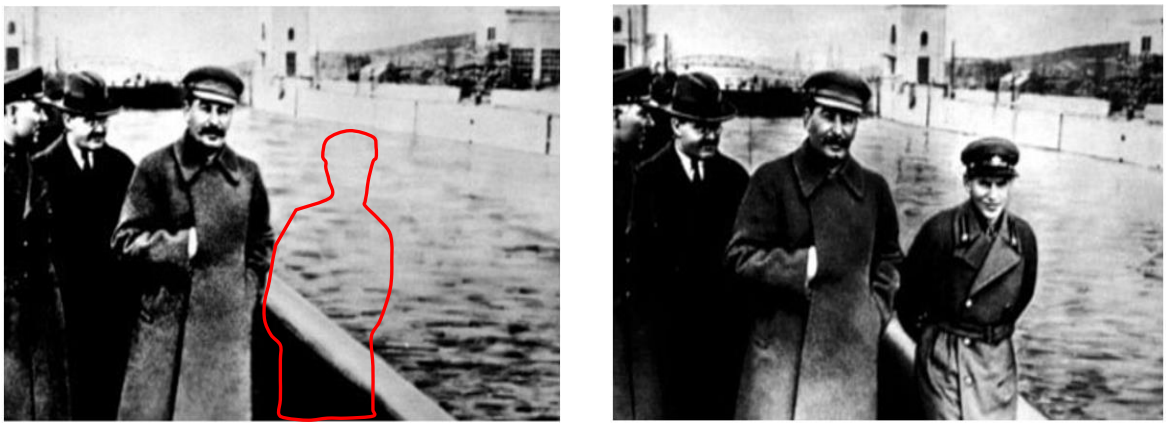
1.1 Preamble

In today's world, lots of things are going on consistently every minute. A number of technological inventions, advancements and discoveries are observed each moment. This requirement prompts the formation of a secure and suitable framework of communication. Information, considerations, views and ideas can be shared in the form of documents, images, text and videos, etc. With the expansion of internet technology and smartphones, a large amount of data is being shared [4]. Images are a skilled and inherent method of communication for people. In general, the image published or distributed in a newspaper is viewed as actual or real. Similarly, recordings of video surveillance can be used as evidence in authentic issues as trial content [5]. The growth in the internet resource and the fast growth in image processing tools and software facilitate an excellent way to edit images without leaving any digital evidence. This provokes the sharing of altered data through images [6]. Therefore, these forgeries need to be restricted to guarantee that right or genuine information is communicated. Digital image forensics is the branch that deals with the authentication and validation of the image by gathering image information and assessing its origin [7]. This circumstance centers around the necessity

for techniques to restore a digital image history so as to evaluate its legitimacy and approve its trustworthiness [8].

1.2 History of Image Tampering

Image tampering has a long history; it started with the invention of photography without the availability of any photo editing software. Therefore, innocence of photography vanished several years ago. Just a few decades after Niepce produced the first photograph in 1814 [9], image alterations were started. Due to the advancement of image editing tools such as Adobe Photoshop, PaintShop Pro, *etc*, powerful computers, and high-resolution digital cameras, it is becoming more prevalent to manipulate images [10]. Moreover, smart phones are now equipped with several photo editing applications [11 – 12] in order to modify the images. 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 [13]. 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 operations [14].

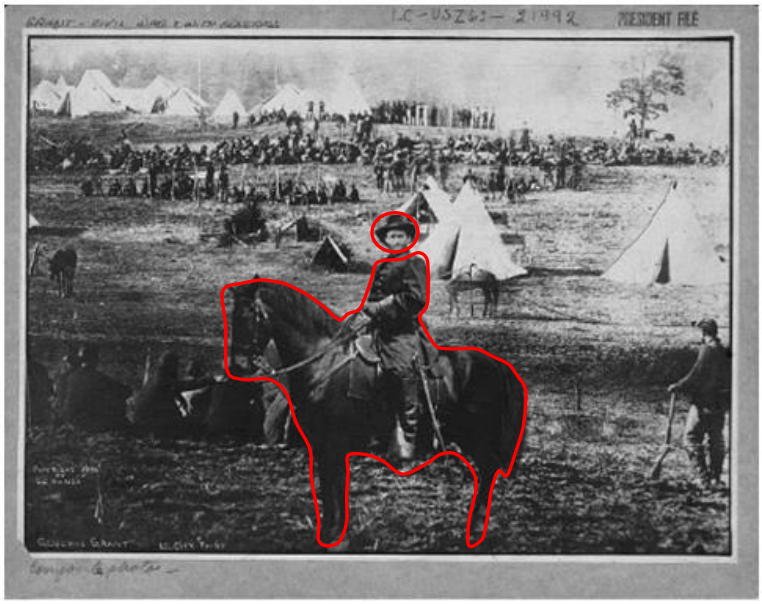


(a) (b)

Figure 1.1: In 1930, an image of Stalin is forged to remove a commissar due to lack of Stalin interest [9].

Stalin was known for many reasons during his rule as a pioneer of Soviet Union from the 1920s to his demise in 1953. In the image Stalin has removed Commissioner Nikolai Yezhov due to lack of interest as shown in Figure 1.1.

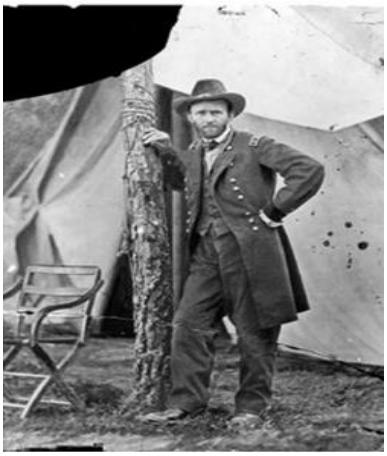
In 1864, during the American Civil War, the image at the top appears to be of US General S. Grant in front of troops shown in Figure 1.2 (a). However, this print was interrogated by some researchers at Prints and Photographs Division, Library of Congress exposed that the image in (a) is made up of three different images: (b) the background is of associated inmates taken at the battle of Fisher's Hill, VA from the image at middle left; (c) the body of Major General Alexander M. McCook and the horse from the image at bottom left; (d) the face of the image is taken from Grant's portrait from the image at right bottom.



(a)

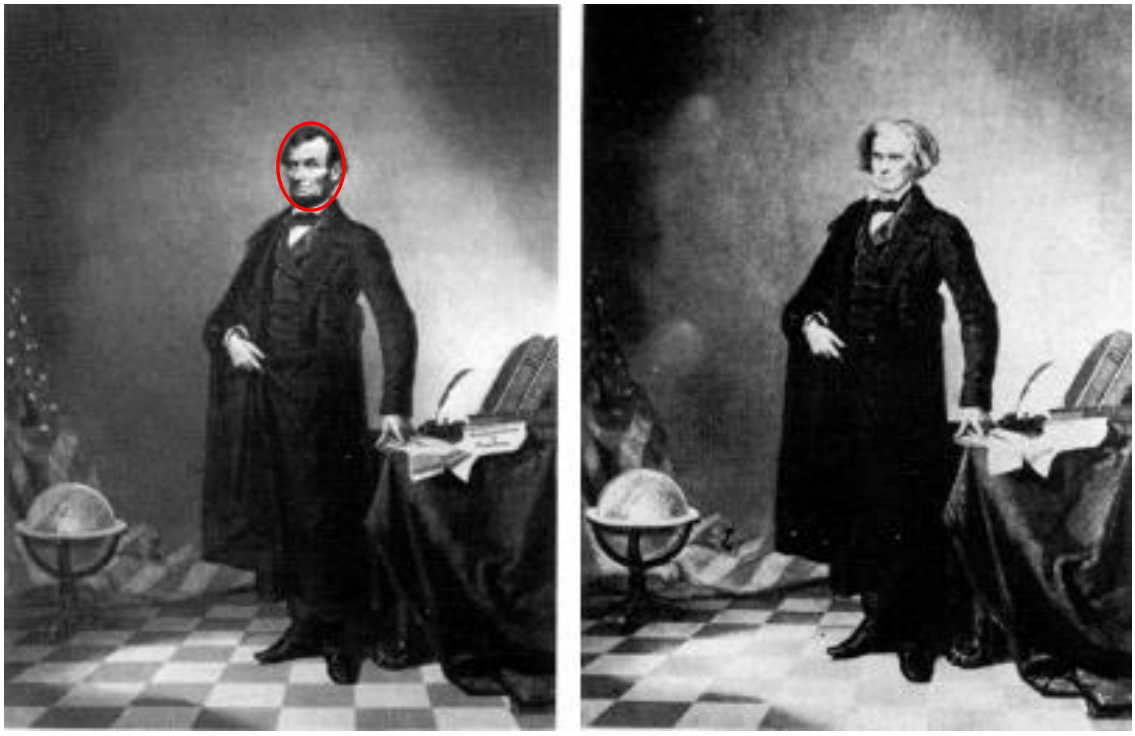
(b)

(c)



(d)

Figure 1.2: A forged image of Ulysses S. Grant during the American Civil War [9].



(a) (b)

Figure 1.3: A forged image of U.S. President Abraham Lincoln [9].

In another case, one of the oldest instances of manipulating an image is President Lincoln's iconic sketch which has been edited with his head emerging on John Calhoun's body shown in Figure 1.3 where, (a) is President Lincoln's image and (b) is John Calhoun's image.

(a) (b)

Figure 1.4: A forged image of Grigoriy Nelyubov [9].

In 1961, for the first time, a group of cosmonauts under command of Yuri Gagarin from Russia completed the orbit of earth. Another, 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 [9].

(a) (b)

Figure 1.5: A forged image of LIFE Magazine [9].

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 [9].

1.3 Life Cycle of Digital Image

The life cycle of digital image in imaging theory is depicted as the construction of various phases, grouped into three primary stages: acquisition stage, coding stage, editing stage. In the acquisition stage, the digital image is formed. The light coming from the actual scene is collected by the digital camera and is then concentrated on sensors (CCD or CMOS) of the camera. An array of color filter known as CFA that specifically allows a specific portion of the light to the sensor is put just before sensor. For creating a full-color image, output of the sensor is then interpolated to obtain each of the RGB colors corresponding to every pixel. This signal passes through extra processing phases in the camera that is usually used to improve picture perception. These phases include procedures such as color processing, white balance, gamma correction, image sharpening, improvement of contrast, etc. [8].

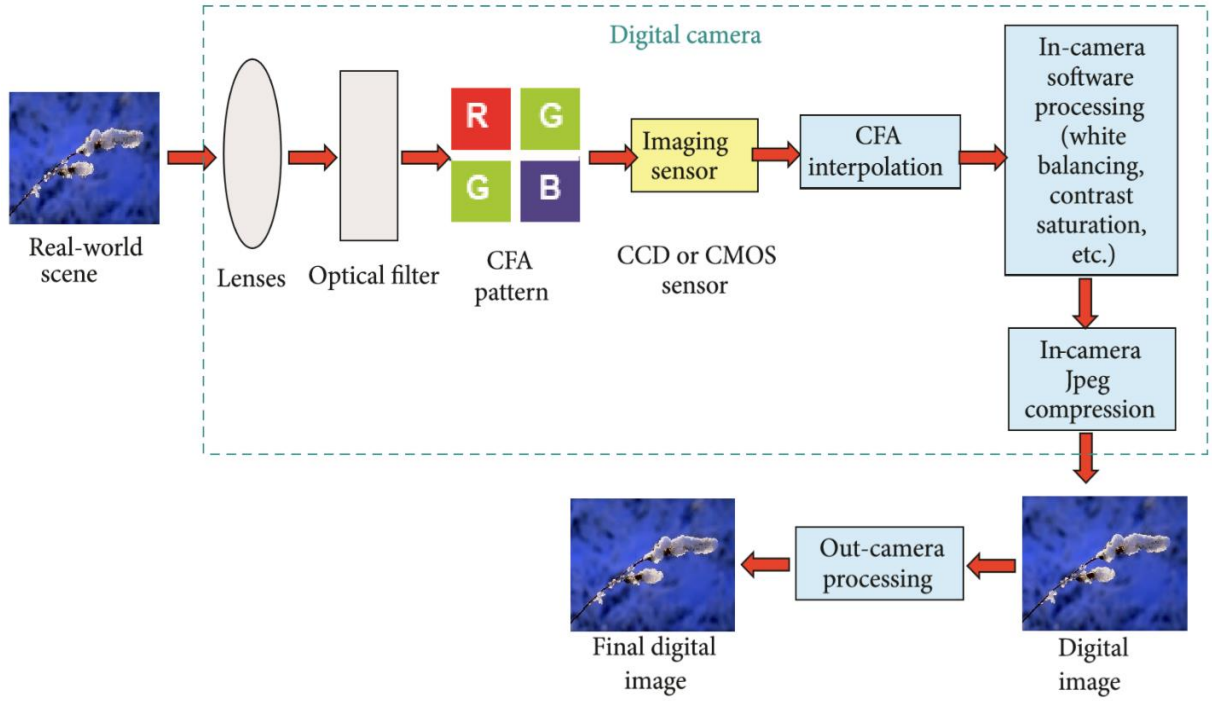


Figure 1.6: A scheme depicted the steps for digital image life cycle [8].

Using the coding method, the obtained image is then stored in the camera memory. The lossy compression JPEG is used in most of the cameras to save memory. At last, to enhance or adjust data, the generated picture can be post-processed. Different procedures of image editing can be encountered on an image during its life cycle: contrast enhancement, blurring, geometric conversion (scaling, rotation, etc.), sharpening and cloning (or copy-move) and image splicing [8].

The basic idea of digital image forensics is to analyze the distinctive marks (such as in digital fingerprinting or traces) that are left in an image during the acquisition phase as well as further successive procedures that occur during the life cycle. Hence, these digital traces can be confined for assessment of the image and catching the historical backdrop of digital information. These traces can be classified into three groups of fingerprints, namely, fingerprint acquisition, fingerprint coding, and fingerprint editing, as the display of the digital image life cycle. Some common editing operations that apply to images are geometric modifications, content modification, and enhancement. These operations include rotation, filtering, zooming, cropping, shearing, cut and paste, seam carving, histogram equalization, copy-move, color modification, copy and paste, contrast adjustment [15].

1.4 Digital Image Forensics

Forensic science is a branch which deals with the investigation and prosecution of a crime using logical methods. Digital forensics is a branch of forensic science which deals with the utilization of digital data which is created, stored and transmitted by considering the digital devices. The image can be manipulated at any phase in the life cycle of a digital image. With an expansion in the availability of social media in a particular manner, information security has become a major problem. The criminal and scientific examination, medicinal imaging and framework observation among the others are the different field serves by forensics. It is now easy to forge photos without leaving any traces because of the availability of several softwares [6]. GIMP, Paintshop Adobe and Pro [16] have automated the ways of editing and perhaps most powerful photo editing softwares. Also, FaceApp [17] and Deep Photo Style Transfer [18] are available to alter outer look or age and visual effects respectively. These are not only easily accessible but are also simple to use. This facilitation additionally makes difficulties for law implementation authorities, security and medical services [19 – 21]. Therefore, it has turned out to be essential to recognize the history of the information that is being shared as it influences many individuals. For images, it is necessary to ensure that the information given by image is unchanged and the modified image can easily be identified. This image processing domain is regarded as digital image forensics [5]. In the present electronic age, Internet of Things (IoT) is becoming reality [22 – 23] and due to ease availability of wireless standards [24 – 26] it is possible to change or alter the information of an image and make it look authentic. Digital image forensics is a promising field of investigation that can depend on detailed formalizations to gather history of an image [27]. The main focus of forensic analysis is based on the validation of image authenticity by reconstructing the generation process of given tampered digital image [28 – 29]. Reconstruction of its digital image life cycle analyzes the picture under investigation. Any anomalies are then inspected for the different traces remaining during the procedures. The image inconsistencies would eventually show the data manipulation or forgery [8]. Digital forensics is also working for security applications with the aim of restoration of acceptance and trust in digital media [2], [30].

1.4.1 Image Tampering Detection Techniques

The methods for determining an image authenticity can be divided into two main types. In the first one, the data contained within the image under consideration is well defined. If the altered image and the reference image are both known, localizing the modified region is simple. Second category is where there is only a forged image. In this situation, the image statistical characteristics are assessed to identify irregularities that would conclusively disclose the forgery.

1.4.1.1 Active Methods

Two primary active methods are based on digital watermarking and signature, as something is incorporated in pictures during acquisition phase. If embedded information cannot be extracted from that image acquired, researchers can identify that the image is tampered. However, the image can be tampered by altering their properties before the embedding of digital signature and watermark. To prevent image from tampering, the watermark takes time to embed in the image, therefore it is the main problem in active methods. Additionally, the inserted watermark must be robust, i.e., the watermark can withstand attacks and cannot be simply changed or removed [31].

1.4.1.2 Passive Methods

In passive methods, there is no such type embedding of information. Therefore, forgery detection using passive methods is a big challenge. There is no such technique that can handle all types of cases; however numerous strategies can identify an uncommon forgery in its own particular manner. These methods detect the duplicated region pixels of the image. In reality, this technique can determine whether the image is modified by any operation through two primary principles, first by attempting to reveal structural distortion (forgery) by learning the irregularities in natural picture statistics. The second set of methods respond to issues like which equipment has been used to record this picture [31]. In Figure 1.7, passive methods depend on irregularities due to impurity and inconsistencies.

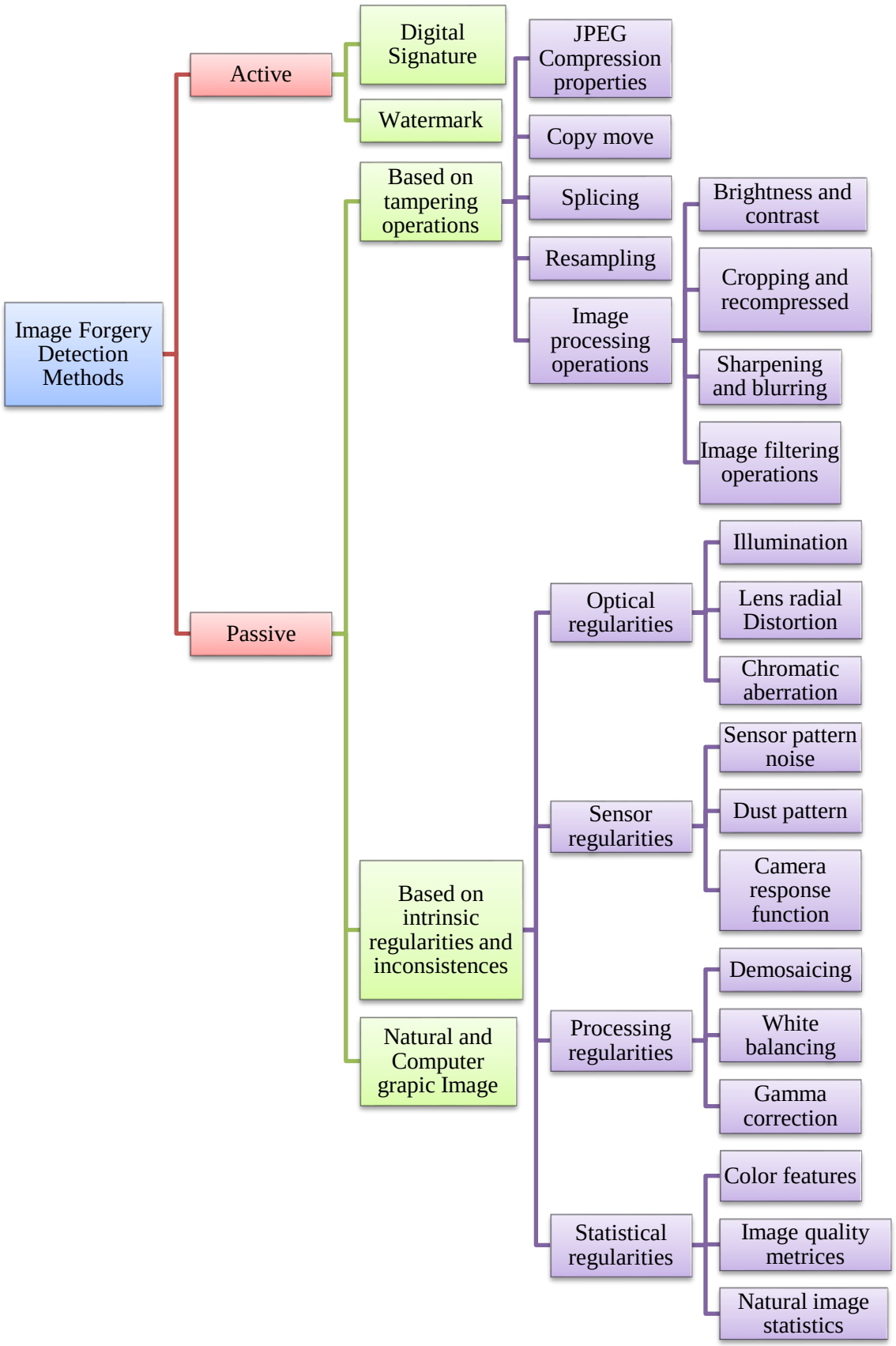


Figure 1.7: Different image forgery methods for the analysis of the image history and reliability [5].

The detection of blind forgery of image involves preprocessing of image, extraction of feature, selection of classifier and classification. Image preprocessing helps to improve the performance by applying some operation. Some image processing operations are transforming RGB to gray, DCT or DWT transformation, cropping, resizing, etc. are utilized to get better features performance. In feature extraction process, a set of features are obtained that helps to differentiate between classes. Haar wavelets, Speeded-up robust features (SURF), Local binary patterns (LBP), Color histograms, and Histogram of oriented gradients (HOG) are the different feature extraction techniques. Features like global transformation features, statistical features, series expansion features, geometrical features, and topological features are generally extracted by these methods. In classifier selection, an appropriate classifier based on extracted features is selected for better classification accuracy. At last, the classifier will discriminate between the two sets of images, i.e., authentic images and forged images based on learned features [32]. The classification accuracy will tell how well the method has performed the task.

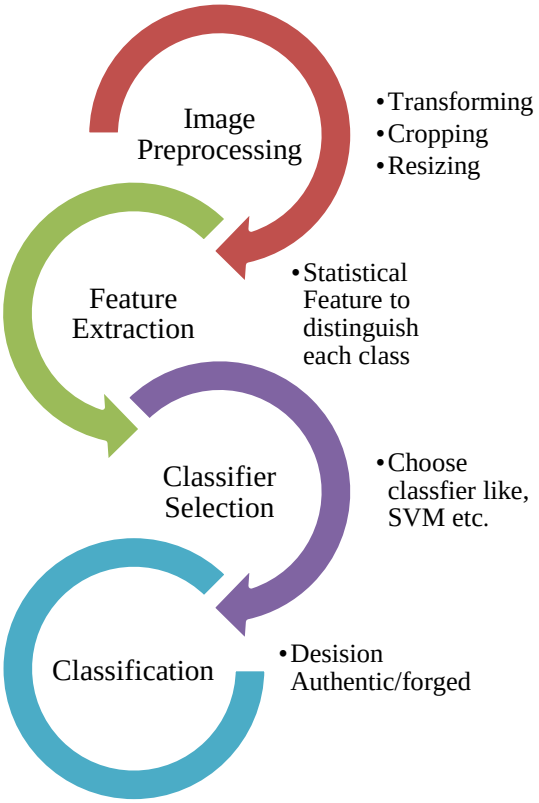


Figure 1.8: Image Forgery detection general framework [32].

1.5 Digital Image Anti-Forensics

Anti-forensic techniques are the actions that are taken in order to create barrier in the forensic investigation process. Activities like overwriting with the new data and protection tools against forensics analysis are included in the anti-forensic techniques [3]. These techniques have been used with the aim that it cannot be interpreted by the unauthorized persons, thus, increasing the security. But, there is disadvantage that, these techniques can be misused by offenders with a defined objective to protect against revelation of their actions [33]. The anti-forensic tool users can eliminate the proof of the different criminal activities of hackers, terrorists etc. Anti-forensics of image is employed by counterfeiters to conceal the traces of different image processing or editing methods namely re-sampling, JPEG compression *etc*. in order to mislead or create a barrier in the process of forensic analysis. The anti-forensics also motivates the researchers to improve the forensic schemes by revealing the limitations of forensic techniques [3]. 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 [34] is to reveal the introduced footprints related to the particular image processing operation in the presence of a corresponding anti-forensic attack. Mostly, counter anti-forensics schemes rely on some of the anti-forensic attack footprint and at a particular time can capture a particular attack. These counter anti-forensics schemes do not work for anti-forensics approaches related to the other image processing operation. Therefore, the researchers are much inspired to design a multi-purpose counter anti-forensics method which is alone proficient of detecting different anti-forensics approaches depends on various image processing methods. It is worth noting that robustness of anti-forensic schemes can be evaluated by considering many forensic attacks. On the other hand, the efficacy of counter JPEG anti-forensics approach is evaluated against different anti-forensic attacks.

Digital image forensics is still a new and interesting area for the researchers and image anti-forensics field is even more contemporary [35]. It can be observed from the literature that there are more publications related to forensics than those on anti-forensics. The existing anti-forensic methods hide the artifacts of JPEG compression in [36] and adding noise to cover the traces left by filtering in [37] to conceal the footprints. However, some advanced forensic techniques [38 – 39] 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 [40]. From image anti-forensics point of view, forensic undetectability is much vital as compared to image quality. Any anti-forensic strategy is regarded ineffective if it is exposed by a certain forensic detector.

The present work firstly aims to develop an anti-forensic scheme for JPEG compressed images, with the goal of fooling forensic detectors by removing the artifacts of JPEG compression. Therefore, an approach which offers resistance to different forensic detectors and yields better balance between visual quality and forensic undetectability of image is needed. Numerous natural image statistical models are used in this framework. Moreover, some anti-forensic approaches are also integrated to enhance the forensic undetectability. By following this approach, the desired JPEG forgery is attained with superior image quality and forensic undetectability.

1.5.1 Categorization of Digital Image Anti-Forensics Techniques

Anti-forensics schemes behave like obstacle for forensic study as they conceal the footprints utilized by forensic detectors and thus limit the capability of the detector. Hence, it inspires the research community to work in the area of digital image forensics. Three classes of anti-forensic techniques are presented in [3] as follows:

1.5.1.1 Robustness versus Security

The robustness or security flaws of digital image forensics are misused by the forgers for the purpose of anti-forensics. Initially, the robustness refers to the reliability of the digital image forensics under reasonable post-processing operation. For instance, numerous forensic techniques do not provide acceptable results for the images processed with strong JPEG compression. Hence, such kind of post-processing operation can work as an anti-forensic method, till it is capable to preserve the forgeries from the recognition by forensic techniques. Secondly, the image forensics security refers to its capability of revealing the intentionally hidden footprints of reliable post-processing. The flaws of the image model utilized by image

forensic methods are exploited by the image counterfeiters. The capable anti-forensic approach can create image forgeries moving away from the decision zone of trustworthy images [3].

1.5.1.2 Post-Processing and Integrated Attacks

In case of post-processing anti-forensic attacks, the forensic detectors can't detect these images because the anti-forensic attacks conceal the traces left by JPEG compression that are used by forensic detectors for image forensics. In contrast, the image generation process is directly interfered by integrated the anti-forensic attacks [3].

1.5.1.3 Targeted and Universal attacks

The anti-forensic technique is considered a target when the flaw of a specific forensic tool is exploited by an anti-forensic technique. It is also likely that some other forensic algorithm based on improved image models can detect such kind of anti-forensics. During the universal anti-forensic physical attack, the statistical properties of the generated forgeries are preserved to a greater extent, so that it goes on untraceable by the unfamiliar forensic detectors.

1.6 Motivation

JPEG is a commonly used compression scheme that is widely used in digital cameras and software used in processing of image [41]. Furthermore, according to [42] around 74.2% of websites are rely on the JPEG formatting. As a result, JPEG compression has become vital in many image forgeries. When a section of one image is copied on another image with dissimilar quality and it is saved under another quality factor in a forgery creation scenario, the final image is double JPEG compressed. In this way, compression detection introduces a significant effect in digital image authenticity [7], [43 – 44]. On the contrary, JPEG compression is the basis of most detectors used in the digital forensic. Proficient anti-forensic approaches, which are helpful and challenging in the improvement of forensics, has to be develop to determine the capabilities of the above detectors.

The idea of the proposed JPEG anti-forensics was motivated by the work done by the researchers in [45 – 47]. The study of these works reveals various aspects that can be used for the further enhancement of anti-forensics. For example, JPEG anti-forensic approach for concealing

of any traces left behind after JPEG compression is proposed in [48]. The dithering process is employed in [48] to smooth the histogram as it fills the gaps of histograms in the complete sub-bands at the cost of degradation in the visual effect of the image and also forensic undetectability.

Further, research presented by Fan *et al.* in [47] motivates for further investigations on countering JPEG anti-forensics schemes. Therefore, to develop a forensic method for identification of compression artifacts in JPEG anti-forensics is desirable. Further, out of numerous available anti-forensic schemes, conceal the footprints related to first order statistics. Therefore, a second-order statistical forensic analysis can be used to identify the compression elements even after the employment of anti-forensic attack.

1.7 Research Objectives

Based on the initial studies, literature survey and the understanding established, the following objectives were proposed:

1. To study and analyze the existing forensics and anti-forensics techniques for JPEG compression.
2. To propose the anti-forensic technique for JPEG, compression in DCT domain by removing the compression artifacts in order to fool the existing forensic detectors.
3. To evaluate the robustness of the proposed scheme against different types of forensic attacks.
4. To propose the forensic technique to detect the JPEG compression artifacts with a comparative study.

1.8 Research Methodology

The main emphasis of the research work is to enhance the digital image anti-forensic and forensic techniques based on JPEG compression. Thus, available anti-forensic and forensic techniques for JPEG 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 an anti-forensic scheme for JPEG compression via rectification of the compressed artifacts in both spatial and DCT representation. The analysis would be carried out by considering the DCT coefficients based histogram obtained with the given image. The analysis of histogram provides the information of the compression artifacts and these artifacts would be removed by using various

techniques such as histogram smoothing, filtering and by fulfilling the histogram gaps. Further, shifted block DCT and DFrCT approaches with TV-based deblocking are proposed to efficiently hide the JPEG compression artifacts and provide outstanding results in terms of forensic undetectability and image visual quality.

Moreover, a statistical analysis of higher orders, for forensic scheme based on MTPMs, is performed to design a counter anti-forensic scheme for JPEG format. In this examination, a feature is generated based on a statistical analysis of higher order by revealing the artifacts introduced during the anti-forensics of JPEG format. Further, considered anti-forensic and forensic methods for JPEG format are evaluated by considering the UCID and BOSSBase image datasets. The robustness of the proposed techniques is evaluated against different attacks. Further, comparative analysis with existing techniques has been done. All the simulations are performed in MATLAB-R2016a using a PC with specification, 3 GB RAM and 2.13 GHz CPU. Finally, flow of the research work carried out in this thesis is provided in Figure 1.9.

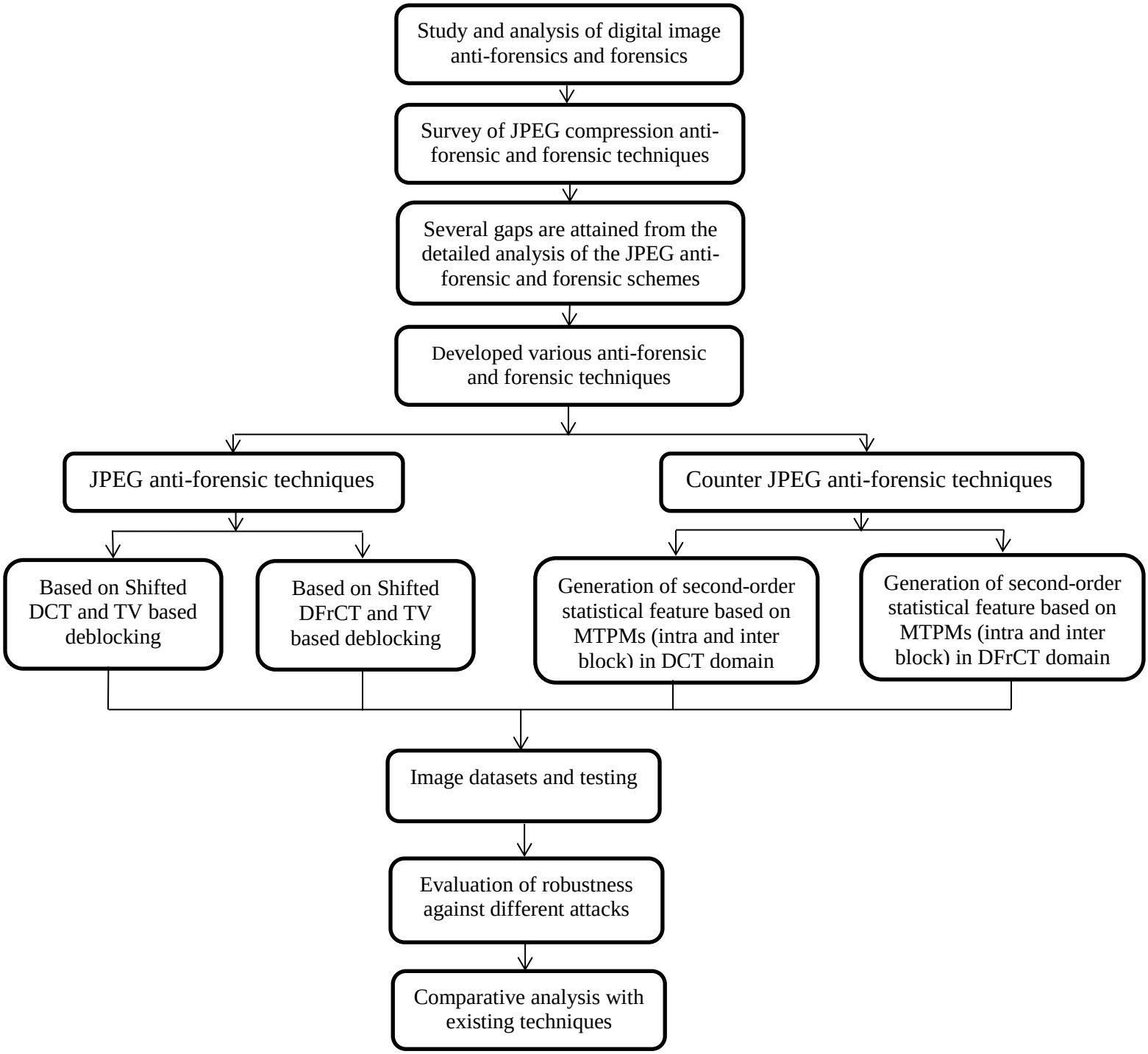


Figure 1.9: Flowchart of the work done.

1.9 Contribution of Research Work

The investigation the different anti-forensic and forensic techniques for JPEG compression has been done in order to set up the establishment for the research work. The detection and examination of JPEG compression artifacts in an image assist the examiner to find the genuineness of an image. In many image forgery scenarios, an image is tampered through cut-paste or splicing operation. Here, a sub-image part is extracted from a never compressed image or from the image which is compressed with different quantization tables. The final image is saved again by utilizing the JPEG compression format which results in the occurrence of JPEG compression artifacts.

The major contributions of the presented work are as follows:

- Most of the techniques available in the literature for the removal of JPEG blocking artifacts work in the spatial domain. This work considers the DCT domain as well as spatial domain to remove the JPEG artifacts.
- The techniques available till date provide forensic undetectability but with the reduction in image visual quality due to the dithering operation (histogram smoothing) of anti-forensic techniques. This dithering operation results in the addition of unwanted grainy noise which reduces the image visual quality.
- An anti-forensic technique based on shifted block DCT approach is proposed. The proposed anti-forensic approach led to the addition of dithering noise itself without the need of any adaptive dithering model. Therefore, reduces the forgery generation time by reducing the computation cost.
- The proposed technique efficiently removes the compression artifacts and fools the forensic techniques in terms of lower values of forensic detector measures.
- Moreover, the proposed scheme provides good tradeoff between image visual quality and forensic undetectability.
- A better anti-forensic technique based on DFrCT approach is presented in this work. The extra degree of freedom provided by the DFrCT approach helps to design an improved JPEG anti-forensic technique.

- The proposed scheme employs a shifted block-based DFrCT approach instead of DCT along with TV-based deblocking. The proposed method performs histogram smoothing without adding any dithering signal, i.e, it is capable of applying dithering by itself, thereby reducing the computation time significantly.
- The robustness of the presented approach is confirmed against several forensic detection attacks. Moreover, the presented technique has raised a serious concern regarding the robustness of forensics techniques.
- It is a difficult task to fool the machine learning based detectors. Therefore, the presented approach is further evaluated by machine learning based detectors. The robustness of the presented approach is also analyzed with the double JPEG compression detectors.
- The effectiveness of the proposed algorithm is confirmed on the basis of various performance metrics when compared to the existing approaches. The proposed approach provides good trade-off among the quality of image and forensic undetectability.
- Most of the existing JPEG anti-forensic techniques remove the footprints based on first-order statistics, but it is very difficult for these techniques to properly conceal the footprints based on second-order statistics. Therefore, a JPEG forensic technique with MTPMs based second-order statistical analysis in DCT domain is proposed to reveal the JPEG compression artifacts even in the presence of an anti-forensic attack.
- MTPMs based second-order statistical analysis is initially employed in image steganalysis but has not been used in the existing literature for JPEG forensics for countering JPEG anti-forensics.
- Most of the efficient JPEG anti-forensic techniques are not considered during the performance evaluation of existing JPEG forensic techniques due to different strengths. Due to these different strengths of anti-forensic techniques, a forensic method designed to counter a particular anti-forensic technique is not able to counter another anti-forensic technique. Therefore, this problem of different strengths of anti-forensic techniques is resolved in this work by designing an efficient second-order statistical feature.
- The presented counter JPEG anti-forensic technique further employed DFrCT instead of DCT. The presented approach based on MTPM together with DFrCT approach performed a second-order statistical analysis to detect the footprints left by the anti-forensic techniques.

- The proposed counter JPEG anti-forensic framework provides better detection results against various anti-forensic techniques when compared to the existing techniques.

1.10 Thesis Organization

The thesis is arranged as follows:

Chapter 1 describes the general introduction and depiction of the thesis. It provides detailed information associated with history of image tampering, digital image anti-forensics and forensics with their classification, motivation, contributions of the research work and thesis organization.

Chapter 2 summarizes the existing literature related to various anti-forensic, JPEG compression forensic, and counter anti-forensic techniques. Various evaluation metrics are also discussed based on which the performance of several forensic and anti-forensic techniques is evaluated. Moreover, the detailed information regarding the image datasets, settings, and forensic testing required for evaluation purposes is also discussed. Furthermore, this chapter includes the objectives, research gaps, and research methods.

Chapter 3 introduces an improved JPEG anti-forensic framework by considering JPEG artifacts both in DCT as well in spatial domain to disguise the existing forensic detectors. The goal of the suggested JPEG anti-forensics is to achieve better image visual quality and forensic undetectability. The proposed technique is robust against various forensic detectors and results in better tradeoff among the visual quality of the image and forensic undetectability in comparison to the existing state-of-the-art anti-forensic techniques.

Chapter 4 elaborates JPEG anti-forensic algorithm which can deceive the scalar-based and machine learning-based forensic detectors by hiding the artifacts of compression in DFrCT domain. The presented technique possesses the advantage of having an additional fractional parameter to increase its flexibility. 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. Moreover, the presented technique has raised a serious concern regarding the robustness of forensics techniques because it is able to beat most of them.

Chapter 5 describes counter JPEG anti-forensic scheme by considering the second-order statistical analysis based on MTPMs in DCT domain. The capability of the proposed forensic technique is confirmed from the extensive experimental analysis. The experiment results confirm that the presented approach outperforms the existing schemes in countering various JPEG anti-forensic approaches.

Chapter 6 describes the further extension of counter JPEG anti-forensic framework presented in previous chapter. In this chapter, the proposed approach employed DFrCT instead of DCT. The presented approach based on MTPM together with DFrCT approach performed a higher order statistical analysis to detect the footprints left by the anti-forensic techniques. The ability of the work is authenticated from the extensive experimental analysis. The proposed approach provides better detection results in terms of minimum decision error when evaluated against various anti-forensic attacks when compared to the existing techniques.

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

CHAPTER 2

LITERATURE SURVEY

This chapter summarizes the existing literature based on various forensic and anti-forensic approaches related to JPEG compression. Various metrics for evaluation are also discussed based on which the performance of several anti-forensic and forensic techniques is calculated. Moreover, the detailed information regarding the image datasets, settings, and forensic testing required for evaluation purposes is also discussed. Furthermore, this chapter includes the objectives, research gaps, and research methodology.

2.1 JPEG Forensics and Anti-Forensics

This section discusses the basic theory of JPEG compression and its artifacts in the domain of DCT transform and spatial. Moreover, various study related to different JPEG anti-forensic methods, JPEG compression detection methods, and Counter JPEG anti-forensic methods are also considered.

2.1.1 JPEG Compression

JPEG is an extensively used compression standard by various cameras and photo editing software that was developed by members of ISO and ITU in 1980 [49]. Intending to support numerous applications for continuous-tone images, the JPEG standard aims to be generic. The JPEG compression is categorized into two types: lossy and lossless compression. The baseline system is used for the lossless and the predictive system is used for lossy compression. Lin *et al*. [50] introduces a technique to calculate the coding efficacy based on the degree of distortion. The foremost motive of data compression is to reduce the data correlation by employing DCT as given in Figure 2.1. DCT transforms the data present in the time domain to the frequency domain. The image data can be compressed by suppressing its high-frequency component, since human visualization is less sensitive to high frequency.

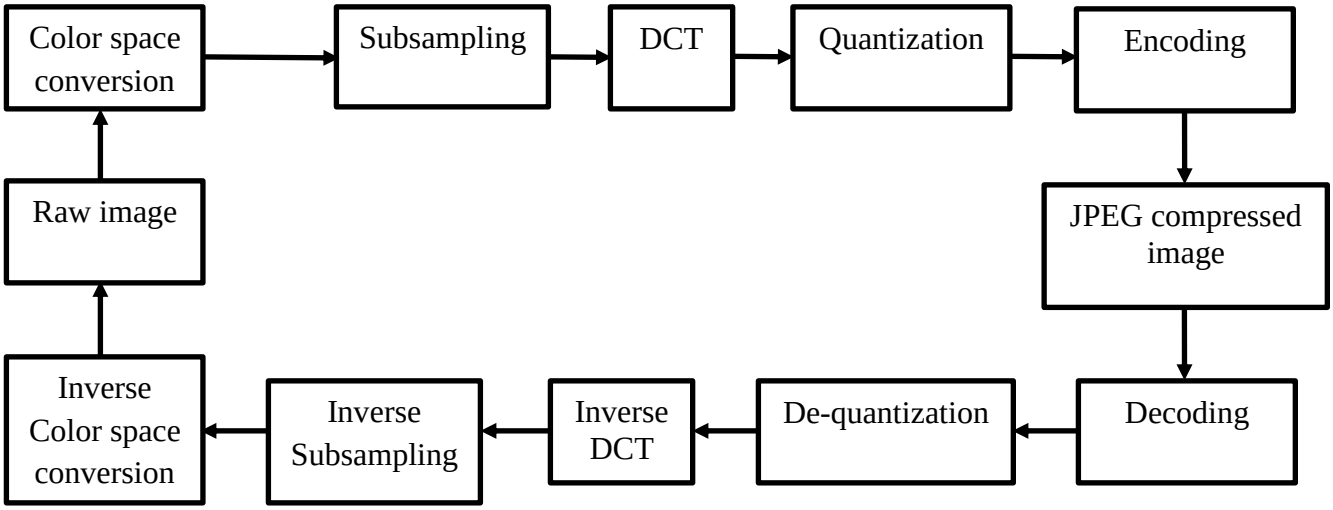


Figure 2.1: Basic steps in JPEG compression.

Initially, the image $\boldsymbol{I}$, a new uncompressed is divided into L blocks of 8×8. Then, the DCT of every pixel block is taken to get its coefficients block. Because of the orthogonal linear nature of DCT, the mapping of this procedure can be stated as matrix multiplication, symbolized by $D_{matrix}\boldsymbol{I}$, where D_{matrix} is a DCT block matrix. Then, the (r, c)-th $(r, c = 1, 2, 3, \dots, 8)$ represented by DCT coefficient $(D_{matrix}\boldsymbol{I})_{r,c}^{l}$, where $l = 1, 2, 3, \dots, L$ quantized uniformly as [51]:

$$(q_{block}(D_{matrix}\boldsymbol{I}))_{r,c}^{l} = round\left(\frac{(D_{matrix}\boldsymbol{I})_{r,c}^{l}}{q_{r,c}}\right) \tag{2.1}$$

Where, $round(.)$ is the rounding function and $q_{r,c}$ denotes the (r, c)-th entry of the quantization table matrix. Consequently, these quantized DCT coefficients $q_{block}(D_{matrix}\boldsymbol{I})$ are encoded losslessly. For decompression procedure, first decoded bit stream yields the quantized coefficient of DCT which is further de-quantized with a corresponding step size of quantizer which is represented as [51]:

$$(q_{block}^{-1}(q_{block}(D_{matrix}\boldsymbol{I})))_{r,c}^{l} = (q_{block}(D_{matrix}\boldsymbol{I}))_{r,c}^{l} \times q_{r,c} \tag{2.2}$$

Further, Inverse Discrete Cosine Transform is used to get the spatial domain. This procedure can be denoted by multiplying the de-quantized DCT coefficients with IDCT matrix as

$D_{matrix}^{-1} q_{block}^{-1}(q_{block}(D_{matrix}\boldsymbol{I}))$. Lastly, truncation and rounding error which is symbolized by $RT_{error}(.)$ is employed to make the pixel values an integer in the range [0, 255], thus the decoded JPEG image is achieved as [51]:

$$\mathcal{T} = RT_{error}(D_{matrix}^{-1} q_{block}^{-1}(q_{block}(D_{matrix}\boldsymbol{I}))) \tag{2.3}$$

There are a few issues related to JPEG compression. The compressed image with blocking artifacts is generated by dividing an image into 8×8 blocks [51 – 52]. There is a lack of smooth transition among the blocks in a compressed image. Each block is transformed as well as quantized independently. The decoupling of the image occurs when we try to exploit the consistency of a region that is greater than 8×8 block. Since DCT is calculated from samples of the cosine function, thus, it works best only when input data is periodic. DCT is a global transformation matrix where each element is affected by each other element of the input matrix. Consequently, if there is any disturbance in the input matrix, it also disturbs each element in the resulting transformed matrix. A digital image goes through numerous steps in its life cycle. Starting from acquiring an image, coding, then editing is also performed on it in order to enhance its quality. Further, this image can undergo its feature enhancement, for instance, brightness adjustment, contrast, and correction of the gamma function. These enhancement techniques produce pixel modifications or inconsistencies in the resulting image which are used by the forensic detectors for further investigation.

2.1.2 Artifacts of JPEG compression

There are two types of artifacts in JPEG compressed images i.e blocking artifacts in spatial and quantization artifacts in DCT domain [51], [53]. Further, analysis of these artifacts shows the compression history of a digital image under examination. The quality factor of 50 is used to compress the uncompressed image of Lena to demonstrate the induced compression artifacts as shown in Figure 2.2. The histograms of DCT coefficients of (4, 4) sub-band related to original and JPEG compressed Lena image are given in Figures 2.2 (c) and (d) respectively. It is noticed from the histograms of DCT coefficients that in case of the compressed image, maximum neighboring bins coefficients are moved to the center bin since most of the quantized coefficients become zero. It is noted that in JPEG compression, rounding and truncation are responsible for DCT coefficient error. This DCT coefficient error is not counted in Figure 2.2 (d).

2.1.2.1 Quantization Artifacts

The quantized DCT coefficient $(q_{block}(D_{matrix}I))^{l}_{r,c}$ is multiplied with its corresponding quantization step which results in the de-quantized DCT coefficient and is represented by $(q^{-1}_{block}(q_{block}(D_{matrix}I)))^{l}_{r,c}$ [51]. In the compressed image, DCT coefficients assemble themselves in the shape of comb-like distribution as presented in Figure 2.2 (d). The DCT coefficients of compressed image are available in periodic spacing. This form of the artifacts generally termed as quantized artifacts in DCT domain. These artifacts are generally used in the forensic study of the image tampering based on JPEG compression.

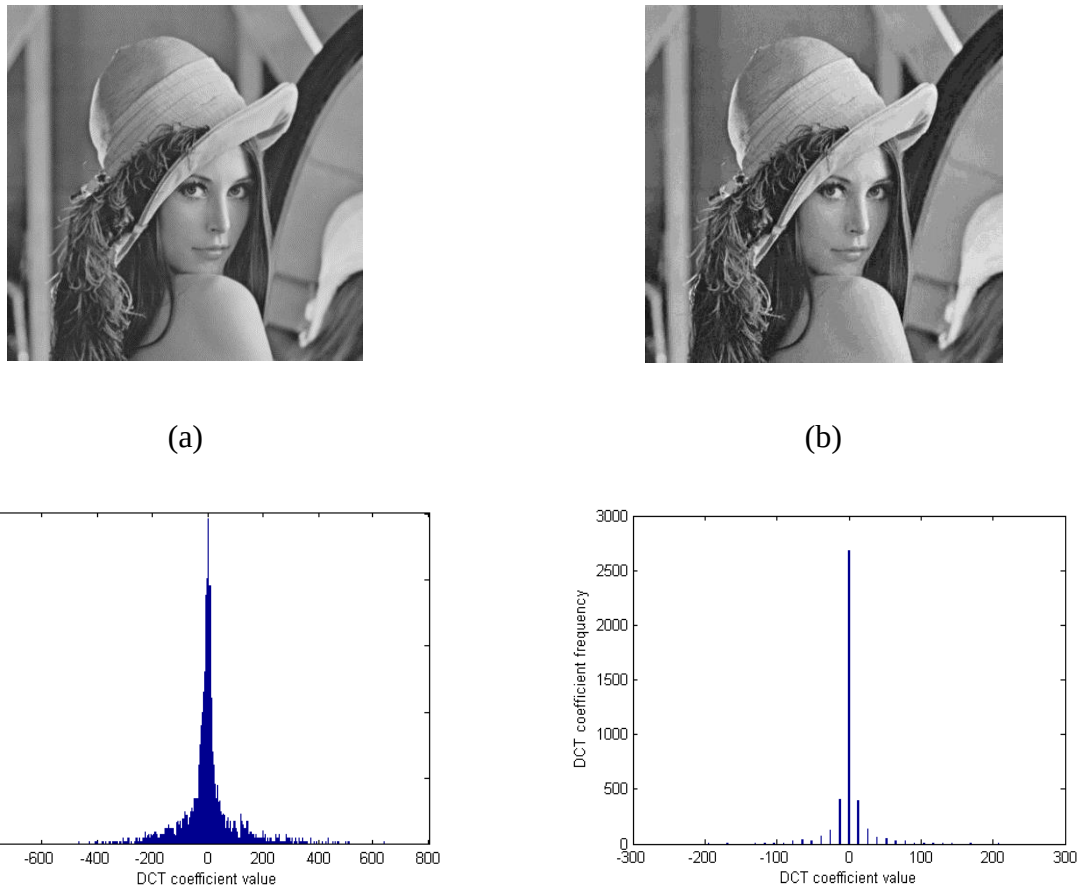


Figure 2.2: Lena images (a) Uncompressed, (b) JPEG with 50 as quality factor (c) Histogram representation of an uncompressed image with DCT coefficients of sub-band (4, 4) (d) Histogram of compressed image with 50 as quality factor.

2.1.2.2 Blocking- artifacts

JPEG compression causes spatial blocking artifacts by virtue of a block-based DCT transform as shown in Figure 2.2 (b). Firstly, in the JPEG compression method, the image is divided into non-overlapping blocks of 8×8. Further, transformation and quantization is used which results in the gaps or blocking artifacts across the block borders [1].

The compression noise is usually correlated in the spatial domain as pointed by Robertson and Stevenson [54]. For moderately smooth signal, most of the energy is contained by the lower range of frequency. In contrast, higher range of frequency has comparatively low energy and thus, adds less quantization noise. The subsequent positions to the block boundaries have large error variance because low-frequency sub-bands have extensive quantization noise due to DCT basis functions as exhibited in Figure 2.3. The textured region of the digital image is an illustration of a complex signal and in this case, the middle of the block has high error variance than the boundaries.

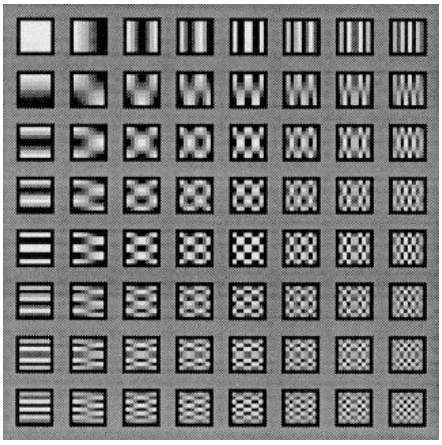


Figure 2.3: DCT basis functions.

2.1.3 Discrete Fractional Cosine Transform

In many fields of science and engineering, the Fourier Transform (FT) is used. Heat conduction and diffusion, acoustics, statistics, physics, optics, antenna and array processing, electrical engineering, are some domains where this transform is extensively used [55]. The Fractional

Fourier Transform (FRFT) is the generalization of the classical FT [56]. It was first introduced in 1980 by Namias [57]. In the 1990s, Pei *et al.* undertook a lot of work to consolidate FrFT [58 – 60]. FrFT provides additional degree of freedom in various applications of signal processing [61] such as signal processing, beam shaping, pattern recognition, filtering, etc. which is not available in FT. Thus, the FrFT can be used to replace the FT and related concepts [62]. The Discrete Fourier Transform (DFT) came into existence with the advent of computers to analyse the FT of discrete-time signals. The introduction of DSP processors and the fast Fourier transform (FFT) algorithm has significantly strengthened this capacity. A necessity for discretization of FrFT arose along similar lines. However, there are numerous discrete fractional Fourier transform formulations when analysing FrFT in the discrete domain (DFrFT) [63 – 65]. These definitions are classified according to the methodology used for calculations by Pie *et al.* [66]. In the field of digital image processing, compression and encryption are becoming very imperative issues. Image compression using discrete cosine transform (DCT), provides low bitrate representation by preserving a high visual quality of decompressed image [67]. Similar to FrFT, Discrete Fractional Cosine Transform (DFrCT) is introduced in [68] to explore the advantage of extra degree of freedom. The DFrCT is a generalization of the DCT. There is an extra degree of freedom in DFrCT $\alpha = a\pi/2$, where $'a'$ can range from zero to unity [69 – 70] which can be used in any situation where DCT is found to be useful. It's also worth noting that, this methodology is used in a variety of image processing applications, including diabetes screening using iris scans, verification of online handwritten signature and satellite/aerial images [71 – 73]. The additional fractional parameter $'\alpha'$ in DFrCT gives more flexibility when designing a system, in contrast to DCT [74]. This fractional parameter can be used to solve problems that the DCT is unable to address. The basic equation for 2D-DCT with (2.4) and (2.5):

$$Z(k_1,k_2) = \left(\frac{2}{M}\right)^2 \left(\frac{2}{N}\right)^2 \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \Lambda(i)\,\Lambda(j) \cos\left[\frac{\pi k_1}{2M}(2i+1)\right] \cos\left[\frac{\pi k_2}{2N}(2j+1)\right] z(i,j) \quad (2.4)$$

$$\text{where, } \Lambda(i),\Lambda(j) = \begin{cases} \frac{1}{\sqrt{2}} & for\ i,j = 0 \\ 1 & ohterwise \end{cases} \quad (2.5)$$

The size of the input image is denoted by M and N. The intensity of a pixel in the i^{th} row and j^{th} column is represented by $z(i,j)$. The DCT coefficients in row k_1 and column k_2 are represented

as $Z(k_1, k_2)$. The exclusive eigenvectors in the cosine case are produced using the even Hermite–Gauss eigenvectors of the Fourier matrix D_N^a in DFrCT, which uses the eigen decomposition of the DCT kernel. In order to determine DFrCT coefficients, the N-point DFrCT kernel matrix is specified as [68], [75 – 76]:

$$C_{N,\alpha} = V_N D_N^a V_N^T = V_N D_N^{2\alpha/\pi} V_N^T$$

$$C_{N,\alpha} = V_N \begin{bmatrix} 1 & & 0 \\ & e^{-2j\alpha} & \\ & & \ddots \\ 0 & & e^{-j2(N-1)\alpha} \end{bmatrix} V_N^T \quad (2.6)$$

where, rotation angle $\alpha = a\pi/2$ i.e. $0 < |a| < 2$, $V_N = [v_0|v_2|\cdots|v_{2N-1}|]$ and diagonal matrix D_N having the same eigenvalues as matrix V_N column eigenvectors. $C_\alpha = C_{N,\alpha} z$ calculates the DFrCT of signal $z(n)$ for $z = [z(0), z(1), \ldots\ldots, z(N-1)]^T$ [77]. To the best of our knowledge, the existing literature of image forensics and anti-forensics has not been explored in the Fractional domain.

2.1.4 Forensic Examination of JPEG Compressed images

Digital examination of an image provides the significant information related to the camera or device attributes used for the shooting. On the basis of this data, one can discover that the considered image is tampered or not [78 – 79]. A digital camera image is compressed one time for shooting, then again, if the same image is decompressed and re-saved using different compression methods during forgery generation, the resulting image is termed as doubly compressed image. As a result, the forensic detective can effortlessly identify the image manipulations by exposing the double compression artifacts [80]. Several acquisition systems and related devices use JPEG compression for images in advanced analysis. The problems faced during the analysis of an image may be divided into two categories based on validity of the visual document, and the type of the device used for the acquisition of image [81].

2.1.4.1 Image Tampering detection by analyzing the artifacts of JPEG compression

Several techniques have been reported in the literature for image tampering detection. These techniques comprise of coding-based schemes, acquisition-based schemes, and editing-based

schemes to detect the source of digital image and to authenticate its legitimacy without any previous knowledge [82]. Stamm *et al*. [83] discussed the progression of image forensics over the last few years. The useful information related to the numerous applications of information forensics is provided. This information can be utilized in the future to produce effective forensic procedures [83]. Various methodologies are used to examine the statistical distribution of DCT coefficient values. The performances of above methods are calculated, considering various image datasets, compression ratio, and various sorts of forgeries [84]. The histogram of an image is used to determine whether it is JPEG compressed or not. Several statistical approaches are presented by Popescu and Farid [85] to discover the traces of digital tampering in the lack of any digital watermark or signature. The statistical relationships among the neighboring pixels of an image become inconsistent due to the digital manipulations. Consequently, these statistical relationships are scrutinized to validate the legitimacy of digital images [85]. An effectual technique based on machine learning (SVM classifier) is introduced to distinguish between single as well as double compressed JPEG image. Primarily, difference JPEG 2-D arrays achieved by measuring 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 improve the DJPG compression artifacts. Then, Markov random process is used to model difference 2-D arrays to apply second-order statistics [86]. Furthermore, Thing *et al*. [87] recommended a JPEG compression detection method based on a periodic function to detect the altered areas. Authors in [88] suggested a method for examining of doubly compressed image with the same quantization matrix. A unique approach for identifying DJPG compressed images is suggested in [89] based on primary quantized matrix. Moreover, [90] describes a method for determining the DJPG compression using the identical quantization matrix.

Furthermore, [91] presents a procedure which expose copy-move falsification based on high JPEG compression artifacts. Features extraction is accomplished by applying the Fast Fourier Transform (FFT), Singular Value Decomposition (SVD), and Principal Component Analysis (PCA) while their cascading matchers are used for feature matching. Further, the upper left corners pixels from detected duplicate blocks are utilized for examination of visual effects. This approach is robust against different attacks like Gaussian noise, JPEG compression, and blurring attacks. A fast and effective method for copy-move detection using hierarchical feature point matching is presented by Li and Zhou [92]. This method resolved the problem of keypoint

matching over an immense number of key points. An iterative localization method is also proposed to reduce false alarm rate and a perfect localization of tampered areas by applying the scale, dominant alignment, and color data of each key point. Another, detection technique is presented by Khuspe and Mane [93] to detect tampering in the image based on k-means clustering and Mirror Invariance Feature Transform (MIFT). After K-means clustering, the key points are mapped to combined histogram vector [94]. Further, this histogram is applied to the multiclass SVM for classification. The same process is accomplished in case of the testing phase. Authors in [95] presents identical quantization table for image recompression during duplication, which assures that the grid of the pasted piece is not aligned with the previous one.

During the JPEG compression, the blocking artifacts left behind are used as an indication of compression. A forensic methodology is proposed in [96] based on the fact that in the uncompressed image, the pixel difference taken over the boundaries of 8×8 block and within the blocks should be the same. The blocking signature parameter is based on the difference of energy among the histograms and it can be denoted as:

$$K_F = \sum_n |H_1(n) - H_2(n)| \tag{2.7}$$

Where, $H_1(n)$ and $H_2(n)$ are normalized histograms based on block borders and inside the block, respectively based on pixel value differences. Furthermore, a forensic procedure is proposed in [97] to identify the JPEG compression which does not need an original image and thus called a blind blocking artifact measurement technique. The goal of this technique is to identify and calculate the strength of a blocky signal. So, the blocking artifacts measures are commonly involved in the forensic analysis of JPEG compressed images.

An effective forensic detection procedure is presented in [98] for DJPG compressed images by examining the histograms of DCT coefficients. These histograms comprise specific periodic artifacts that are investigated to generate the feature vector for classification using SVM. Various quantization steps have been utilized for secondary and primary compressions which produce certain asymmetrical statistical patterns in the histogram of Quantized DCT (QDCT) coefficients. Based on periodicity measure, a detection method is produced in [85] which depends on the fact that whether the Fourier transform of the histogram has specific artifacts or

not. In reality, image recompression has periodic artifacts and histogram gaps. Based on these artifacts/discontinuities, features are used to train the SVM classifier and hence to detect JPEG re-compression [99].

Furthermore, He *et al.* [100] presents a technique to classify tampered images due to various types of synthesizing methodologies, like alpha matting and inpainting in [101] and [102] respectively. Also, this method is the fastest method which reduces memory requirement and computational complexity, as it can be used to decompress the image in JPEG format completely. Process of detection becomes challenging when the original image presenting the non-tampered section is not a JPEG image. In this condition, the effect of double quantization of the non-tampered portion cannot be identified. Moreover, this technique also fails if the quality factor is kept low after image forgery. As a result, a forensic technique is suggested in [103] to display the image forgeries by examining the difference domain. The tested image is re-compressed at several quantization factors as well as compared with the certain tampered image, in this technique. The emergence of spatial local minima (JPEG ghost) among the certain image and its JPEG compressed version validates that the certain image is tampered with double compression. This methodology works for tempered area having lesser quality factor than the rest of image. Likewise, depending on the study of JPEG compression and features of blocking artifacts, specific technique is considered in [104] to represent blocking artifacts based on the symmetrical characteristics added by encoder. BACM displays a symmetrical outline for an original JPEG image. The operations like cropping and recompression can modify this symmetrical property. Consequently, features derived from BACM are used to train the SVM classifier to identify whether it is original or cropped or resaved JPEG image. The improved results are achieved provided quality factor during first compression is lesser than last compression. This technique is reliable for the large-sized forged area [104]. This methodology is further improved in [105] to localize the tampered area without any prior knowledge.

Further, the periodic nature of blocking artifacts is analyzed using a procedure suggested by Chen *et al.* [106] by producing a linear model which is function of pixel differences, and further, a periodic map using each pixel is constructed which is associated with this model. Finally, a peak window is extracted using the spectrum of the periodic pixel map. The peak energy distribution performs differently for single as well as DJPG compressed images. This property is

employed to obtain the statistical features from the peak windows for classification purposes. Besides, Chen *et al.* [107] recommended a robust forensic approach by executing the investigation of periodic characteristics of compressed JPEG image space and in DCT representation to detect both the block-aligned and misaligned recompression procedures. It is supposed that initially JPEG compression is used to compress the original image and all forgery procedures comprise recompression. It is also noticed that the performance of [107] is superior when compared to the BACM scheme [104] in many cases. Meng *et al.* [108] proposed a copy-paste block detection methodology by examining the artifacts of DJPG compression and it is perceived that these characteristics are closely associated with the quality factor. The copy-paste tampering interrupts the JPEG compression footprints of the resulting tampered image and it is detected that the DCT blocks are different for the two compressions.

Some procedures do not depend on the classifier to identify the existence of DJPG compression artifacts. These methodologies rely on a simple threshold detector. A single feature is calculated in [109] based on the integer periodic property DCT coefficients of each of block concerning the grid of preceding JPEG. Compression of JPEG image is detected by noticing the clustering of DCT coefficients close to a particular lattice. Bianchi and Piva [109] carried out the comparison with Luo *et al.* [104] technique and Chen *et al.* [107] technique by calculating their features on the same database and then these features are fed to SVM using radial basis function kernel. In comparison to method [104], method [109] detector is 5% to 15% more precise for equal-sized images. Though compared to the method [107], it has 10% to 25% more detection accuracy for minor-sized images.

A lot of detection approaches need prior knowledge of features corresponding to genuine and forged areas. To detect the forged area instinctively, a large number of image blocks are required to be processed, which also raises the computational load. The method [110] works on a specific JPEG image by discarding its DCT coefficients and quantization matrices for one Luma and two Chrominance (YUV) channels. This method is capable of identifying the tampered areas automatically, which is impossible with the prior methods.

The drawback of the technique [110] is that if x is the value of DCT coefficient and $H_0(H_1)$ specifies the hypothesis of being forged then the conditional probability $p(x|H_1)$ is calculated

conforming to the detected histogram of x. Such a histogram is the fusion of $p(x|H_1)$ and $p(x|H_0)$ for forged images. Hence for large forgeries, the histogram of x is estimated to be a poor approximation of $p(x|H_1)$ [111]. This limitation of [110] is solved in [111] by splitting the two conditional probabilities. It is also noticed that the efficacy of the procedure [111] is superior in comparison to the procedure [110]. An image tampering detection approach is presented in [112] based on the analysis of CFA artifacts by using MTPM. Furthermore, a second-order statistical analysis is conducted using MTPM in [113] for image manipulation detection. A study on Co-occurrence matrix and MTPM is performed in [114] by considering JPEG compression.

2.1.5 Anti-Forensics technique for JPEG Compression

Anti-forensic scheme for JPEG compression presented by Stamm *et al.* [48], outperforms the approach based on DCT coefficients histogram. Basically, dithering operation [48] is used in smoothing of DCT histogram, which is further based on the Laplace distributions of the AC coefficients. It is noteworthy to mention that dithering process presented in [48] effectively deceived the forensic detection approach suggested in [96]. Again, Stamm *et al.* [115] proposed a median filtering-based deblocking operation to disguise spatial domain forensic detection operation. Advanced forensic detectors are presented in [116 – 117] to detect the traces left by anti-forensic scheme presented in [48]. Also, the anti-forensic methodology proposed in [48] dramatically reduces image quality which can be restored by perceptual dithering of [118]. In [119], an image deblocking approach is presented by using sparse representation. Moreover, TV-based deblocking method is suggested in [120] to reduce the blocking artifacts as well as ringing effects. In [121], a deblocking operation is suggested by solving the weighted total variation optimization problem.

Li *et al.* in [122] presents novel forensic technique for the detection of anti-forensically processed JPEG images. However, dithering process disturbs the correlation between the intra block and inter-block of the image. The original JPEG uncompressed and decompressed images are used to classify forged image based on transition matrix of DCT coefficients. Further, the JPEG forgery presented by Stamm *et al*. in [123] fails to mislead the machine learning approach based on the steganalysis in [124]. In [46], an anti-forensic methodology based on variable energy reduction is presented to mislead current forensic tools in the spatial domain. Further,

anti-forensics of DJPG compression is presented in [125] and machine learning based steganalysis forensic approach is presented in [38].

An anti-forensic approach in [48] used to hide the footprints of JPEG compression using dithering operation by smoothing the DCT histogram. Dithering operation presented [48] fills up the gaps in DCT histograms of all the sub-bands to remove the compression artifacts. Hence, the resulting image after dithering can be acknowledged as an anti-forensically processed image. The Laplacian distribution AC coefficient of uncompressed image is defined as:

$$P(Y = y) = \frac{L_p}{2} e^{-L_p|y|} \tag{2.8}$$

where, Y is the DCT coefficient before the compression for (r, c)-th sub-band and γ is a Laplacian factor.

Further, the quantized AC coefficients are modeled as Laplace distribution in discrete form for JPEG image. The distribution for the (r, c)-th sub-band coefficients, with step $q_{r,c}$ of the quantization matrix q, is given as [48]:

$$P(Z = z) = \begin{cases} 1 - e^{-\frac{L_p q_{r,c}}{2}} & if\ z = 0 \\ e^{-L_p|z|} \sin\left(\frac{L_p q_{r,c}}{2}\right) & if\ z = k q_{r,c} \\ 0 & otherwise \end{cases} \tag{2.9}$$

where, $Z = q_{r,c}.round(Y/q_{r,c})$. Also, MLE is used to generate the parameter $L_p = L_{p_{mle}}$. The discrete nature of Laplacian distribution results in comb-like DCT histograms. Therefore, DCT coefficients can be reconstructed approximately using histogram of each sub-band and noise is added to each of the sub-band as follows:

$$D = Z + N_i \tag{2.10}$$

Here, D denotes the dithered coefficient of the image and N_i represent the additional noise. Also, the noise distribution of the coefficient Z with zero value at the (r,c)-th location is denoted as [48]:

$$P(N=n|Z=0)=\begin{cases}\frac{1}{c_0}e^{-L_p|n|} & if\ \frac{-q_{r,c}}{2}\le n<\frac{q_{r,c}}{2}\\ 0 & otherwise\end{cases} \quad (2.11)$$

Where, $c_0 = 1 - e^{-L_p q_{r,c}/2}$.

Further, the distribution of the non-zero coefficient can be given as:

$$P(N=n|Z=z)=\begin{cases}\frac{1}{c_1}e^{-sgn(z)L_p(n+q/2)} & if\ \frac{-q_{r,c}}{2}\le n<\frac{q_{r,c}}{2}\\ 0 & otherwise\end{cases} \quad (2.12)$$

Where,$c_1 = (1/L_p)(1 - e^{-L_p q_{r,c}})$.

Moreover, an optimal anti-forensic scheme is presented in [126] relies on the convex cost function. This method fool the forensic methods based on first-order image histogram. A similar scheme for JPEG anti-forensic is proposed in [47] which is comprising of four steps. First step includes first-round TV-based deblocking and second step is smoothing of histogram. Whereas, second round TV-based deblocking and operation of decalibration are third and fourth steps, respectively. TV-deblocking procedure fills up gaps in the histogram of DCT coefficients. Also, an adaptive local dithering model [47] is applied to fill the gaps completely followed by applying Laplace and uniform distributions. Thereafter, the blocking artifacts in spatial domain are removed with the help of TV-based deblocking. It is noticeable that the second round of TV-based deblocking yields with a JPEG forgery which can fool almost all forensic detectors.

2.1.6 Counter Anti-Forensics approaches based on JPEG compression

According to [45], [116], [127] the dithering operation of anti-forensic techniques [48] reduces the quality of an image. To overcome this effect, Valenzise *et al*. [127] built an effective forensic detector by examining the noise impacts of doubly compressed image based on TV. Quality factors $q = \{1, 2, 3, \ldots, 100\}$ are used to re-compress the images under test. Thereafter, (q) is used to calculate the TV of doubly compressed images as:

$$K_V = \max_{q\in\{1,2,3,\ldots,100\}} \Delta TV(q) \quad (2.13)$$

where,$\Delta TV(q)$ is the finite backward difference of first-order and is given as:

$$\Delta TV(q) = TV(q) - TV(q-1) \tag{2.14}$$

Lai and Bohme suggested a calibration-based detector in [117], enhanced version of anti-forensic technique for JPEG presented in [48]. Variance of sub-bands of a certain image X is compared with calibrated version X_{cal}. The calibration parameter K_L is given as:

$$K_L = \frac{1}{28}\sum_{k=1}^{28}\left|\frac{var(D_k X) - var(D_k\, X_{cal})}{var(D_k X)}\right| \tag{2.15}$$

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

Data hiding proposed by [48], [115] is employed by Li *et al.* [122] for JPEG steganalysis. Intra and inter-block based image statistics are customized by the anti-forensic techniques. Markov Transition Probability Matrix (MTPM) can be used to measure the changes in [124]. On the other hand, the Subtractive Pixel Adjacency Matrix (SPAM) is used to avoid anti-forensics of JPEG compression [127].

Further, JPEG blocking artifacts can be recognized with the help of measure [46] as:

$$K_U^p = \left|B_{gr}^p(X) - B_{gr}^p(X_{cal})\right| \tag{2.16}$$

where, B_{gr}^p is the blockiness based on gradient, given as the l_p norm of weighted gradient obtained from 8×8 block borders of four adjacent pixel values. By varying the parameter p, we can obtain related different measures. Furthermore, [128] present an autoregressive model for a multi-purpose forensic detector.

Further, [129] presented an adversary-aware compression recognition for DJPG based on SVM classifier which is capable of detecting the compression traces. A huge number of features vectors are used to identify the footprints in the DJPG compression. However, due to unavailability data of all the anti-forensic attacks, only limited number of data is used for training process.

Based on intensive literature survey numerous forensic schemes have been outlined which are used to propose forensic and anti-forensic approaches:

- K_F: JPEG compression-based detector for blocking artifacts [96].
- K_F^q: detector based on table of quantization estimation [96].
- K_{Weiqi}^q: detector based on step size of quantization estimation [53].
- K_{Weiqi}: detector based on JPEG identification [53].
- K_L: JPEG feature calibration detector [117].
- K_V: total variation approach for JPEG detection [127].
- $K_U^1$and K_U^2: JPEG blocking artifacts based detector [46].
- K_P^{S162}: 162-D SPAM feature detector [38].
- K_{Li}^{S100}: 100-D correlation detector using intra and inter block [122], [124].
- K_{AR}^{S10}: autoregressive detector [128].
- K_{SPAM}^{S686}: 686-D SPAM detector [38].
- K_{SRM}^{S714}: residual detector [130].

Performance validation for different proposed schemes are as follow:

- $\mathcal{F}D_{S_qS_b}$: Anti-forensic scheme using deblocking & dithering [115].
- $\mathcal{F}D_V$: shows the dithering approach for anti-forensic [45].
- $\mathcal{F}D_{S_u}$: SAZ attack technique for anti-forensic [125].
- $\mathcal{F}D_F$: anti-forensic scheme based on TV approach [46].
- $\mathcal{F}D_{S_q}$: anti-forensic scheme based on DCT histogram smoothing [48].
- $\mathcal{F}D_{Fan}$: four-step adaptive dithering-based anti-forensic scheme [47].

2.2 Metrics for Evaluation

The image anti-forensics aims to achieve high visual quality image and undetectability for better forensic detection as mentioned in Chapter 1. The forensic undetectability can be evaluated from the Receiver Operating Characteristics (ROC) curve [47]. 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 undetectability. However, visual quality of the image is also a significant concern to be considered during the

evaluation of a particular scheme of anti-forensics. This leads to the fact that a low-quality image may raise doubt on the authenticity of image processing techniques. The image quality is evaluated using Structural Similarity (SSIM) and Peak Signal-to-Noise Ratio (PSNR).

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 output of classification for a group of the images is compared with the actual values in order to estimate the efficacy of proposed technique. 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 positive value categorized as true 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 [131]:

$$FPR = \frac{N_{FP}}{N_N}, \quad TPR = \frac{N_{TP}}{N_P} \tag{2.17}$$

The various classification strategies of a forensic detector provide (FPR, TPR) pairs based on which ROC curve is drawn. Afterward, the accuracy of the classifier can be measured from the Area Under Curve (AUC) [132]. Lesser the distance between the curve and the diagonal indicates more forensic undetectability. Whereas, the curves near the upper left corner shows more forensic undetectability as shown in Figure 2.4. It is noteworthy to mention that high value of the undetectability indicates better mislead by the detectors. Both the original and tampered 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. The database of identical image forgeries is generated with the help of different anti-forensic schemes. Finally, forensic testing is performed by considering an equal number of original and processed images.

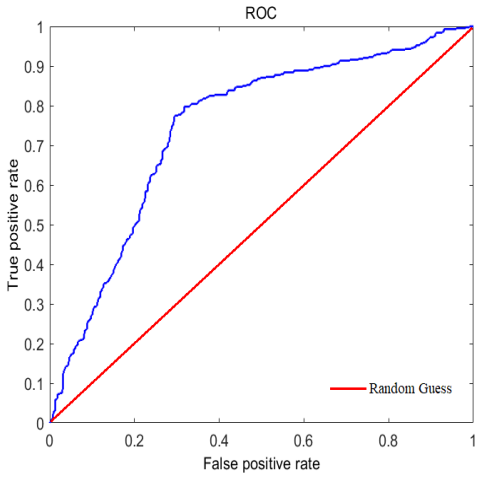


Figure 2.4: ROC Curve.

On the contrary, the characterization of a particular forensic technique are divided into two class namely scalar and vector, based on which 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

A forensic detector based on scalar characterization produces only one feature value of a particular image. Based on the comparison between the feature and a pre-defined threshold, the image under investigation may be identified 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) [46].

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 [47]. For a heavily compressed image, the DCT coefficients in the high-frequency range have been quantized to zero. Consequently, the quantization stages are difficult to determine [47]. Therefore, in case of scalar-based detector K^{q}_{Weiqi}, the quantization steps values are computed

and values greater than one are used as features. All scalar-based forensic detectors gives final output as K_F, K_{Weiqi}, K_{Weiqi}^{q}, K_V, K_L, K_U^1, K_U^2 considered in this thesis to measure the capability of the projected anti-forensics and counter anti-forensics. Based on the magnitude of threshold, image under consideration may termed as compressed or uncompressed.

2.2.1.2 SVM-based Forensic Detectors

Various forensic detectors gives their output as a vector. 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 [47]. SVM classifier is utilized to estimate the efficacy of the JPEG forensics and anti-forensics schemes. It is assumed that detective knows about various forensic and anti-forensic approaches. Therefore, the examiner can generate a dataset of images to train the detector, which is worst situation for the anti-forensic strategy. Here, available SVM detectors, K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} may effectively by-pass the JPEG anti-forensic scheme. Authors in [3], [47] reported that hardly any anti-forensic scheme may mislead the detectors using machine learning approach, is worst situation for anti-forensics scheme but good for image forensics. The SVM detectors is trained for every kind anti-forensic image of JPEG format using the specified feature vector are used to train SVM- based detectors using each classes of the anti-forensic of JPEG images. The SVM detectors K_{Li}^{S100},K_{AR}^{S10},K_{SPAM}^{S686} and K_{SRM}^{S714} are often employed in steganalysis, having excellent accuracy of detection along with least decision error lesser than 0.1. Afterward, situation (optimistic scenario) with lesser challenging estimation of JPEG anti-forensics is considered. In this scenario, each of the feature vectors of both compressed and original images are used in training.

Modification rate (denoted by bits per pixel (bpp)) with very high value, is observed in steganalysis due the modification in the coefficient of DCT. Substitution process [47] is employed to create JPEG forgeries while evaluating the performance analysis of the proposed scheme. The middle part of the uncompressed image is exchanged with anti-forensically processed JPEG image. Here, the rate of swapping varies in between 0.05 and 1. The uncompressed images and images after processing are used in forensic testing. LIBSVM [133] with Gaussian kernel is used during the SVM training. Further, SVM parameters are obtained with the help of cross validation with five-fold [38] along with grid based on multiplicative

property. Also, the uncompressed versions and SVM classifiers are trained using anti-forensic JPEG pictures. Figure 2.5 shows the creation of composite JPEG forgery. Firstly, some portion is taken from the processed image of quality q_2 and is pasted to an original image of quality q_1. Afterward, this compressed image in JPEG format again with q_3 as the value of a quality factor result in composite JPEG forgery.

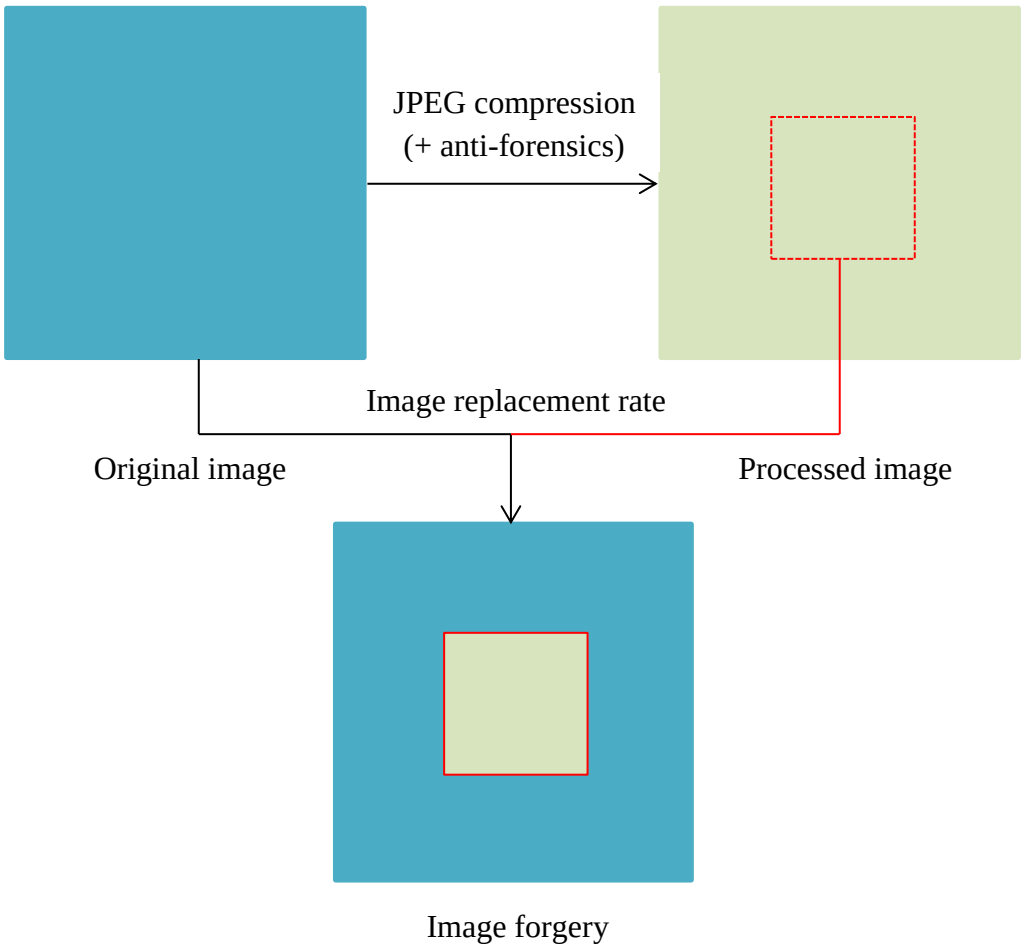


Figure 2.5: Illustration of generating a composite JPEG image.

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 with the estimation of minimum decision error. It is worth noting that designing a SVM-based counter anti-forensic scheme for JPEG format is also the main focus of the research work along with the enhancement of JPEG anti-forensics.

2.2.2 Image Quality

Assessment methods for the quality of image are categorized into two classes *i.e.*, no-reference and full-reference techniques based on the fact that whether the original image is accessible [134]. The true image is commonly unknown for real-world setups. 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 $M \times N$ and its anti-forensically processed version is denoted by 'y'. The PSNR value in decibel (dB) can be calculated as [134]:

$$PSNR = 10\ log_{10}\left(\frac{{Max_Y}^2}{MSE}\right) \tag{2.18}$$

where, Max_Y: Maximum pixel value and further, MSE can be given as:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[x(i,j) - y(i,j)]^2 \tag{2.19}$$

The PSNR is a traditional evaluation metric of image quality which is further improved by Wang *et al.* [135] by suggesting the SSIM metric with enhanced correlation with subjective scores of image quality. The SSIM metric is depends on Human Visual System (HVS) as compared to the PSNR and SSIM can be denoted as:

$$SSIM(x,y) \quad = \frac{(2\mu_x\mu_y + Q_1)(2\sigma_{xy} + Q_2)}{(\mu_x^2 + \mu_y^2 + Q_1)(\sigma_x^2 + \sigma_y^2 + Q_2)} \tag{2.20}$$

Where, μ_x and μ_y are the mean values of intensities, σ_x and σ_y are the contrast amplitude, whereas Q_1 and Q_2 are the constants correspond to x and y images. More is the value of SSIM measure, higher is the image quality of processed image 'y'.

2.3 Image Datasets for 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 schemes along with counter anti-forensic approaches have been presented in Chapter 3 to Chapter 6 on the basis of numerous test on Uncompressed Color Image Database (UCID) [136]. UCID dataset of size 512×384 of a total 1338 uncompressed images in TIFF format which contains various real-world scenes. Initially, quality factors with value equal to $\{50, 51, 52, \ldots..95\}$ are used in compression of image database to obtain compressed JPEG image. Further, numerous anti-forensic methods are used to create JPEG dataset with forgeries. A total 669 random images are taken from UCID dataset to create training dataset (UCIDTrain) and rest of the images are employed to test the dataset (UCIDTest).

Furthermore, another relatively large image database is also considered to present the efficacy of the counter anti-forensics in the JPEG format called as BOSSBase dataset [137]. A total 10,000 images with high resolution but in raw format is available in BOSS Base dataset. First of all, these raw images are converted into PPM format with the help of *UFRaw* utility, and then it is converted into 8-bit PGM grayscale images [138]. The center of each grayscale BOSSBase image is cropped by size of 512×512, and then used for testing. Also testing and training of BOSSBase dataset images are obtained using UCID strategy. A total 5000 images are used as test image whereas, remaining is used as training images to train the SVM-based detectors. Further, as represented in Chapter 5, a real case with spliced images is used to analyze the efficacy of the presented scheme. Furthermore, efficacy of the proposed scheme is evaluated with by conducting many tests on CASIA v1.0 [139] and Columbia database [140]. The evaluation dataset for image manipulation detection using CASIA is abbreviated as (CITDE) provides a variety of image, around 921 tampered and 800 authentic images are used in tampering detection [139]. Whereas, Columbia dataset includes a total 363 total images in BIMP and TIFF formats in which 183 are authentic and rest of the images are tampered [140].

2.4 Research Gaps

Above extensive literature survey resulting in following unique research gaps:

- In the previous JPEG anti-forensic work, most of the techniques are focused on removing JPEG blocking artifacts in the spatial domain. So, there is a scope to introduce an anti-forensics by removing the compression artifacts in spatial as well as in DCT domain.
- In the previous JPEG anti-forensic work, most of the schemes employ histogram smoothing by using the dithering operation. This operation introduces unnatural noise in the processed image which results in the reduction of image quality. So, there is a scope to develop a technique by avoiding the addition of un-natural noise.
- Most of the techniques include the detection procedure to detect the presence of non-aligned double JPEG compression (NA-JPEG) and aligned double JPEG compression (A-JPEG) in compressed images. So there is a scope to develop an anti-forensic technique which is capable of hiding the non - aligned and aligned JPEG compression artifacts.
- The existing anti-forensic techniques used traditional transforms such as DCT. So there is scope to design JPEG anti-forensic in DFrCT domain because it provides extra fractional parameter. This additional fractional parameter in DFrCT provides extra degree of freedom to design a system. On the other hand, DCT doesn't have any such parameter. This fractional parameter is capable of providing solutions to problems that are not solved by the DCT.
- Most of the existing anti-forensic techniques do not provide good trade-off between image visual quality and forensic un-detectability. So, there is a scope to attain a better trade-off between image visual quality and forensic undetectability.
- The existing forensic techniques for the detection of JPEG compression are easily circumvented by adopting counter-forensic attacks. So, there is a scope to improve the detection technique.
- Most of the forensic techniques for the detection of JPEG compressed 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 example by considering MTPM for better detection.

- Moreover, the existing counter JPEG anti-forensic schemes have not considered all of the existing JPEG anti-forensic techniques due to the issue of different strengths of anti-forensic techniques. So, there is a scope to resolve this issue by generating an effective feature which is capable of detecting the existing JPEG anti-forensic attacks.
- Most of the existing JPEG forensic techniques are based on the DCT domain analysis. So, there is scope to conduct the JPEG forensic analysis by considering DFrCT.

2.5 Summary

This chapter provides the detailed survey of JPEG forensics and anti-forensics work carried out by the researchers. The information related to existing JPEG forensics and anti-forensics techniques is provided in a very effective way by focusing on their contributions and limitations. After analyzing the existing works the objectives for the presented work are identified on the basis of gaps obtained in existing work. We further provide the information related to the metrics that are widely used for the evaluation of JPEG forensics and anti-forensics techniques. Lastly, image datasets for testing and research gaps are also briefly discussed.

CHAPTER 3

JPEG COMPRESSION ANTI-FORENSICS

This chapter presents an anti-forensic framework by taking into account JPEG artifacts in both DCT and spatial domain to disguise existing forensic detectors. The available anti-forensic methods generally lower the quality of processed image. The presented approaches provide high image quality in addition to improved forensic undetectability. The efficacy of suggested method is validated on the basis of its undetectability along with high image visual quality against several forensic detection attacks [96], [53], [141 – 144] in spatial as well as DCT domain. The capability of recommended schemes is further confirmed through detectors based on machine learning [122], [145]. Moreover, the DJPG compression detectors suggested in [7], [146], [109] are used for analyzing the robustness of the proposed anti-forensic approaches based on JPEG compression. The simulation results prove 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.

3.1 Anti-Forensic approach for JPEG compression

This section aims to provide an improved JPEG anti-forensic approach for achieving improved results. The perceptual histogram smoothing with dithering is generally used by the majority of existing anti-forensic schemes which intends to add an unnatural or grainy noise while processing the image thus reducing the quality of an image. Besides, this operation needs excess time for creating JPEG forgery since it possesses the computational complexity of order $O(D^3)$. Hence, the proposed approach intends to evade the necessity of perceptual histogram smoothing for reducing the effect of unnatural grainy noise and computation time. The suggested method employed shifted block DCT method in addition to the TV-based deblocking operation which is used for disguising several JPEG forensic detectors as depicted in Figure 3.1.

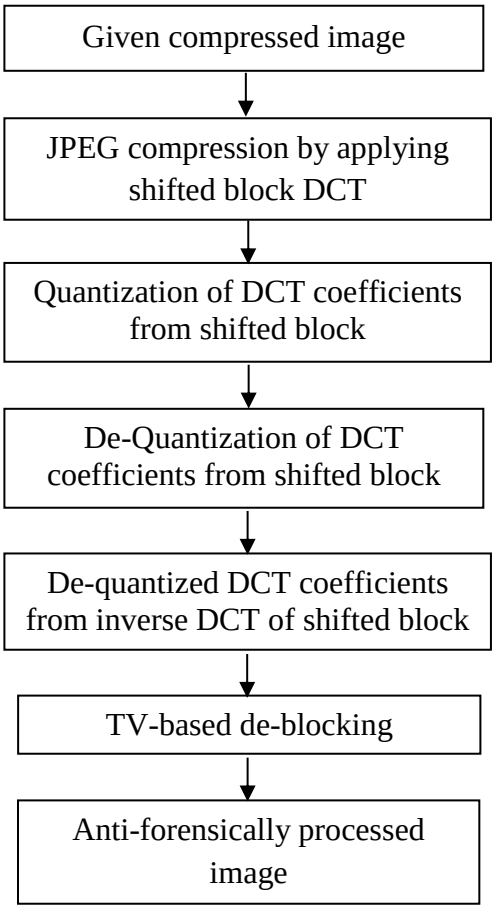


Figure 3.1: Proposed JPEG anti-forensic technique.

3.1.1 JPEG compression by applying shifted block DCT

In this section, the shifted DCT block method is employed as illustrated in Figure 3.2, in addition to the application of a TV-based deblocking for disguising JPEG forensic detectors. In this approach, DCT of the 8×8 block is computed by shifting the columns while leaving the fixed rows as depicted in Figure 3.2. Here, (N_1, N_2) refers to row and column respectively. As depicted in Figure 3.2, initially, 1^{st} row is left and columns are shifted one after the other. The shaded region shows rows and columns that are left while the unshaded area shows the 8×8 block where DCT is applied. Thus, a total of 8 combinations are obtained from (1, 1) to (1, 8). Subsequently, next 8 combinations are obtained from (2, 1) to (2, 8). Hence, a total of 64

combinations are obtained. Thus, concept of the proposed anti-forensic approach is clarified from Figure 3.2 by taking into consideration all the possible 64 combinations of (N1, N2). Its performance is confirmed from the metrics provided in Table 3.2 of section 3.2. However, the DCT employed in proposed approach is defined as [147]:

$$G_{row,col}(u,v) = \left(\frac{2}{M}\right)^{\frac{1}{2}}\left(\frac{2}{N}\right)^{\frac{1}{2}}\sum_{\mathrm{i}=0}^{M-1}\sum_{j=0}^{N-1}\Lambda(i)\Lambda(j)cos\left[\frac{\pi u}{2\,M}(2i+1)\right]cos\left[\frac{\pi v}{2\,N}(2j + 1)\right]Y(i,j) \quad (3.1)$$

$$\Lambda(\xi) = \begin{cases}\frac{1}{\sqrt{2}} for\ \xi = 0\\ 1\ otherwise\end{cases}$$

where M and N refers to the size of input image. $Y(i,j)$ refers to the pixel intensity at i^{th} row and j^{th} column. $G_{row,col}(u,v)$ gives row u and column v DCT coefficients. The DCT plays a vital role in the JPEG compression. The distribution of DCT coefficients generally provides imperative evidence related to the history of compression. However, when employing the shifted block DCT method, by splitting DCT coefficients into AC and DC coefficients, the shifted quantization error is calculated. The DC coefficients possess wide dynamic range as well as small quantization step along with a uniform distribution of quantization error whereas Laplacian distribution is followed by the quantization error for AC coefficients. It is worth noting that forensic detectors are not able to detect compression case of shifted block DCT approach because majority of detectors can only detect the DCT based JPEG compression artifacts. The image that was anti-forensically processed was chosen based on optimum PSNR and SSIM that are used to determine the visual quality of image as well as other forensic parameters from the 64 combinations in order to attain greater forensic undetectability and image quality trade-off. The resultant coefficients are quantized to a numerous step size of quantization after applying the shifted block DCT as determined based on quantization matrix of JPEG. The reconstructed DCT coefficients have a different distribution from the original one at the time of image decoding. Afterwards, shifted block DCT coefficients are dequantized as mentioned previously.

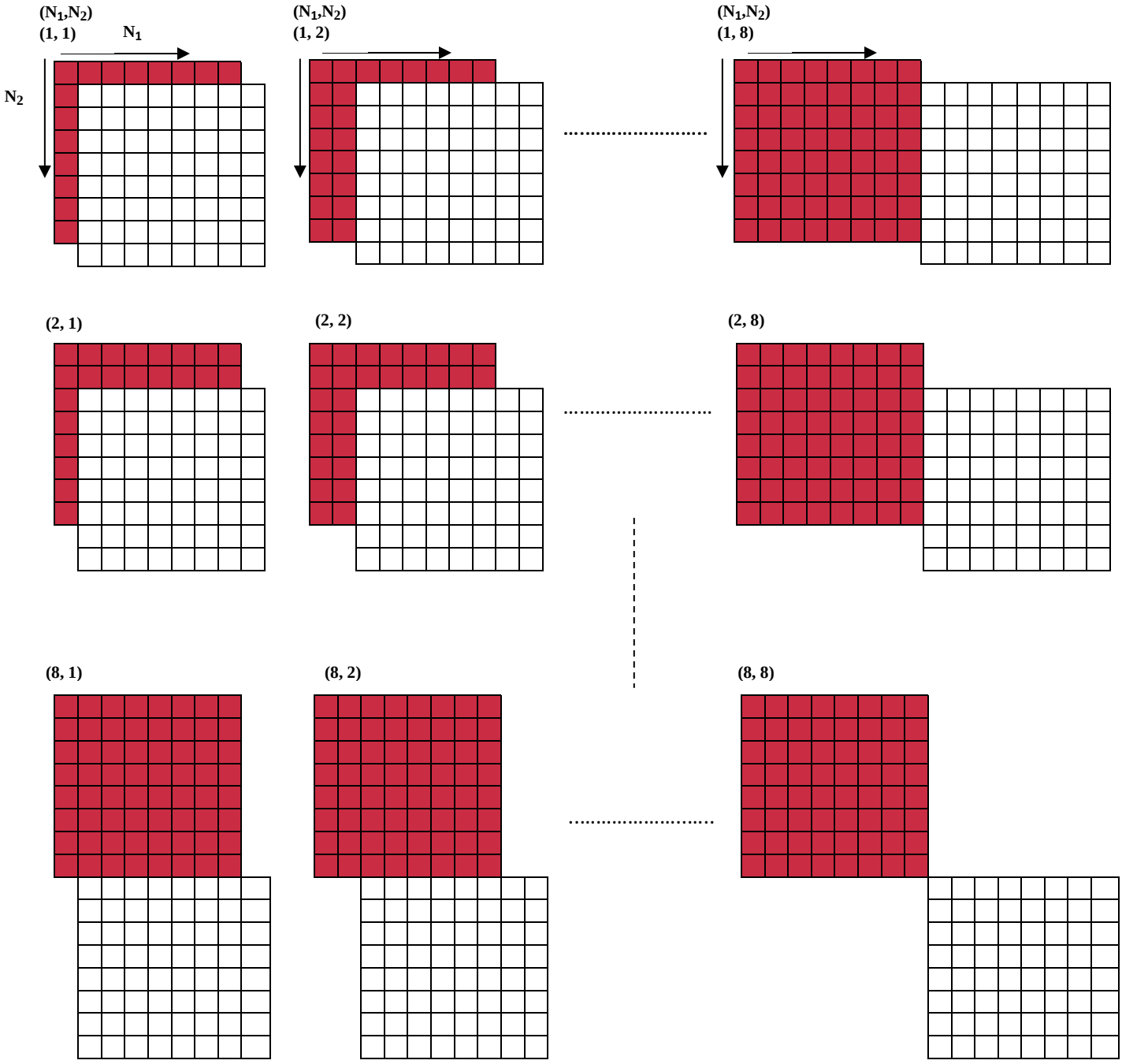


Figure 3.2: Illustration of Shifted block DCT approach.

The image is recovered using the inverse DCT (IDCT) of shifted dequantized DCT coefficients after quantization and dequantization. After applying IDCT, after JPEG compression, the remaining blocking artifacts in the spatial domain are removed by TV-based deblocking by considering the mutual effect of total energy fluctuation in both the vertical and horizontal directions.

3.1.2 Deblocking operation based on total variation

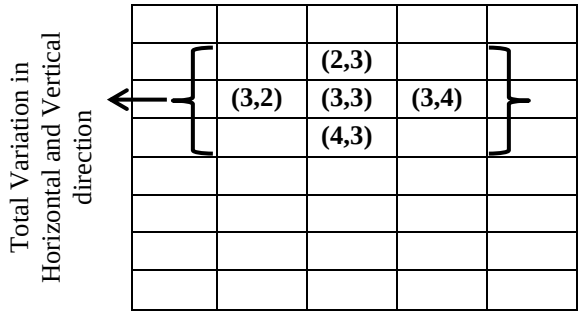
The efficient strategies are utilized for examining and eliminating the JPEG blocking artifacts. However, such strategies solely focus on the enhancement of image visual quality. But, any anti-forensic approach needs to maintain the suitable tradeoff between the forensic undetectability and visual quality of image. The purpose of TV-based deblocking is to keep energy to a minimum on the basis of TV. The term energy includes total variation based TV and blocking estimation. Based on the image Y of size $M \times N$, the expression of TV can be stated below [47] where, TV-term takes into consideration both vertical and horizontal directions for evaluating total variation term.

$$TV(Y) = \sum_{1 \le i \le M, 1 \le j \le N} t_{i,j} \tag{3.2}$$

where, $t_{i,j}$ refers to the total variation in vertical and horizontal directions.

$$t_{i,j} = \left(\left(Y_{i-1,j} + Y_{i+1,j} - 2Y_{i,j} \right)^2 + \left(Y_{i,j-1} + Y_{i,j+1} - 2Y_{i,j} \right)^2 \right)^{1/2} \tag{3.3}$$

where, the pixel value is provided by $Y_{i,j}$ at the $(i,j)^{\text{th}}$ location.



The statistical footprints of JPEG blocking artifacts are eradicated by TV-based deblocking. It is based on the premise that the sum of total energy across within the block should be close to the block's borders. Therefore, the pixels in the block are classified into two sets based on the pixel position in block as illustrated in Figure 3.3, where, Set A refers to the shaded pixel locations while others are categorized as set B. The energy difference is defined as:

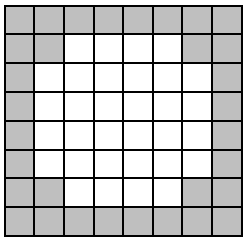


Figure 3.3: Categorization of pixels into two groups: A (shaded) and B (unshaded).

$$E(X) = \left| \sum_{Y_{i,j} \in A} t_{i,j} - \sum_{Y_{i,j} \in B} t_{i,j} \right| \tag{3.4}$$

The constraint image space (S) can be described as follows to provide a processed image of higher quality that is forensically undetectable:

$$S = \left\{ Y \in M^{M \times N} | (D_{matrix} Y)^{l}_{r,c} \in \left[\left(h^{l}_{r,c} - \beta \right) q_{r,c}, \left(h^{l}_{r,c} + \beta \right) q_{r,c} \right] \right\} \tag{3.5}$$

where, M refers to the set of integers ranging between $[0, 255]$. Here, β possess a small positive value that regulates quantized DCT coefficients for an uncompressed image given by $h^{l}_{r,c} = (q_{block}(D_{matrix}\boldsymbol{I}))^{l}_{r,c}$ and the constraint image space (S). The problem of TV-based minimization is defined as:

$$Y^{*} = \arg\min_{X \in \mathbb{C}} T(Y) = \arg\min_{X \in \mathbb{C}} \left(TV(Y) + \varphi E(Y) \right) \tag{3.6}$$

By choosing positive values for the regularisation parameter α, the two energy terms are balanced. $T(Y)$ is a convex function that is not differentiable, but $\mathbb{C}$ is a convex set [148 – 149]. For solving the energy minimization problem, the projected subgradient approach is as follows:

$$Y^{(h+1)} = O_S \left(Y^{(h)} - t_{step} \times G\left(Y^{(h)} \right) \right) \tag{3.7}$$

Thus, at the h^{th} iteration, the processed picture is denoted by $Y^{(h)}$, and the considered JPEG image is represented by $Y^{(0)}$, O_S refers to the projection operator [143], subgradient of $T(Y)$ is given by $G(Y)$, where, t_{step} represents a positive step size. The t_{step} and regularization parameter φ can be altered for realizing an improved balance among the histogram quality of restored DCT coefficients and image visual quality. The optimal φ is 1.5 at h^{th} iteration, where, $t_{step} = 1/h$ [148]. The parameter β is set to 0.5 in order to keep the processed DCT coefficients in the same quantization bin as their original value. As a result, it can be determined that by carefully regulating these factors, good results can be achieved. When the processed DCT coefficients do not lie in the first quantization bin, then projection operator O_S will be used to

map such coefficients to the first quantization bin. The adequacy of presented JPEG anti-forensic approach is validated by utilizing K_F and K_U^p forensic detectors as attacks.

The blocking signature measure K_F is used to choose the deblocked candidate image. The efficiency of the proposed anti-forensic approach is verified by utilizing forensic detectors K_F and K_U^p. For uncompressed images, K_F has high detection strength and low standard deviation in comparison to another blocking signature K_U^p. Thus, K_F parameter is utilized for selecting the deblocked image. After performing the simulations for 50 iterations, the image with the lowest K_F value is chosen to be deblocked.

3.2 Experimental Results

The ability of the presented approach is established in this section by performing numerous tests using a standard UCID dataset [129]. The UCID dataset comprises of 1338 uncompressed TIFF images having disparity in terms of scene contents. By compressing the UCID dataset images with a quality factor ranging between 50 and 95, a dataset comprising of single and double compressed images can be created. After JPEG compression of original uncompressed image, image $\mathcal{T}$ is obtained. The various JPEG anti-forensic schemes are as follows:

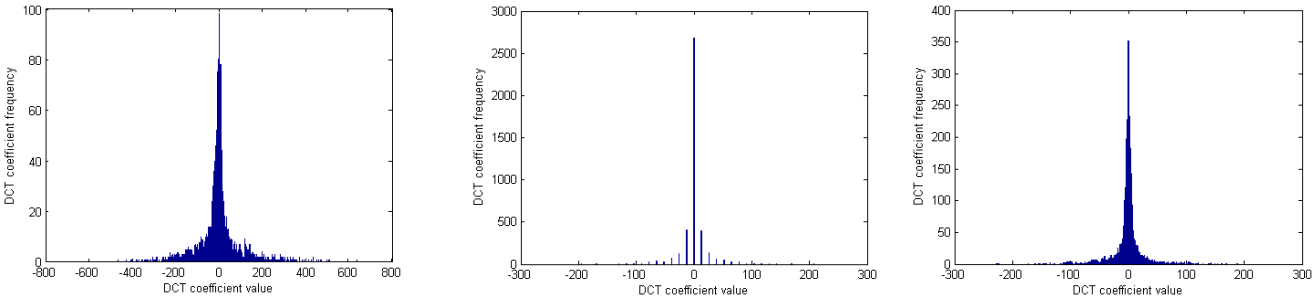
- $\mathcal{F}D_{S_qS_b}$, refers to the dithering and deblocking operation-based anti-forensic approach [115].
- $\mathcal{F}D_V$, corresponds to perceptual anti-forensic dithering approach [150].
- $\mathcal{F}D_{S_u}$, represents an anti-forensic technique with SAZ attack [125].
- $\mathcal{F}D_F$, refers to anti-forensic scheme based on TV [143].
- $\mathcal{F}D_{S_q}$, denotes anti-forensic technique based on DCT histogram smoothing [151].
- $\mathcal{F}D_{Fan}$, four-step adaptive dithering-based anti-forensic scheme [47].
- $\mathcal{F}D_{Gur}$, corresponds to scheme based on denoising and dithering [152].
- $\mathcal{F}D$, corresponds to the proposed shifted block DCT based anti-forensic approach.

The robustness of presented JPEG anti-forensic approach is validated by considering the forensic detectors as:

- K_F, denotes the JPEG compression blocking artifacts based detector [96].
- K_F^q, refers to detector based on the estimation of quantization table [96].

- K^{q}_{Weiqi}, corresponds to the detector based on the estimation of quantization step [53].
- K_{Weiqi}, refers to the detector that identifies JPEG [53].
- K_L, denotes calibration feature-based JPEG detector [141].
- K_V, denotes total variation-based JPEG forensic detector [142].
- K^1_U and K^2_U, denotes JPEG blocking artifacts-based detectors [143].
- K_P^{S162}, refers to 162-D SPAM feature-based detector [145].
- K_{Li}^{S100}, 100-D correlation detector using intra and inter-block [122], [144].

For the presented anti-forensic approach, Figure 3.4 shows the DCT coefficients histogram for the (4, 4) subband of an uncompressed original Lena image, the histogram of a JPEG compressed Lena image with a quality factor of 50, and the histogram of the (4, 4) subband of a JPEG compressed Lena image with a quality factor of 50. Figure 3.4 (b) shows the periodic gaps that remain during JPEG compression. The proposed anti-forensic approach appropriately filled such gaps without introducing any grainy noise and the resultant histogram is depicted in Figure 3.4 (c).



(a) (b) (c)

Figure 3.4: (a) The DCT coefficients histogram of an uncompressed image for the (4, 4) subband, (b) Histogram of a JPEG compressed image with 50 quality-factor, (c) After the anti-forensic method, the histogram of the subband (4, 4).

3.2.1 Comparison with existing state-of-the-art anti-forensic methods

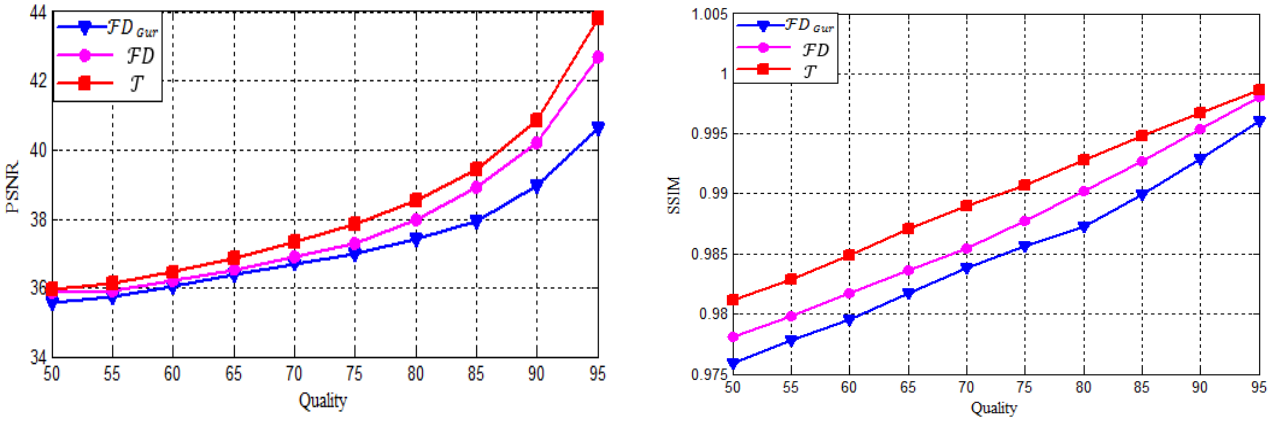
This section performs the comparison of proposed anti-forensic approach with state-of-the-art existing approaches. Moreover, the adequacy of the proposed approach $\mathcal{FD}$ is apparent from Figure 3.5. A test is conducted on the classical Lena image with the original image as reference for quantifying the proposed approach in terms of SSIM and PSNR.

It is perceived that the Lena image which is compressed with the quality factor 50 has PSNR (dB) and SSIM of 35.8085 and 0.9809 respectively. The JPEG forgery $\mathcal{FD}_{Gur}$ [152] produced by the JPEG compressed Lena image has PSNR (dB) and SSIM value of 35.5590 and 0.9755 respectively. However, the presented JPEG forgery $\mathcal{FD}$ obtains the PSNR (dB) and SSIM of 35.851 and 0.978 respectively. Thus, the proposed approach $\mathcal{FD}$ performs better than the existing $\mathcal{FD}_{Gur}$ approach in terms of PSNR and SSIM.

(a) (b) (c)

Figure 3.5: (a) Lena image $\mathcal{I}$ with a quality factor of 50, having PSNR value 35.9279 dB and SSIM value 0.9812, (b) JPEG forgery $\mathcal{FD}_{Gur}$ with PSNR of 35.5590 dB and SSIM value 0.9755, (c) PSNR value 35.851 dB and SSIM value 0.978 for proposed JPEG forgery $\mathcal{FD}$.

Figure 3.6 shows PSNR and SSIM of the final image attained after applying the suggested and existing anti-forensic approaches, $\mathcal{FD}$ and $\mathcal{FD}_{Gur}$, respectively. The existing schemes indicate that disguising the traces of JPEG compression without significant loss of quality is quite challenging. After the analysis of curves in Figure 3.6, it is evident that improved PSNR and SSIM are obtained by the proposed anti-forensic approach $\mathcal{FD}$ than the existing approach $\mathcal{FD}_{Gur}$. The anti-forensic schemes are primarily intended to achieve PSNR and SSIM comparable to that of the uncompressed image as reference. Table 3.1 provides the average values of PSNR and SSIM obtained by the anti-forensic approaches based on distinct images where original uncompressed image is considered as a reference.



(a) (b)

Figure 3.6: Parameters for the Lena image obtained after applying $\mathcal{T}$, $\mathcal{FD}_{Gur}$ and proposed technique $\mathcal{FD}$ with uncompressed image as reference (a) PSNR (b) SSIM.

The average PSNR of 35.718 dB and SSIM of 0.9762 is attained by the proposed JPEG anti-forensic approach $\mathcal{FD}$ upon conducting a test on a vast scale on the images of UCID database. It shows that the proposed approach $\mathcal{FD}$ has the capability of providing better forensic undetectability besides higher image quality than the existing schemes.

Table-3.1: Average PSNR and SSIM values attained by testing distinct images considering different anti-forensic methods, where reference is original uncompressed image.

	$\mathcal{T}$	$\mathcal{FD}_{S_q}$	$\mathcal{FD}_{S_qS_b}$	$\mathcal{FD}_V$	$\mathcal{FD}_{S_u}$	$\mathcal{FD}_F$	$\mathcal{FD}_{Fan}$	$\mathcal{FD}_{Gur}$	$\mathcal{FD}$
PSNR	36.948	33.2395	31.0479	32.3840	31.3792	34.8364	35.3725	35.4871	**35.718**
SSIM	0.9914	0.9693	0.9435	0.9659	0.9631	0.9687	0.9747	0.9753	**0.9762**

3.2.2 Evaluation of anti-forensic approach against JPEG forensic detectors

This subsection deals with the validation of presented anti-forensic approach by considering JPEG forensic detectors as attacks. It is carried out by performing evaluation on Lena image compressed with quality factor of 50 in terms of PSNR, SSIM, and currently available forensic detectors namely K_L, K_F, K_U^1, K_U^2 as given in Table 3.2. It is worth noting that high PSNR and SSIM signifies better image visual quality while low value of K_L, K_F, K_U^1, K_U^2 indicates better forensic undetectability.

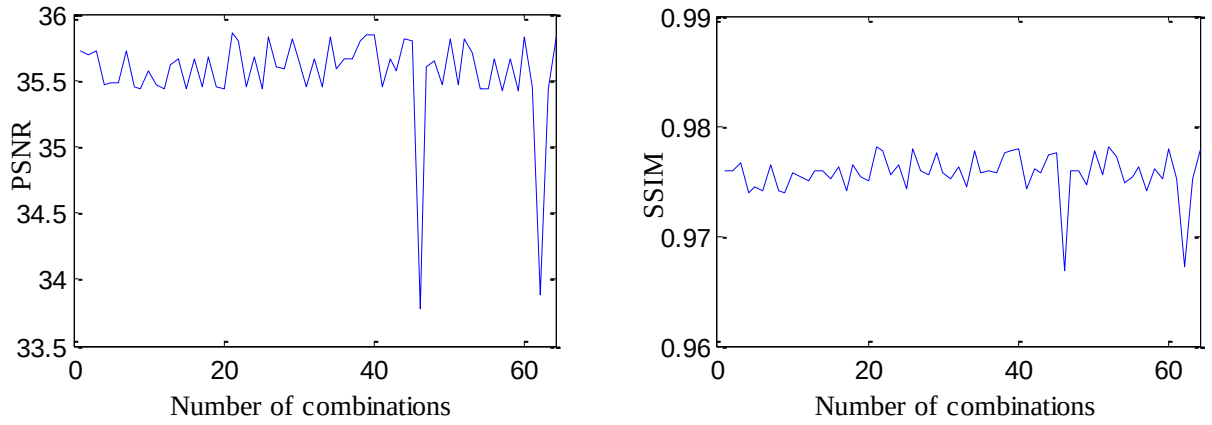
Table-3.2: Parameters produced by the suggested anti-forensic technique for Lena image considering 50 as a quality factor for compression.

(N1,N2)	**PSNR**	**SSIM**	K_L	K_F	K_U^1	K_U^2
(1,1)	35.7285	0.9759	0.5908	0.1260	0.3278	17.2473
(1,2)	35.6913	0.9760	0.5545	0.1179	0.2919	16.4193
(1,3)	35.7221	0.9766	0.6015	0.1099	0.3215	15.0820
(1,4)	35.4610	0.9740	0.3567	0.0912	0.5679	14.4693
(1,5)	35.4867	0.9745	0.4158	0.1038	0.5019	12.1049
(1,6)	35.4799	0.9741	0.3671	0.1053	0.5697	14.1228
(1,7)	35.7181	0.9764	0.5909	0.1290	0.2863	19.0847
(1,8)	35.4565	0.9741	0.3804	0.0897	0.5004	9.6602
(2,1)	35.4388	0.9740	0.3652	0.0937	0.6002	13.9576
(2,2)	**35.5687**	**0.9757**	**0.3893**	**0.1698**	**0.3146**	**0.3591**
(2,3)	35.4594	0.9753	0.2522	0.1063	0.9064	25.9432
(2,4)	35.4365	0.9750	0.2787	0.1421	0.9458	26.3222
(2,5)	35.6087	0.9760	0.3450	0.1255	0.4033	10.7719
(2,6)	35.6588	0.9759	0.4904	0.1361	0.9494	32.1248
(2,7)	35.4301	0.9751	0.2677	0.0942	0.8426	23.8395
(2,8)	35.6668	0.9763	0.4757	0.1386	0.7697	21.7954
(3,1)	35.4434	0.9741	0.3069	0.0695	0.6563	13.2753
(3,2)	35.6737	0.9765	0.4818	0.1512	0.9376	32.4836
(3,3)	35.4492	0.9754	0.2743	0.1134	0.8485	26.5057
(3,4)	35.4416	0.9750	0.2550	0.1446	0.9524	27.2688
(3,5)	**35.8497**	0.9781	0.7039	0.1623	1.1272	42.6612
(3,6)	35.8023	0.9777	0.5417	0.1607	0.6407	24.2462
(3,7)	35.4512	0.9755	0.2598	0.1023	0.8619	25.6318
(3,8)	35.6725	0.9764	0.4684	0.1527	0.9460	29.2699
(4,1)	35.4341	0.9742	0.2949	0.0690	0.6891	18.2528
(4,2)	35.8316	0.9779	0.7330	0.1466	1.0121	41.6953
(4,3)	35.5991	0.9760	0.3185	0.1159	0.4325	8.9160

(4,4)	35.5867	0.9756	0.3308	0.1250	0.4053	9.1721
(4,5)	35.8076	0.9776	0.5605	0.1295	0.6613	28.9096
(4,6)	35.6538	0.9757	0.4870	0.1582	0.7990	28.0975
(4,7)	35.4572	0.9751	0.2778	0.1209	0.8060	20.7588
(4,8)	35.6551	0.9762	0.4903	0.1446	0.8485	27.5423
(5,1)	35.4573	0.9744	0.3633	0.1179	0.5481	12.7696
(5,2)	35.8213	0.9778	0.5036	0.1416	0.5729	23.0270
(5,3)	35.5898	0.9758	0.3962	0.1199	0.4729	12.2162
(5,4)	35.6650	0.9759	0.4877	0.1713	0.8568	29.0685
(5,5)	35.6603	0.9758	0.5297	0.1456	0.7571	23.0916
(5,6)	35.7998	0.9776	0.5771	0.1381	0.6542	28.1457
(5,7)	35.8449	0.9778	0.7362	0.1537	1.1952	40.7348
(5,8)	35.8370	**0.9780**	0.6372	0.1471	0.6820	31.7221
(6,1)	35.4493	0.9742	0.3234	**0.0564**	0.6227	13.0510
(6,2)	35.6585	0.9761	0.4863	0.1426	0.8990	29.6699
(6,3)	35.5672	0.9757	0.3577	0.1058	0.5343	11.3236
(6,4)	35.8103	0.9773	0.4954	0.1517	0.6035	24.3592
(6,5)	35.7976	0.9775	0.5749	0.1537	0.6304	26.3504
(6,6)	33.7761	0.9668	**0.2231**	0.1471	2.0391	114.1392
(6,7)	35.5941	0.9760	0.3357	0.1164	0.4518	7.7993
(6,8)	35.6462	0.9760	0.4346	0.1572	0.7712	24.1843
(7,1)	35.4659	0.9746	0.3099	0.0731	0.6474	16.2775
(7,2)	35.8097	0.9777	0.4590	0.1371	0.6621	23.8220
(7,3)	35.4603	0.9755	0.2609	0.1008	0.9062	28.5234
(7,4)	35.8162	0.9781	0.5543	0.1476	0.6624	27.3220
(7,5)	35.7070	0.9771	0.3949	0.1325	**0.0130**	9.8317
(7,6)	35.4338	0.9749	0.2501	0.1194	0.9439	27.9922
(7,7)	35.4391	0.9754	0.2602	0.0857	0.8994	27.0475
(7,8)	35.6617	0.9763	0.4428	0.1356	0.8836	29.5935
(8,1)	35.4224	0.9741	0.3684	0.0877	0.6237	12.5253

(8,2)	35.6544	0.9761	0.4733	0.1668	0.9167	31.7726
(8,3)	35.4245	0.9752	0.2640	0.1038	0.8987	26.3440
(8,4)	35.8325	0.9779	0.6317	0.1643	0.7323	28.7929
(8,5)	35.4561	0.9752	0.2887	0.1325	1.0186	28.0677
(8,6)	33.8785	0.9671	0.2629	0.1537	1.2771	86.9388
(8,7)	35.4415	0.9751	0.2655	0.1295	0.8121	20.2781
(8,8)	35.8216	0.9780	0.6545	0.1723	1.0839	37.8763

Here, the proposed JPEG anti-forensic approach provides PSNR and SSIM of 35.8497 and 0.9780, respectively which demonstrate its ability to achieve high visual quality. Moreover, the value of detector K_U^2 declines rapidly from 114.1392 to 0.3591 at (2, 2) as shown in Table 3.2. Likewise, extremely low values exist for forensic detectors namely K_L, K_F, and K_U^1 . It exhibits the proficiency of proposed approach for achieving high image visual quality along with better forensic undetectability. Based on the optimum value shown in Table 3.2, the corresponding anti-forensically processed image is chosen. The optimum values obtained in this manner aid to decrease the time required to generate forgery by lowering computing costs and establishing a better balance of forensic undetectability and quality of image. These findings reveal that the suggested approach successfully misguides current forensic detectors.



(a) (b)

Figure 3.7: Variation in value of (a) PSNR (b) SSIM.

After analyzing Figure 3.7 and Figure 3.8, it can be revealed that the suggested method renders better results as high PSNR and SSIM in addition to extremely low forensic detectors values K_L,

K_F, K_U^1 and K_U^2. It is worth noticing that with the reduction in forensic detector parameter, forensic undetectability improves. On the basis of these optimal parameters, an anti-forensically processed image is chosen. This demonstrates that the presented anti-forensic approach successfully misguides the existing forensic detectors.

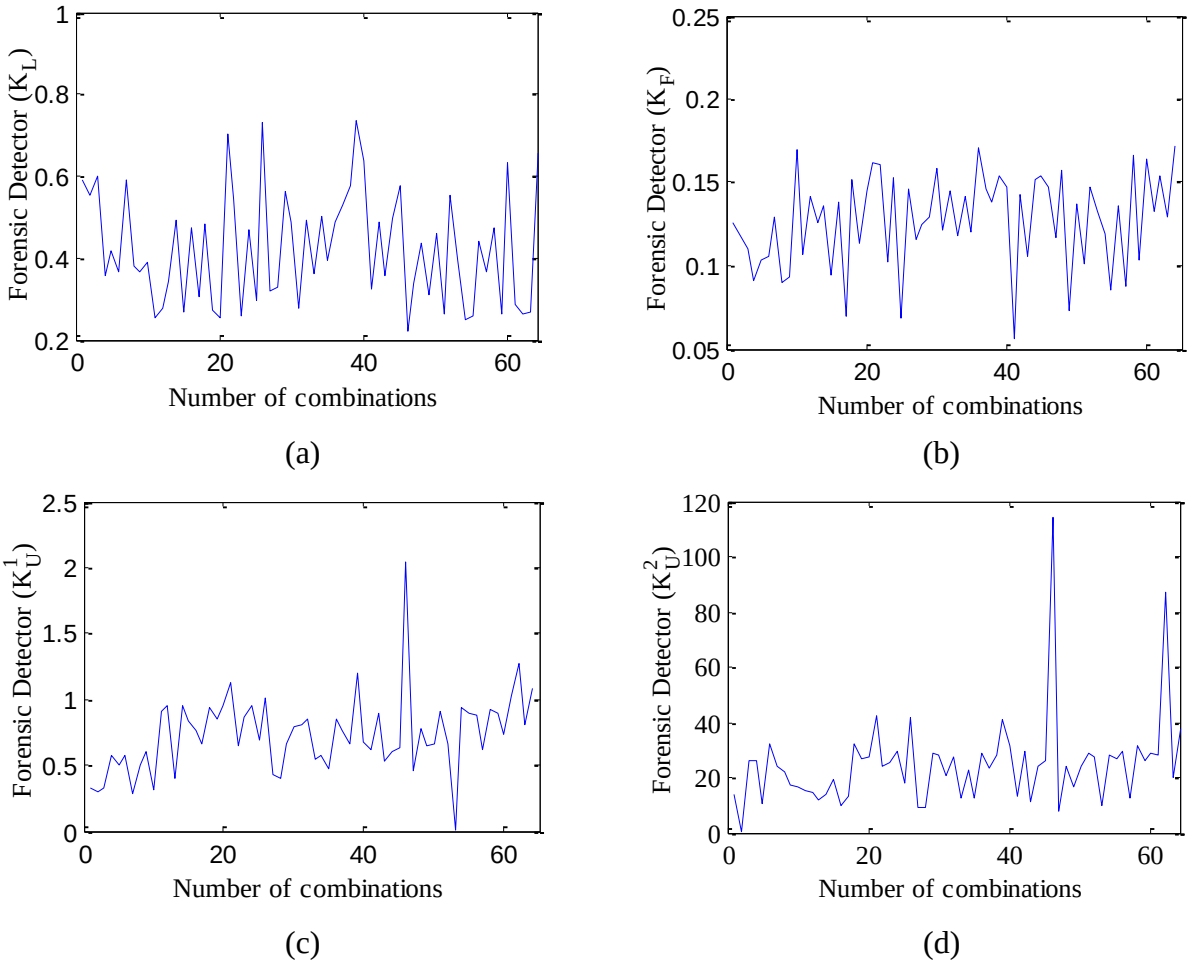


Figure 3.8: Behaviour of various forensic detectors (a) K_L, (b) K_F, (c) K_U^1 and (d) K_U^2, for proposed approach $\mathcal{F}D$.

The presented approach $\mathcal{F}D$ is evaluated on distinct images that are compressed by a quality factor of 50 in terms of PSNR, SSIM and prevailing forensic detectors namely K_L, K_F, K_U^1, K_U^2, K_F^q .

Table-3.3: Parameter values attained by testing distinct compressed images having the quality factor 50 with $\mathcal{T}$, $\mathcal{FD}_{Gur}$ and proposed approach $\mathcal{FD}$, when an uncompressed image is considered as reference.

Images	**PSNR**	**SSIM**	K_L	K_F	K_U^1	K_U^2	K_F^q
Lena $\mathcal{T}$	35.927	0.981	59.423	1.364	8.6492	326.849	38.000
Lena $\mathcal{FD}_{Gur}$	35.559	0.975	0.0512	0.075	0.2045	4.1759	0.0000
Lena $\mathcal{FD}$	**35.851**	**0.978**	**0.2231**	**0.056**	**0.0130**	**0.3591**	**0.0000**
Peppers $\mathcal{T}$	34.722	0.978	43.496	1.507	7.9472	286.386	41.000
Peppers $\mathcal{FD}_{Gur}$	34.492	0.971	0.0672	0.183	0.8139	17.7931	1.0000
Peppers $\mathcal{FD}$	**34.827**	**0.973**	**0.0363**	**0.081**	**0.0784**	**0.5913**	**0.0000**
Barbara $\mathcal{T}$	32.496	0.981	92.730	0.836	12.693	628.749	48.000
Barbara $\mathcal{FD}_{Gur}$	31.954	0.971	0.0649	0.237	0.7482	123.947	0.0000
Barbara $\mathcal{FD}$	**32.769**	**0.975**	**0.0364**	**0.139**	**0.0683**	**1.1752**	**0.0000**
Baboon $\mathcal{T}$	28.749	0.980	45.546	0.535	16.641	1812.85	60.000
Baboon $\mathcal{FD}_{Gur}$	27.385	0.971	0.0583	0.250	0.8742	212.529	0.0000
Baboon $\mathcal{FD}$	**28.959**	**0.976**	**0.0310**	**0.192**	**0.3729**	**3.8497**	**0.0000**

Table-3.4: Average parameter values when evaluated on different UCID images by using suggested anti-forensic method with different quality factors.

Quality	**PSNR**	**SSIM**	K_L	K_F	K_U^1	K_U^2	K_F^q
50	35.851	0.978	0.223	0.056	0.013	0.3591	0.0000
55	35.934	0.978	0.193	0.048	0.012	0.2852	0.0000
60	36.048	0.979	0.117	0.042	0.011	0.2385	0.0000
65	36.175	0.979	0.094	0.039	0.011	0.2076	0.0000
70	36.386	0.980	0.089	0.033	0.009	0.1748	0.0000
75	36.399	0.981	0.081	0.027	0.008	0.1291	0.0000
80	36.425	0.982	0.073	0.020	0.008	0.1218	0.0000
85	36.586	0.982	0.063	0.016	0.007	0.0963	0.0000
90	36.715	0.983	0.058	0.015	0.007	0.0910	0.0000
95	36.889	0.984	0.045	0.014	0.006	5.8981	0.0000

It is evident that the proposed approach $\mathcal{FD}$ performs effectively in comparison to the $\mathcal{FD}_{Gur}$ method; it gives good SSIM and PSNR values while yielding exceptionally low forensic detector parameters values. Table 3.4 shows the different parameters values obtained after applying the suggested method $\mathcal{FD}$.

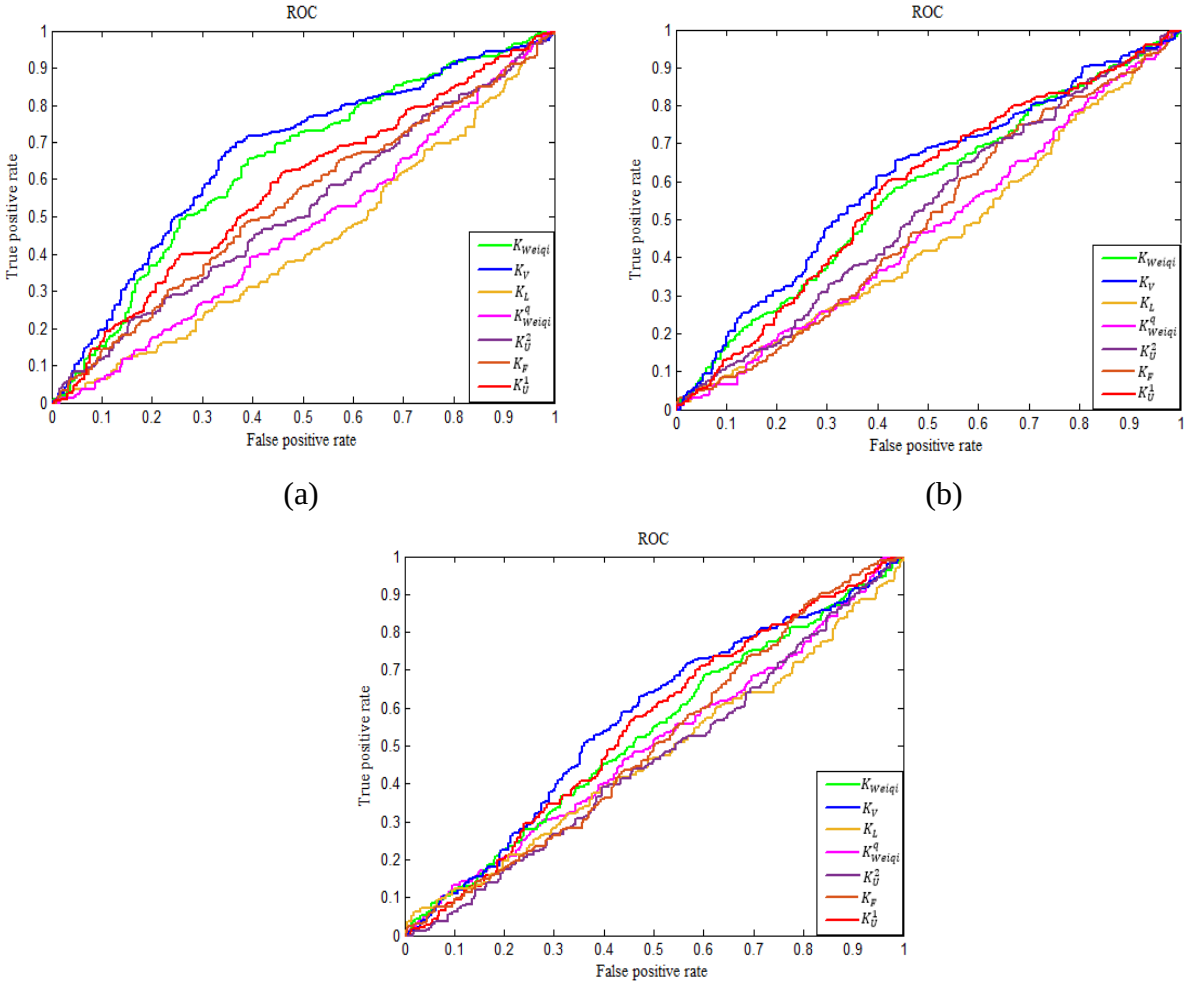


Figure 3.9: ROC curves of (a) $\mathcal{FD}_{Fan}$, (b) $\mathcal{FD}_{Gur}$ and (c) $\mathcal{FD}$ against various forensic detectors. The detectors are deceived better when the ROC curves reaches the diagonal (random guess).

Besides, Receiver Operating Characteristics (ROC) curves are also scrutinized to validate the adequacy of proposed approach as compared to previous anti-forensic JPEG techniques for several forensic detectors [47], [152]. It is observed that curve is closer to the diagonal (random

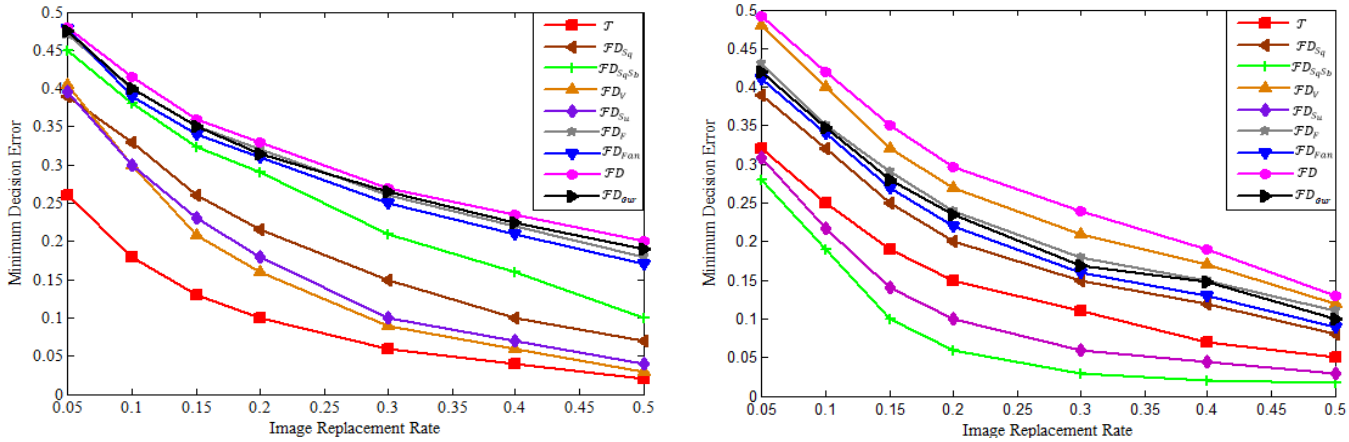
guess) as illustrated in Figure 3.9 (c). Thus, it can be deduced that the proposed approach efficiently mislead forensic detectors when compared to existing anti-forensic approaches. The JPEG forgery made by the anti-forensic method $\mathcal{FD}_{S_q}$ is detectable by forensic detectors, as shown in Table 3.5. Although the perceptual dithering based anti-forensic approach $\mathcal{FD}_V$ attains high SSIM value but its forensic undetectability is equivalent to that of $\mathcal{FD}_{S_q}$ approach. Conversely, JPEG forgery approach $\mathcal{FD}_{S_qS_b}$ utilized median filtering to improve forensic undetectability when compared to several detectors but lead to loss of 6.9 dB for PSNR. However, the presented approach can effectively fool detectors, thus resulting in high minimum decision error than existing anti-forensic methods which is evident from Table 3.5.

Table-3.5: Using an uncompressed image as a reference, all of the JPEG anti-forensic methods were tested against various forensic detectors, yielding the average minimum decision error.

	K_F	K_{Weiqi}	K^q_{Weiqi}	K_V	K_L	K^1_U	K^2_U
$\mathcal{T}$	0.0074	0	0.0047	0.0141	0.0317	0.0383	0.1583
$\mathcal{FD}_{S_q}$	0.1379	0.4093	0.2235	0.0163	0.0582	0.0672	0.1219
$\mathcal{FD}_{S_qS_b}$	0.3284	**0.4364**	0.3173	0.2094	0.4671	0.4065	0.4694
$\mathcal{FD}_V$	0.0512	0.4103	0.2098	0.0428	0.0218	0.0390	0.1538
$\mathcal{FD}_{S_u}$	0.1485	0.0816	0.0947	**0.4820**	0.0583	0.3539	**0.4912**
$\mathcal{FD}_F$	0.3568	0.3438	0.4716	0.3425	0.4793	0.3814	0.4516
$\mathcal{FD}_{Fan}$	0.3813	0.3804	0.4782	0.3928	0.4836	**0.4092**	0.4728
$\mathcal{FD}_{Gur}$	0.4714	0.4281	0.4744	0.4258	0.4984	0.0751	0.4831
$\mathcal{FD}$	**0.4914**	0.4316	**0.4951**	0.4403	**0.4987**	0.0637	0.4892

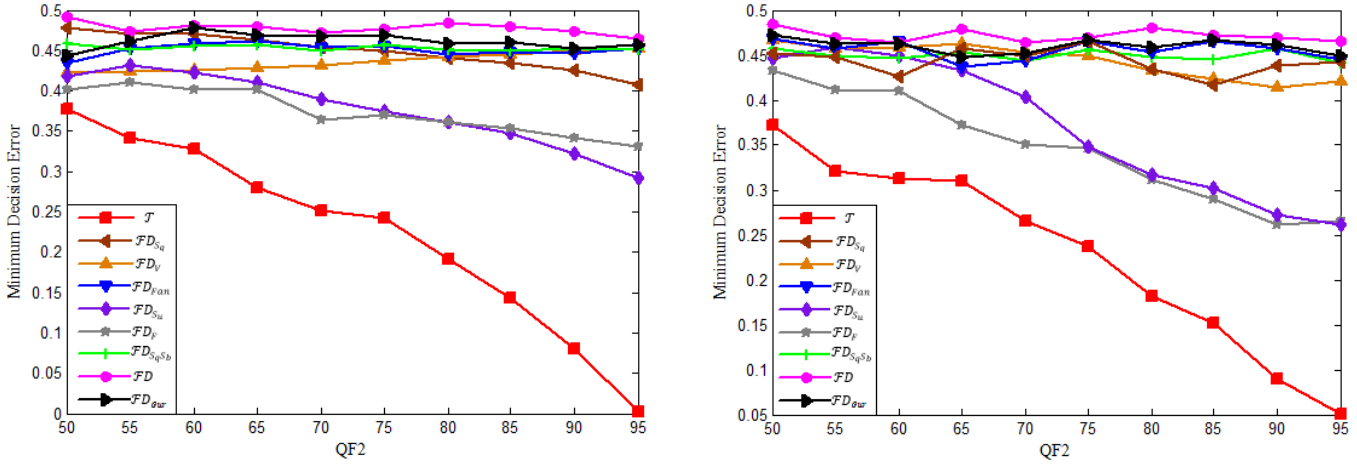
Moreover, the proposed JPEG anti-forensic approach $\mathcal{FD}$ can also mislead the advanced forensic detector K_V because the minimization in proposed TV-term can suppress the unnatural noises. Even the calibration-based detector K_L is defeated by proposed approach due to inclusion of decalibration operation. Further, the images are identified as not JPEG compressed in 98.58% of the cases when JPEG forgeries generated with proposed approach are taken into account.

The adequacy of presented anti-forensic approach is further confirmed by utilizing the experimental setup of the steganography work [153] for creating JPEG forgeries. With a replacement rate ranging from 0.05 to 0.5, the center area of an uncompressed image is replaced by a JPEG anti-forensic image. In Figure 3.10 minimum decision error is measured against SVM-based forensic detectors as a function of image replacement rate. The testing of proposed approach against the forensic detectors K_{Li}^{S100} and K_{P}^{S162} provides high minimum decision error than the existing approach as shown in Figure 3.10.

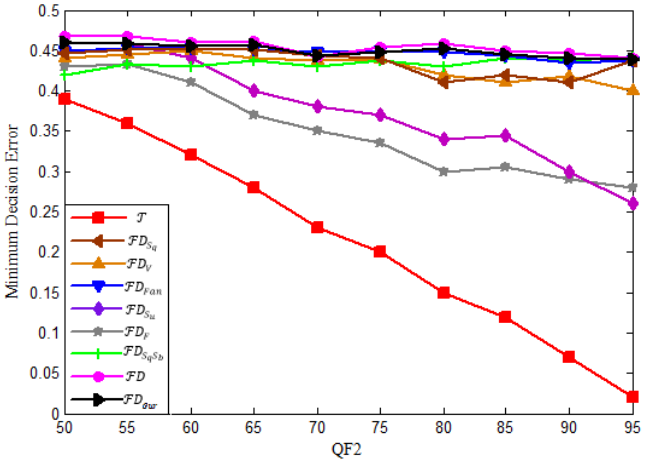


(a) (b)

Figure 3.10: Minimum decision error measured against SVM-based forensic detectors as a function of image replacement rate (a) K_{Li}^{S100}, (b) K_{P}^{S162}.



(a) (b)



(c)

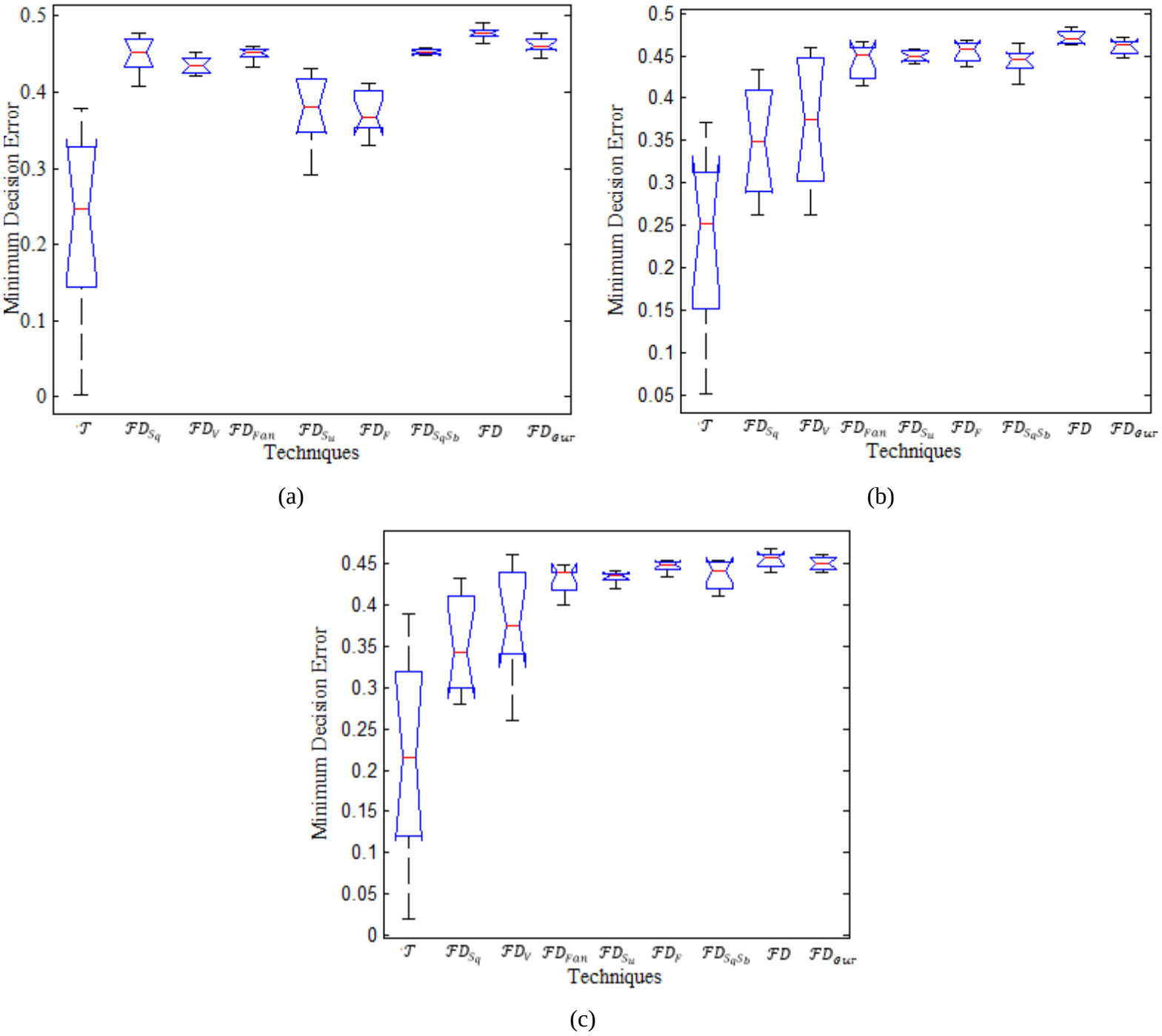
Figure 3.11: Minimum decision error evaluation against different forensic detectors proposed in [7], [109], [146], for double compressed JPEG images.

Figure 3.11 demonstrates that the proposed technique outperforms previous approaches in terms of minimal decision error which reaches 0.5, when evaluated with forensic detectors and all quality factors are taken into consideration.

3.3 Statistical Analysis of considered Anti-Forensic Techniques

This section deals with the investigation of nature of balance among forensic undetectability and visual quality of image. Analysis of Variance (ANOVA) method is used for comparing the minimum decision error with respect to varying the quality factors for several schemes in order to see if there is a statistically substantial discrepancy between two or more distinct approaches means. The examination with various techniques is shown in Figure 3.12 in terms of minimum decision error for varying quality factors upon testing against numerous forensic detectors [7], [109], [146]. It can be seen from Figure 3.12(a) that the whiskers (which depicts maximum and minimum values) of approach $\mathcal{FD}$ are high when compared with the existing approaches which accounts to approximately 0.5, besides, at 95% confidence level, the median values are also high as compared to existing ones. Moreover, it can be observed from Figure 3.12 (a) that the proposed approach is stronger than the existing approaches $\mathcal{FD}_{S_u}$ and $\mathcal{FD}_F$. In a similar manner, data given in the box plot of Figure 3.12 (b) and (c) is analyzed. It is found that at 95% confidence level, whiskers are high for both of them that validates the superiority of proposed

approach $\mathcal{FD}$. Consequently, the analysis of data given in box plots demonstrates that the proposed approach $\mathcal{FD}$ is better than the existing ones.



(a) (b)

(c)

Figure 3.12: Statistical examination of the minimum decision error for various approaches of anti-forensic when compared to numerous forensic detectors offered in [7], [109], [146].

3.4 Computation Time

Table 3.6 illustrates the time to execute images at various resolutions and produce multiple JPEG forgeries. It is determined by the amount of pixels in a given image.

Table-3.6: Time taken to make different types of JPEG forgeries using images of various resolutions (in seconds).

Techniques / Images	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}$
Cameraman[1] (256×256)	4.502	58.978	255.3478	**2.315**
Boat[1] (512×512)	18.245	232.247	1020.254	**8.821**
Building[2] (768×512)	24.325	350.012	1575.232	**14.056**
Male[3] (1024×1024)	74.384	1003.32	5418.307	**35.166**

[1] https://homepages.cae.wisc.edu/~ece533/images/

[2] http://r0k.us/graphics/kodak/

[3] http://sipi.usc.edu/database/database.php

The proposed technique $\mathcal{FD}$ execution time per pixel is between 0.000033 and 0.000036 sec/pixel. It needs around 9 seconds to generate JPEG forgery of image size 512×512. The adaptive dithering operation or perceptual DCT histogram smoothing is, in fact, the bottleneck of computational cost. However, in the proposed approach, there is no requirement of dithering process. As shown in Table 3.6, the proposed anti-forensic approach performs efficiently than existing schemes by having a shorter execution time.

3.5 Summary

In this chapter, shifted block DCT based JPEG anti-forensic approach is proposed that is able to disguise the JPEG compression artifacts. By concealing artifacts of compression in the DCT domain, this method has the potential to deceive forensic detectors. This approach has an inherent characteristic that dithering noise is added itself and it does not require any adaptive dithering model, that is, addition of histogram smoothing is evaded while decreasing the time to create forgery, thus reducing its computational cost. Additionally, TV-based deblocking approach assists in reducing the blocking artifacts. The robustness of proposed approach is

confirmed on the UCID dataset against the existing forensic detectors. However, there is still need to achieve superior balance with visual image quality, computational cost, and forensic undetectability. Hence, further work is focused on utilization of other transform domains in spite of DCT domain to achieve a more balance among aforesaid results. However, after analyzing the robustness and security of the proposed anti-forensic approaches, it is noticed that a unique anti-forensic approach can defeat almost all the forensics schemes. Therefore, it is required to design a more robust forensic approach against anti-forensic attacks.

CHAPTER 4

DFrCT BASED ANTI-FORENSIC APPROACH FOR JPEG COMPRESSION

The presented technique in this chapter is based on the analysis performed in the last chapter by considering JPEG artifacts in both spatial as well in DCT domain to disguise the existing forensic detectors. This chapter presents an anti-forensic method considering the shifted block DFrCT approach. The compression blocking artifacts are then removed using a Total variation (TV)-based deblocking method. The suggested technique without addition of dithering signal achieves histogram smoothing, implying that it is proficient of applying dithering on its own, due to the shifted block technique. In addition, TV-based deblocking is utilised to remove blocking artifacts that are left over from JPEG compression. The DFrCT method adds a fractional parameter to the proposed method to improve accuracy. This additional fractional parameter $'\alpha'$ in DFrCT gives more flexibility when designing a system, in contrast to DCT. This fractional parameter can be used to solve problems that the DCT is unable to address. The proposed system is assessed using UCID dataset images using forensic detectors that are based on scalars and machine learning. In terms of forensic undetectability, the proposed strategy outperforms previous methods in terms of PSNR and SSIM values.

4.1 Proposed DFrCT based anti-forensic approach

Dithering-based perceptual histogram smoothing was utilized in previous JPEG anti-forensic techniques, which degrades image quality by introducing unnatural or grainy noise. Furthermore, due to the high computational cost of order $O(D^3)$, it takes longer to create JPEG forgery [47] . Furthermore, existing JPEG anti-forensic techniques fail to strike a reasonable balance forensic undetectability and image visual quality. As a result, a method of JPEG anti-forensic is required, which achieves an improved balance between forensic undetectability and visual quality of image. This section discusses an anti-forensic approach on the basis of shifted block DFrCT method and a TV-based deblocking operation based on TV to fulfil the aforementioned requirements, as demonstrated in Figure 4.1. The suggested anti-forensic JPEG technique smooths histograms without introducing dithering signal, implying that presented methodology

able of doing dithering on its own. As a result, it reduces forgeries generation time by lowering computation costs while improving forensic undetectability and image quality. When shifted block DFrCT is combined with TV-based deblocking, image quality and forensic undetectability becomes better.

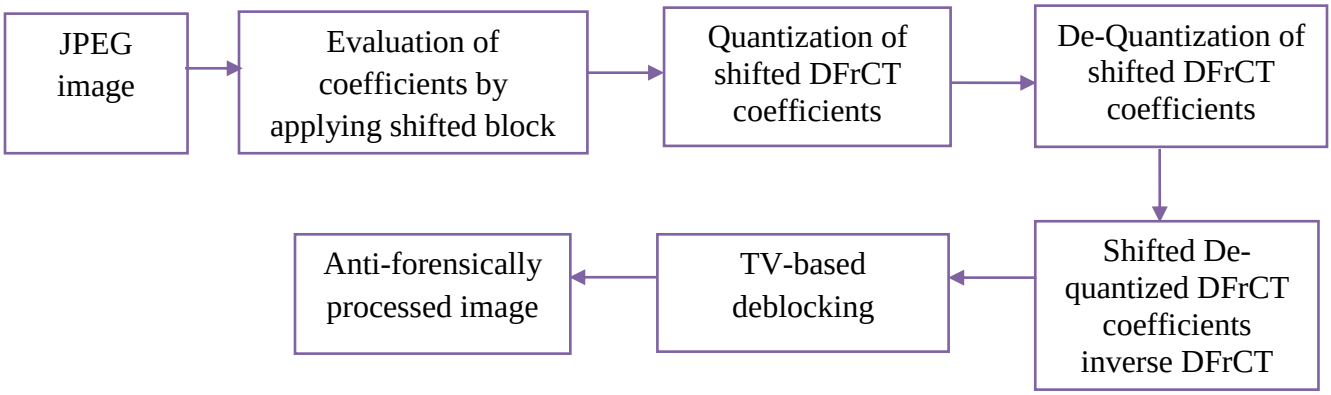


Figure 4.1: A flowchart of a suggested JPEG anti-forensic method.

The following are the various phases involved in the suggested JPEG anti-forensic technique:

- The coefficients of the considered image are first evaluated using the shifted block DFrCT method.
- Shifted DFrCT coefficients are quantized and de-quantized.
- De-quantized DFrCT coefficients undergo shifted inverse DFrCT.
- Furthermore, anti-forensically processed images are created via TV-based deblocking.

The following subsections provide a detailed explanation of these steps of the provided anti-forensic approach.

4.1.1 Apply shifted block DFrCT approach

As shown in Figure 4.2, the shifted block DFrCT is implemented by shifting the columns while leaving the fixed rows. The shaded section of Figure 4.2 depicts the block on which DFrCT is applied, while the unshaded area reflects the number of columns and rows remain after the procedure is completed. Here n_1 represents the row number, while n_2 represents the column number, as illustrated in Figure 4.2, which are left during the shifting operation. Figure 4.2 (a) shows the first row and first column (1,1), while Figure 4.2 (b) shows the first row and first two

columns (1,2). By leaving rows and columns (i.e. altering $n_1$and n_2), we can have a total of 64 possible combinations in the same way as shown in Figure 4.2.

The two-dimensional signal $x(p,q)$ has its DFrCT computed by [75]:

$$C_{(\alpha,\gamma)}(m,n) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} x(p,q)\, C_{(\alpha,\gamma)}(p,q,m,n) \tag{4.1}$$

where, $C_{(\alpha,\gamma)}(p,q,m,n)$is the kernel matrix for two-dimensional $M \times N$ point DFrCT with rotation angles α, γ and $C_{(\alpha,\gamma)}(m,n)$ is the transformed two dimensional signal in DFrCT domain. By multiplying the image with the DFrCT kernel, the shifted DFrCT coefficients may be computed (see Figure 4.2). While leaving the specific row and column, the image which is taken as input is processed using shifted DFrCT, as shown in the preceding equation.

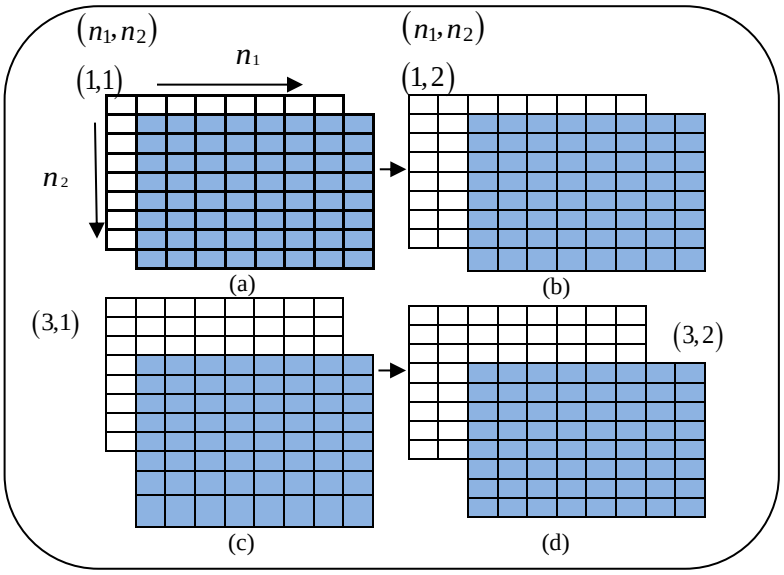


Figure 4.2: DFrCT method with shifted blocks.

The quantization of the shifted DFrCT coefficients refers to the second phase. The JPEG quantization matrix specifies the size of the quantization step is multiplied by each DFrCT coefficient in an image. The decoded image recovered DFrCT coefficients have a different distribution from the original distribution. We must convert the processed image from frequency domain to spatial domain in order to visualise it. As a result, using the Inverse DFrCT (IDFrCT) described as [75], the dequantized DFrCT coefficients are used to obtain the processed image:

$$x(p,q) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} C_{(\alpha,\gamma)}(m,n)\, C_{(-\alpha,-\gamma)}(p,q,m,n) \tag{4.2}$$

where, $x(p,q)$ denotes the recovered signal and $C_{(-\alpha,-\gamma)}(p,q,m,n)$ is the IDFrCT kernel matrix having rotation angles of $-\alpha$ and $-\gamma$, respectively.

4.1.2 Employing TV-based deblocking operation

In this section, TV-based deblocking is utilised as one of the step of the recommended JPEG anti-forensic framework to remove blocking artifacts. The researchers examine and remove JPEG blocking artifacts using effective ways. However, these methods are only concerned with enhancing the processed image quality. As a result, to reduce TV-based energy, the suggested JPEG anti-forensics methodology employs a deblocking operation based on TV. Image anti-forensics works in a similar way as image restoration. When it comes to image restoration, the main goal is to improve quality of image. Image anti-forensics, contrarily, aim for higher forensic undetectability while maintaining the quality of image. The JPEG compression method produces blocking artifacts into the processed image, lowering the image visual quality. After JPEG compression, blocking artifacts are removed using deblocking based on TV, which accounts for both the horizontal and vertical effects of total energy fluctuation. The vertical and horizontal directions specified by [47] are taken into account when evaluating this TV term.

$$TV(X) = \sum_{1\le i\le T, 1\le j\le T} t_{i,j} \tag{4.3}$$

where, $t_{i,j}$ denotes total variation in both vertical and horizontal directions.

$$t_{i,j} = \left(\left(X_{i-1,j} + X_{i+1,j} - 2X_{i,j}\right)^2 + \left(X_{i,j-1} + X_{i,j+1} - 2X_{i,j}\right)^2\right)^{\frac{1}{2}} \tag{4.4}$$

The pixel value at the $(i,j)^{th}$place is represented by $X_{i,j}$. Inside the block, the total energy of pixel value fluctuation at block boundaries should be equivalent to pixel value variation, according to this concept. As a result, every pixel position in the block divides the image pixels into two sets. The pixels that are shaded placed in set P, the others are assigned to set Q, as illustrated in Figure 4.3. This concept is the basis for the second term, which may be written as:

$$E(X) = \left|\sum_{X_{i,j}\in A} t_{i,j} - \sum_{X_{i,j}\in B} t_{i,j}\right| \tag{4.5}$$

$$S = \left\{X \in M^{T\times T'} \middle| (D_{matrix}X)^l_{r,c} \in \left[\left(h^l_{r,c} - \beta\right)q_{r,c}, \left(h^l_{r,c} - \beta\right)q_{r,c}\right]\right\} \tag{4.6}$$

where, M is a collection of integers ranging from [0, 255]. The image constraint space (S) can be adjusted using β in this case. $h_{r,c}^{l} = \left(q_{block}(D_{matrix}I)\right)_{r,c}^{l}$ represents the quantized DFrCT coefficients for the original (uncompressed) picture. The problem of TV-based minimization can be described as:

$$X^{*} = \underset{X \in \mathbb{C}}{\arg\min}\, T(X) = \underset{X \in \mathbb{C}}{\arg\min}(TV(X) + KE(X)) \tag{4.7}$$

The energy terms are balanced by setting the regularization parameter $'K'$ to positive values. The non-differentiable convex function is denoted by $T(X)$, while the convex set is denoted by $\mathbb{C}$ [148 – 149]. The projected subgradient approach is used to address the energy reduction issue as follows:

$$X^{(h+1)} = O_S\left(X^{(h)} - t_{step} \times G\left(X^{(h)}\right)\right) \tag{4.8}$$

$X^{(h)}$ denotes the processed image at the h^{th} iteration, $X^{(0)}$ denotes the supplied JPEG image, $G(X)$ denotes the subgradient of $T(X)$, The projection operator [143] is denoted by O_S, and t_{step} represents the positive step size.

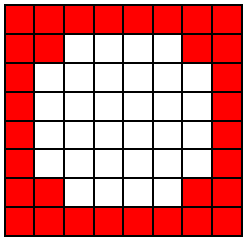


Figure 4.3: Pixels are divided into two sets: P (shaded) and Q (unshaded).

Variations in the $'K'$ regularization parameter and the t_{step} step size aids in achieving a better balance between the image visual quality and the recovered DFrCT coefficients' histogram quality. At the h^{th} iteration, 1.5 is the optimum $'K'$ value, and $t_{step} = 1/h$. As recommended in [47], 0.5 is set as the value of β so that the processed coefficients can only be quantized in the same bin as their initial value. By fine-tuning these parameters, you can get good results. The projection operator O_s is used to assign coefficients to the first quantization bin. To evaluate the capability of proposed JPEG anti-forensic method, forensic detectors such as K_F and K_U^P are used as attacks. Instead of waiting for the optimization problem to converge before selecting the

candidate deblocked image, a different strategy is used. The blocking signature measure K_F is used to choose the candidate deblocked image. For uncompressed images, K_F has a lower standard deviation than blocking signature K_U^P. The least K_F value achieved after executing 50 iterations in the experiment is used to select the resultant deblocked image.

***Algorithm for the proposed anti-forensic technique**:*

Input: I

$\mathcal{T}$: Given compressed image.

***Parameters*:**

$\mathcal{T}_{DFrCT}$: JPEG image DFrCT coefficients

$\mathcal{T}_{dq}$: Dequantized coefficients

$\mathcal{T}_{q}$: Quantized coefficients

$\mathcal{T}_{DFrCT}$: IDFrCT coefficients

T : IDFrCT based intensity image

O_S : Projection operator

Output:

Y : Image that has been anti-forensically processed

Begin

$[\tau_{row}\tau_{col}] = size(\tau);$

for $n_1 = 1:8$ *do*

for $n_2 = 1:8$ *do*

for $i = n_1 : 8 : \tau_{row}$ *do*

for $j = n_2 : 8 : \tau_{col}$ *do*

$tblock = \tau(i:i+7, j:j+7);$

$\tau_{DFrCT} = DFrCT(tblock);$

$\tau_q = quantization\ (\tau_{DFrCT});$

$\tau_{dq} = dequantization\ (\tau_q);$

$\tau_{DFrCT}(i:i+7, j:j+7) = IDFrCT\ (\tau_{dq});$

end

end

$T = mat2gray\ (\tau_{DFrCT});$

$T_1 = projection operator\ (T);$

$Y = TV based deblocking\ \ (T_1);$

end

end

end

4.2 Experiment Results and Discussions

The suggested JPEG anti-forensic method is evaluated in this section to confirm its capability by running several experiments on the UCID and BOSSBase databases. The single and double compressed image datasets were created by using quality values ranging from 50 to 95 to compress the images. Uncompressed version of the original image $\mathcal{T}$ is created by JPEG compressing image $\boldsymbol{I}$, and several anti-forensically processed images are created from this compressed images. All the images of UCID and BOSSBase datasets and their equivalent JPEG (anti-forensic) images are considered for the evaluation purpose. The proposed JPEG anti-forensic techniques are represented as follows:

- $\mathcal{F}D_1$, when shifted DFrCT becomes shifted DCT, represents the proposed approach (i.e. $'a'$ =1).
- $\mathcal{F}D_2$, referred to as anti-forensic strategy based on a shifted DFrCT methodology.

The proposed method primarily consists of a shifted DFrCT technique and the use of TV-based deblocking. The provided JPEG compressed image is subjected to a shifted DFrCT technique, as shown in Figure 4.2, it may smooth histograms on its own by filling gaps in the histogram of DFrCT coefficients distributed in a comb-like pattern.

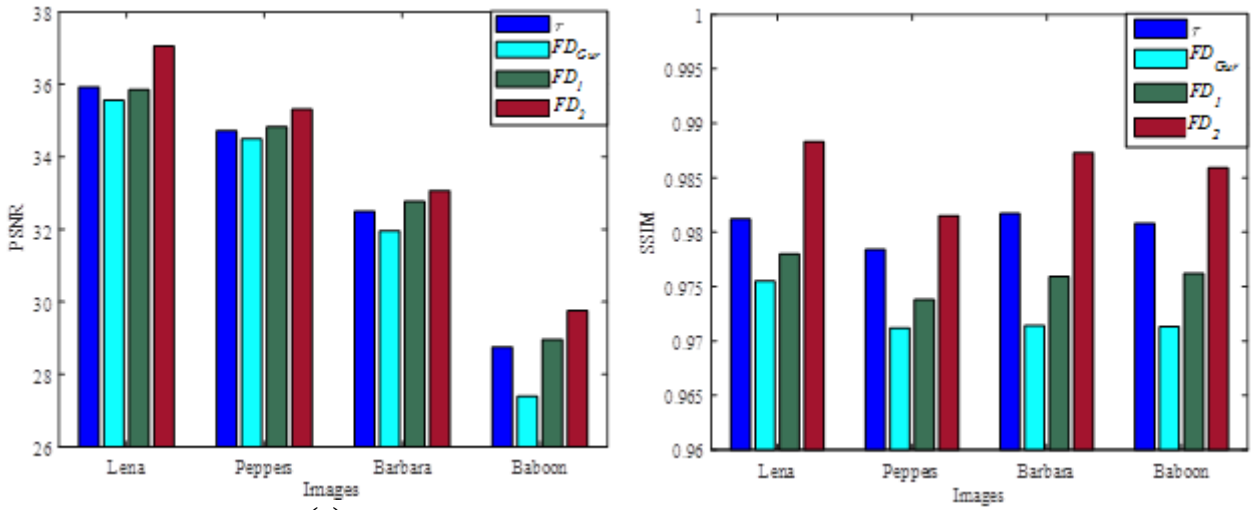
4.2.1 Comparative analysis of Anti-Forensic Methods

This section compares the proposed anti-forensic algorithms to existing anti-forensic approaches to evaluate their effectiveness. Figure 4.4 shows the efficiency of the suggested anti-forensic strategies $\mathcal{F}D_1$ and $\mathcal{F}D_2$. The JPEG forgery $\mathcal{F}D_{Gur}$ [152] 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 $\mathcal{F}D_1$ has PSNR (dB) and SSIM value equals to **35.7736** and **0.9770,** respectively. Similarly, the proposed JPEG forgery $\mathcal{F}D_2$ provides PSNR (dB) and SSIM value equals to **35.7938** and **0.9778,** respectively. Therefore, the proposed techniques $\mathcal{F}D_1$and $\mathcal{F}D_2$ outperforms the existing $\mathcal{F}D_{Gur}$ technique in terms of PSNR and SSIM values.

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

Figure 4.4: (a) Image of Lena compressed in JPEG format with a $\mathcal{QF}$ of 50, (b) JPEG forgery $\mathcal{FD}_{Gur}$ [152], (c) Proposed JPEG forgery $\mathcal{FD}_1$, (d) Proposed JPEG forgery $\mathcal{FD}_2$.

In comparison to existing methodologies, as demonstrated in Figure 4.5, the suggested approach yields better results in terms of large SSIM and PSNR values.



(a) (b)

Figure 4.5: PSNR (dB) and SSIM values were calculated by comparing several types of images compressed with a $\mathcal{QF}$ of 50 using, $\mathcal{FD}_{Gur}$, $\mathcal{FD}_1$, $\mathcal{FD}_2$ in (a) and (b), respectively.

Table 4.1 and 4.2 present the values of PSNR and SSIM for the final image obtained after employing the proposed anti-forensics and existing JPEG anti-forensic methods for quality factor varying from 50 to 95. In most situations, a quality factor of 50 to 95 was chosen since a quality factor of 100 generates a much bigger image than a quality factor of 95 with just a modest gain in image visual quality. Furthermore, the proposed algorithm effectiveness is unaffected even if the quality factor is more than 95 because the image quality is already quite good with few artifacts of compression. The visual quality of an image is severely degraded when the quality factor is less than 50. Existing anti-forensic techniques have a hard time hiding the traces of

JPEG compression without sacrificing significant quality. As a result, a better balance among image visual quality and forensic undetectability is required.

Table-4.1: Lena image PSNR (dB) values after anti-forensic processing with $\mathcal{FD}_{Gur}$, $\mathcal{FD}_1$, $\mathcal{FD}_2$, using an uncompressed image as a reference.

Quality	$\mathcal{T}$	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
50	35.9278	35.5590	35.8510	37.0542
55	36.1309	35.7499	35.8939	37.1013
60	36.4763	36.0173	36.1992	37.3846
65	36.8801	36.3576	36.5445	37.7329
70	37.3470	36.6930	36.9394	38.2613
75	37.8534	37.0292	37.3000	38.6792
80	38.5547	37.4591	37.9844	39.4317
85	39.4585	37.9651	38.9304	40.2899
90	40.8408	39.0000	40.2000	41.6941
95	43.8079	40.6559	42.6900	44.5938

Table-4.2: Lena image SSIM values after anti-forensic processing, $\mathcal{FD}_{Gur}$, $\mathcal{FD}_1$, $\mathcal{FD}_2$, using an uncompressed image as a reference.

Quality	$\mathcal{T}$	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
50	0.9812	0.9759	0.9781	0.9883
55	0.9829	0.9778	0.9798	0.9896
60	0.9849	0.9795	0.9817	0.9904
65	0.9871	0.9817	0.9836	0.9916
70	0.9890	0.9838	0.9855	0.9921
75	0.9907	0.9857	0.9877	0.9933
80	0.9928	0.9873	0.9902	0.9942
85	0.9948	0.9899	0.9927	0.9957
90	0.9967	0.9929	0.9954	0.9972
95	0.9986	0.9961	0.9981	0.9989

The described JPEG anti-forensic method produced an average PSNR of 39.2223 dB when images from the UCID dataset were analysed on a broad scale. Similarly, using the described JPEG anti-forensic technique, the average SSIM value produced is 0.9931. In comparison to previous methodologies, the given anti-forensic methodology is found to provide improved forensic undetectability and image quality.

4.2.2 Evaluating the robustness of anti-forensic techniques against JPEG detectors

The major goal of suggested technique is to hide artifacts of JPEG compression and improve image quality while fooling existing forensic detectors. Anti-forensics are primarily concerned with forensic undetectability. The forensic undetectability refers to the inability of a forensic detector to detect a JPEG image that has been anti-forensically processed. The proposed anti-forensic approaches are tested using JPEG forensic detectors as attacks in this subsection. PSNR, SSIM, and K_L [141], K_F [96], K_U^1 [143] and K_U^2 [143] are used to evaluate the provided approach. Table 4.3 shows the results of forensic detectors such as K_L [141], K_F [96], K_U^1 [143] and K_U^2 [143] to evaluate forensic undetectability using various anti-forensic methods using various image types compressed with a quality factor of 50.

Table-4.3: Measures by a forensic detectors by considering several techniques $\mathcal{T}$, $\mathcal{FD}_{Gur}$, $\mathcal{FD}_1$ and $\mathcal{FD}_2$ based on images with a quality factor of 50.

Images	K_L [141]	K_F [96]	K_U^1 [143]	K_U^2 [143]
Lena T	59.4232	1.3646	8.6492	326.8495
Lena $\mathcal{FD}_{Gur}$	0.0512	0.0759	0.2045	4.1759
Lena $\mathcal{FD}_1$	**0.2231**	**0.0560**	**0.0130**	**0.3591**
Lena FD_2	**0.1147**	**0.0489**	**0.0316**	**0.1403**
Peppers $\mathcal{T}$	43.4967	1.5072	7.9472	286.3860
Peppers $\mathcal{FD}_{Gur}$	0.0672	0.1836	0.8139	17.7931
Peppers $\mathcal{FD}_1$	**0.0363**	**0.0817**	**0.0784**	**0.5913**
Peppers $\mathcal{FD}_2$	**0.0137**	**0.0538**	**0.0615**	**0.3613**
Barbara T	92.7305	0.8364	12.6939	628.7497
Barbara $\mathcal{FD}_{Gur}$	0.0649	0.2374	0.7482	123.9472
Barbara $\mathcal{FD}_1$	**0.0364**	**0.1393**	**0.0683**	**1.1752**
Barbara FD_2	**0.0271**	**0.1025**	**0.0475**	**1.0864**
Baboon $\mathcal{T}$	45.5463	0.5354	16.6410	1812.8530
Baboon $\mathcal{FD}_{Gur}$	0.0583	0.2508	0.8742	212.5296
Baboon $\mathcal{FD}_1$	**0.0310**	**0.1929**	**0.3729**	**3.8497**
Baboon $\mathcal{FD}_2$	**0.0153**	**0.1268**	**0.1849**	**1.9582**

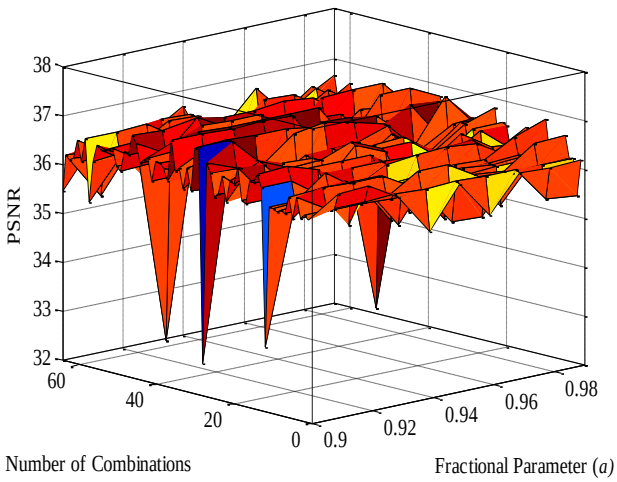
The efficacy of the associated forensic detectors is determined by the value of these measures K_L, K_F, K_U^1 and K_U^2. The values of these forensic detectors have decreased and indicate that the suggested anti-forensic approach has tricked the forensic detectors [143]. In the case of JPEG anti-forensics, lower values lead to stronger forensic undetectability. These measures have higher

values when compared to different anti-forensic methods, on the other hand, suggest that forensic detectors can identify JPEG compression artifacts. K_L is a calibrated metric [141] that is defined as follows:

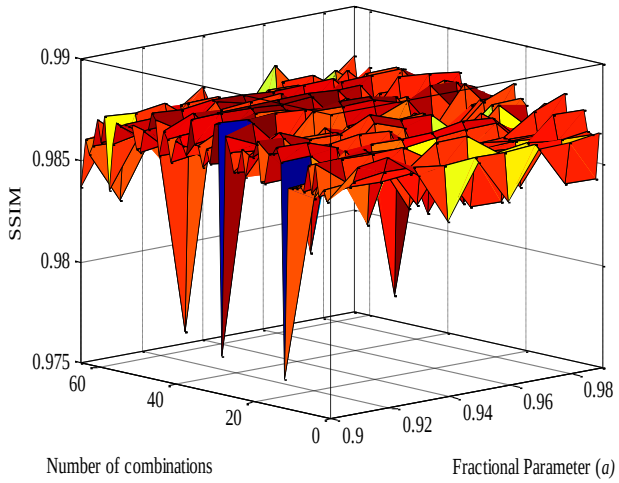
$$K_L = \frac{1}{28}\sum_{k=1}^{28}\left|\frac{var(D_kX)-var(D_kX_{cal})}{var(D_kX)}\right| \quad (4.9)$$

D_k is the k^{th} high-frequency subband's DCT coefficients matrix and var(·) is the variance function. The forensic undetectability improves when the difference in variance between the original image and its calibrated counterpart decreases..

Figure 4.6 shows that the given anti-forensic strategy outperforms in terms of visual quality of image by giving higher SSIM and PSNR values. Lower forensic detector parameter values, contrarily, indicate forensic undetectability, as illustrated in Figure 4.6. It is worth noting that good image quality indicates greater PSNR and SSIM values, whereas lower K_L, K_F, K_U^1 and K_U^2 values lower indicate greater forensic undetectability. For the considered image, 64 different combinations are created for each value of $'a'$ (fractional parameter). In this whole analysis, the fractional DFrCT parameter is varied from 0 to 1 with a step size of 0.01. It is observed that optimal results are obtained in terms of image visual quality and forensic undetectability with fractional parameter value in the range of 0.9 to 0.99 for all the considered images.



(a)



(b)

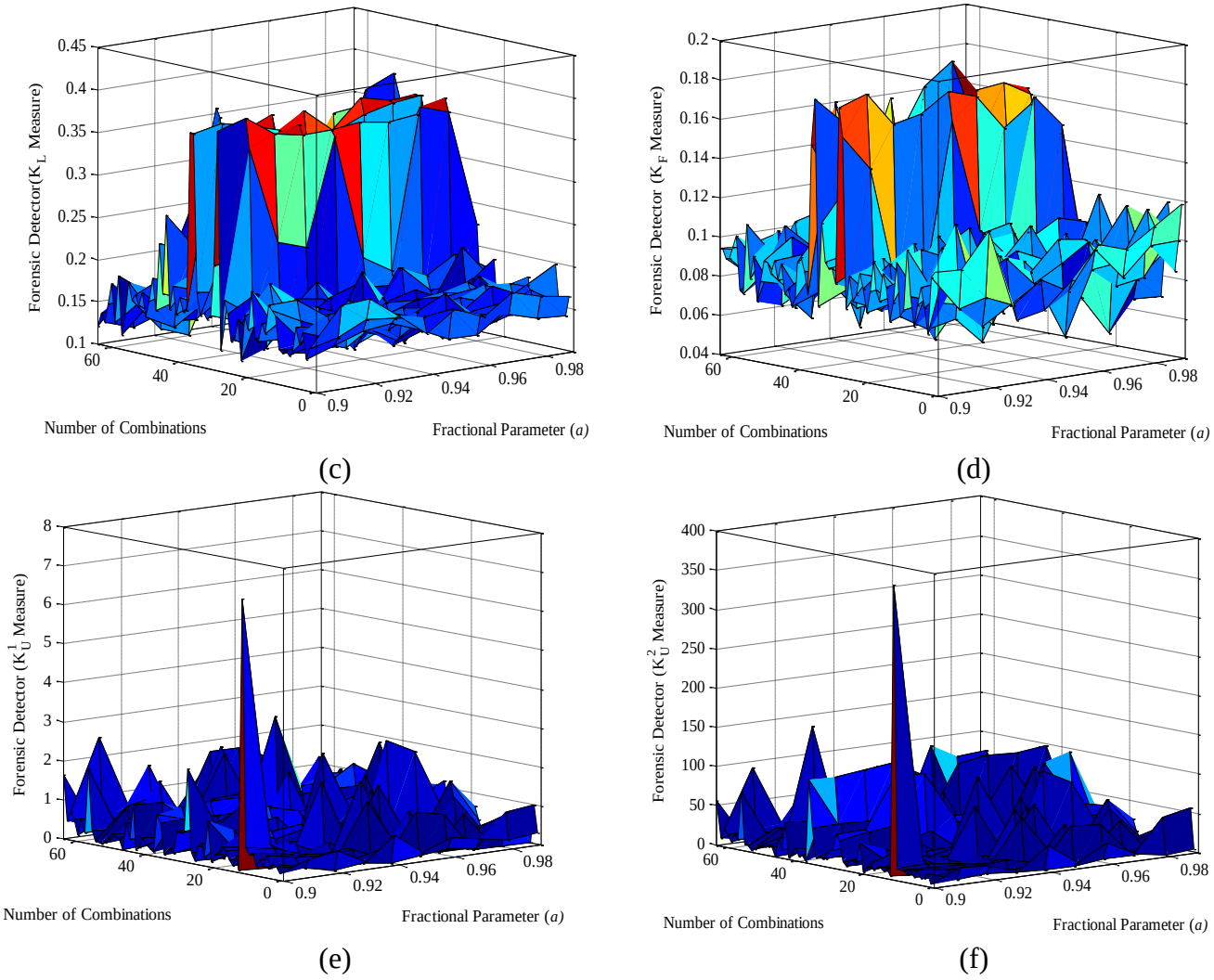
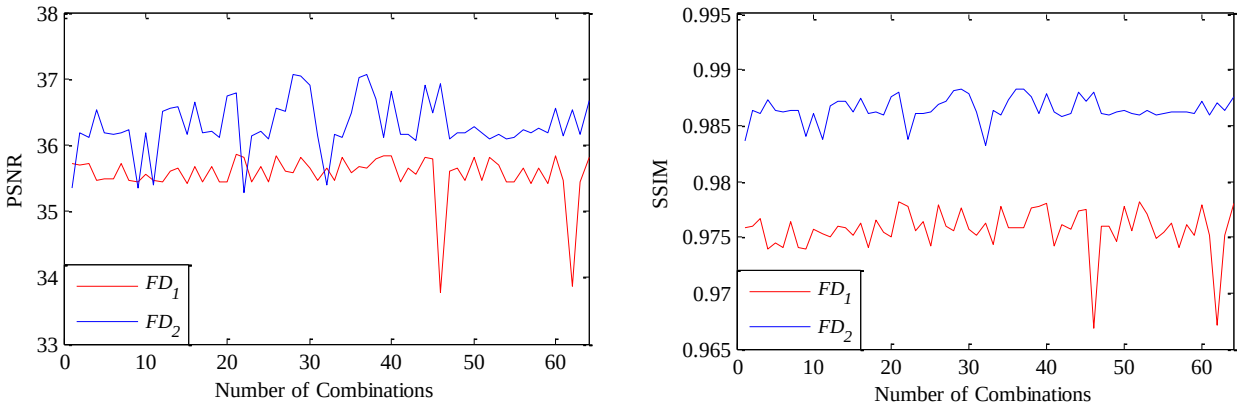


Figure 4.6: 3-D graphs (a) PSNR (dB), (b) SSIM, (c) K_L,(d) K_F, (e) K_U^1 and (f) K_U^2 for the Lena image with respect to $'a'$ and number of combinations.

Fractional order of 0.94 achieves the best results for the standard Lena image. The proposed anti-forensic approach, as illustrated in Figure 4.6 (a), achieves the maximum PSNR of 37.0542 dB out of all 64 combinations. Figure 4.6 (b) shows the SSIM value of 0.9883 for the provided anti-forensic technique. As a result, the given anti-forensic approach is proven to improve image quality while maintaining excellent forensic undetectability. As shown in Figure 4.6 (f), the value of the detector K_U^2 has rapidly decreased from 375.9582 to 0.1403. Other forensic detectors, such as K_L, K_F and K_U^1, have very low values, as shown in Figure 4.6 (c), (d), and (e), respectively. The suggested system aspires to improve PSNR and SSIM values for quality of image as well as forensic undetectability in terms of K_L,K_F, K_U^1 and K_U^2.

As a result, the data in Figure 4.6 demonstrate the effectiveness of the suggested anti-forensics methodology in deceiving existing forensic detectors. A comparison of DFrCT and DCT-based anti-forensic procedures is used to further evaluate the efficiency of the presented method. DFrCT contains an additional free parameter $\alpha = a\pi/2$ that allows $'a'$ to vary from zero to unity. Conventional DCT is produced from DFrCT, when it is unity.



(a) (b)

Figure 4.7: Variation of (a) PSNR (dB), (b) SSIM with respect to feasible combinations using the suggested approaches $\mathcal{F}D_1$ and $\mathcal{F}D_2$.

Figure 4.7 (a) and (b) show both DFrCT and DCT yields good PSNR and SSIM results, however DFrCT outperforms DCT owing to the fractional parameter, which adds flexibility to increase forensic undetectability and image quality. Similarly, when examining both DFrCT and DCT in Figure 4.8, additional forensic detectors namely K_L, K_F, K_U^1 and K_U^2 have very small values. It is worth noting that forensic undetectability rises as the value of the forensic detector parameter decreases. The final anti-forensically processed image is determined based on ideal parameter values shown in Figures 4.7 and 4.8. This demonstrates how effectively the suggested anti-forensics method deceives existing forensic detectors.

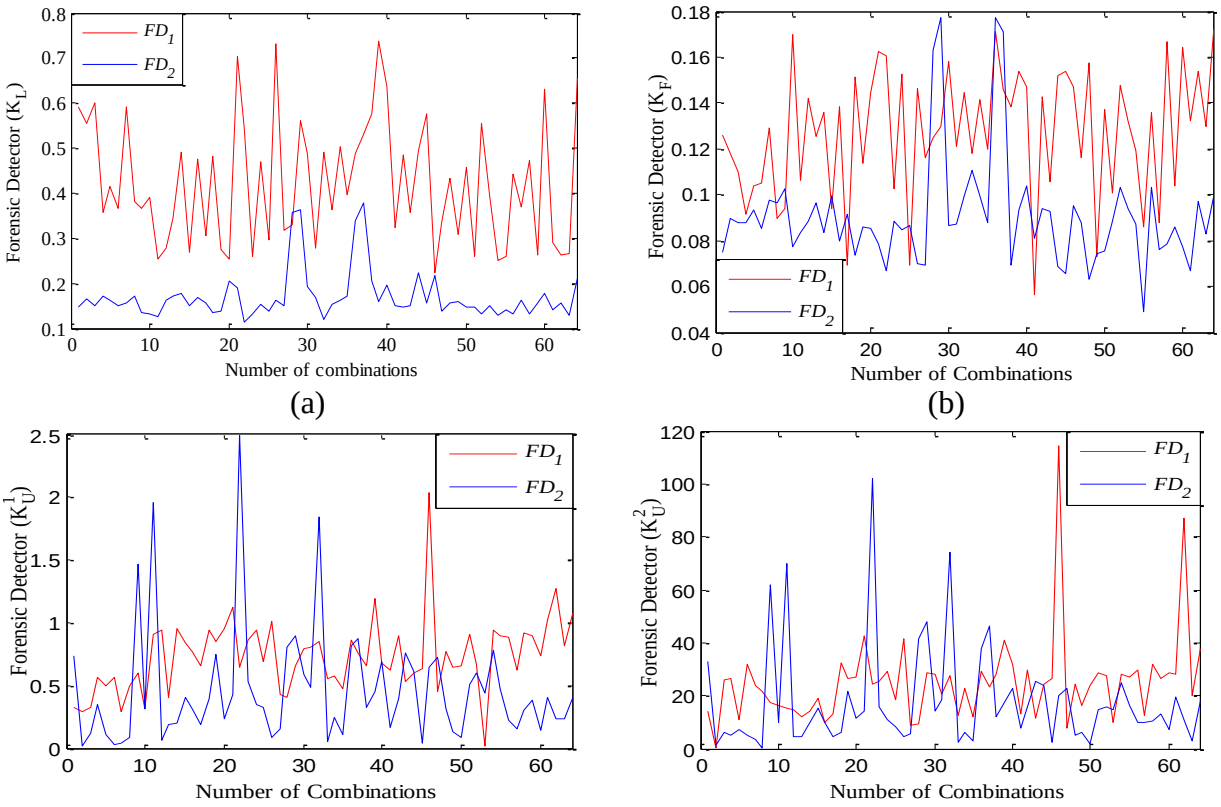


Figure 4.8: Various forensic detectors have different behaviours (a) K_L, (b) K_F, (c) K_U^1 and (d) K_U^2, with respect to the 64 feasible combinations using the suggested anti-forensic approaches $\mathcal{F}D_1$ and $\mathcal{F}D_2$.

The proposed method is designed to hide compression artifacts. The SVM classifier is used to classify the compressed and uncompressed images while taking into account the UCID dataset. The UCID dataset is used to train the classifier. True Positive Rate (TPR) indicates that anti-forensically treated images are accurately recognised as compressed images. Out of the total, 669 images are used for training and remaining images are used for testing. The curve near proximity to the diagonal indicates a high level of forensic undetectability against the detector under consideration (randomness). Figure 4.9 (a) and Figure 4.9 (b) demonstrate current JPEG anti-forensic techniques against various detectors when compared to previous JPEG anti-forensic approaches. The recommended approach ROC curves are closer to the diagonal. The fact that the curve is so near to the diagonal implies a high level of forensic undetectability against the detectors in question. The ability of a specific forensic detector to detect anti-forensic method improves as the curve approaches the upper left corner. It is worth noting that when forensic

undetectability increases, anti-forensic approaches become more effective at deceiving forensic detectors. While JPEG forgeries that are created with the presented technique demonstrates that 98.93% of the images are classified as not JPEG compressed. K_{Li}^{S100} and K_{P}^{S162} are machine learning forensic detectors based on SVM, offer a minimum decision error of less than 0.1 in steganalysis. The JPEG compression artifacts are hidden by modifying the DFrCT coefficients. Modifying the DFrCT coefficients leads to a greater modification rate in image steganalysis (bits per pixel).

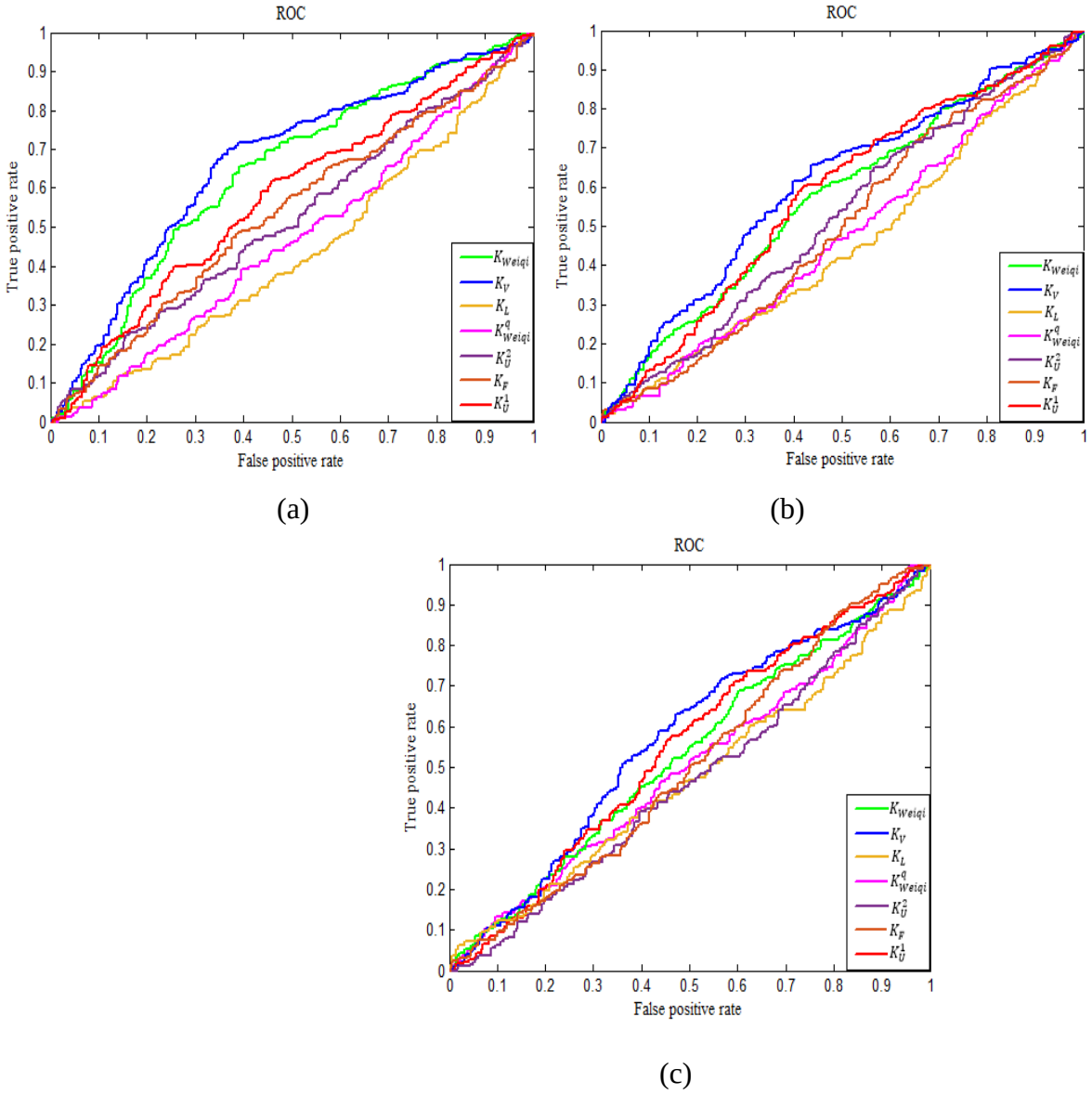


Figure 4.9: ROC curves of (a) $\mathcal{FD}_{Fan}$, (b) $\mathcal{FD}_{Gur}$ and (c) $\mathcal{FD}_2$ against various scalar based forensic detectors.

Table-4.4: Evaluation of minimum decision error while testing against K_{Li}^{S100} by taking various replacement rates of image.

Image Replacement Rate	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
0.05	0.263	0.388	0.448	0.403	0.397	0.465	0.464	0.468	0.480	0.485
0.10	0.181	0.327	0.374	0.302	0.314	0.406	0.385	0.403	0.415	0.426
0.15	0.135	0.263	0.318	0.205	0.228	0.353	0.338	0.345	0.360	0.371
0.20	0.103	0.209	0.286	0.157	0.193	0.324	0.314	0.321	0.330	0.335
0.30	0.062	0.148	0.208	0.086	0.106	0.258	0.262	0.268	0.270	0.273
0.40	0.048	0.112	0.157	0.063	0.068	0.216	0.214	0.227	0.235	0.247
0.50	0.021	0.068	0.103	0.028	0.053	0.174	0.163	0.187	0.202	0.216

Table-4.5: Evaluation of minimum decision error while testing against K_P^{S162} by taking various replacement rates of image.

Image Replacement Rate	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
0.05	0.322	0.387	0.283	0.479	0.309	0.406	0.428	0.421	0.491	0.497
0.10	0.256	0.316	0.186	0.401	0.217	0.338	0.348	0.344	0.423	0.436
0.15	0.197	0.257	0.104	0.323	0.143	0.267	0.286	0.288	0.352	0.372
0.20	0.151	0.203	0.053	0.274	0.106	0.224	0.245	0.235	0.297	0.304
0.30	0.110	0.148	0.032	0.213	0.062	0.163	0.179	0.183	0.247	0.317
0.40	0.075	0.118	0.023	0.172	0.045	0.131	0.154	0.148	0.196	0.230
0.50	0.053	0.091	0.016	0.124	0.031	0.094	0.113	0.104	0.133	0.161

Table-4.6: Evaluation of minimum decision error while testing against $K_{SRM}^{S\,714}$ by taking various replacement rates of image.

Image Replacement Rate	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
0.05	0.285	0.315	0.335	0.361	0.369	0.403	0.415	0.463	0.487	0.492
0.10	0.201	0.225	0.242	0.295	0.315	0.337	0.367	0.405	0.439	0.452
0.15	0.113	0.137	0.163	0.224	0.263	0.274	0.302	0.347	0.385	0.397
0.20	0.072	0.125	0.128	0.165	0.224	0.236	0.259	0.308	0.327	0.351
0.30	0.035	0.062	0.072	0.116	0.155	0.173	0.196	0.238	0.263	0.327
0.40	0.023	0.041	0.053	0.092	0.124	0.138	0.158	0.193	0.229	0.253
0.50	0.014	0.025	0.033	0.073	0.092	0.104	0.127	0.158	0.173	0.194

To assess the effectiveness of the anti-forensic approach that has been presented, JPEG forgeries were created using an experimental steganography setup. The proposed approach is actually

evaluated utilizing the image replacement technique provided in [47]. The anti-forensically processed image replaces the uncompressed image center area. Now, datasets are generated for evaluation purposes using this process, which takes into account numerous anti-forensic methods. When various image replacement rates are taken into consideration, Tables 4.4 to 4.6 indicate the average values of minimal decision error. When compared to previous anti-forensic techniques, the minimum decision error attained is larger when evaluated against K_{Li}^{S100}, K_{P}^{S162} and $K_{SRM}^{S\,714}$ machine learning-based forensic detectors, as shown in Tables 4.4 to 4.6. As a result, the suggested JPEG anti-forensic method is further demonstrated utilising the idea of image replacement rate.

4.2.3 Experimental results obtained by considering BOSSBase dataset

The suggested methodology efficacy is further confirmed in this subsection by using the BOSSBase image dataset [154]. This dataset contains 10,000 raw pictures, with 5000 being used for training while the other half is used for testing. Training and testing databases for BOSSBase are developed in the same manner as that of UCID. The values of minimum decision error versus SVM-based detectors K_{Li}^{S100}, K_{P}^{S162} and $K_{SRM}^{S\,714}$ for the BOSSBase dataset with varied image replacement rates are provided in Tables 4.7 to 4.9. The results produced with the BOSSBase dataset are quite similar to those obtained with the UCID dataset, as seen in Tables 4.7 to 4.9. In comparison to existing strategies, the suggested anti-forensic methodology performs better.

Table-4.7: Evaluation of minimum decision error while testing against K_{Li}^{S100} by taking various replacement rates of image.

Image Replacement Rate	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
0.05	0.226	0.324	0.416	0.383	0.371	0.431	0.453	0.459	0.473	0.483
0.10	0.153	0.292	0.359	0.287	0.301	0.395	0.374	0.409	0.424	0.431
0.15	0.118	0.247	0.305	0.197	0.204	0.313	0.338	0.352	0.359	0.368
0.20	0.091	0.193	0.253	0.145	0.176	0.291	0.302	0.314	0.327	0.331
0.30	0.049	0.114	0.196	0.064	0.093	0.233	0.247	0.253	0.268	0.286
0.40	0.035	0.093	0.135	0.049	0.057	0.193	0.201	0.218	0.229	0.238
0.50	0.016	0.037	0.094	0.021	0.042	0.146	0.153	0.175	0.197	0.207

Table-4.8: Evaluation of minimum decision error while testing against K_P^{S162} by taking various replacement rates of image.

Image Replacement Rate	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
0.05	0.235	0.257	0.304	0.357	0.394	0.403	0.415	0.438	0.459	0.472
0.10	0.179	0.210	0.247	0.304	0.312	0.341	0.347	0.392	0.404	0.434
0.15	0.127	0.132	0.153	0.236	0.258	0.286	0.291	0.314	0.351	0.371
0.20	0.092	0.099	0.148	0.191	0.214	0.237	0.243	0.263	0.295	0.317
0.30	0.048	0.057	0.102	0.137	0.152	0.179	0.186	0.205	0.242	0.303
0.40	0.035	0.041	0.055	0.102	0.117	0.152	0.159	0.167	0.203	0.229
0.50	0.015	0.024	0.031	0.078	0.104	0.118	0.127	0.141	0.166	0.175

Table-4.9: Evaluation of minimum decision error while testing against $K_{SRM}^{S\,714}$ by taking various replacement rates of image.

Image Replacement Rate	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
0.05	0.217	0.251	0.292	0.32	0.34	0.36	0.43	0.451	0.468	0.482
0.10	0.153	0.198	0.225	0.265	0.285	0.31	0.34	0.374	0.413	0.445
0.15	0.106	0.122	0.158	0.195	0.235	0.25	0.275	0.307	0.365	0.388
0.20	0.065	0.085	0.115	0.150	0.195	0.21	0.239	0.258	0.302	0.324
0.30	0.037	0.054	0.067	0.101	0.13	0.15	0.175	0.188	0.261	0.311
0.40	0.013	0.035	0.046	0.077	0.095	0.11	0.128	0.143	0.214	0.246
0.50	0.007	0.020	0.031	0.052	0.065	0.08	0.097	0.110	0.176	0.193

The SVM classifier is also less susceptible to the dimensionality curse [154]. As a result, the size of the dataset has only a minor influence on the SVM classifier's efficiency. The BOSSBase dataset achieved nearly similar minimum decision error values to those obtained using the UCID dataset images validates the stability of the proposed approach's performance. Double compression artifact detectors [7], [109], [146] are used to test double JPEG compressed images to confirm the efficacy of the given anti-forensic method. When evaluated against multiple forensic detectors utilizing all quality factors ranging from 50 to 95, Tables 4.10, 4.11, and 4.12 demonstrate that the proposed anti-forensic technique outperforms current methods with minimum decision error values approaching 0.5.

Table-4.10: Minimum decision error values for double compressed JPEG images using different quality factors ($\mathcal{QF}_2$) versus the forensic detector provided in [7].

Quality	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
50	0.378	0.469	0.453	0.419	0.413	0.406	0.431	0.439	0.491	0.495
55	0.342	0.465	0.450	0.421	0.437	0.418	0.458	0.469	0.473	0.486
60	0.328	0.460	0.454	0.425	0.423	0.404	0.461	0.475	0.481	0.488
65	0.281	0.458	0.457	0.431	0.411	0.401	0.465	0.471	0.479	0.482
70	0.252	0.451	0.448	0.434	0.391	0.374	0.457	0.469	0.472	0.475
75	0.243	0.446	0.455	0.439	0.378	0.379	0.459	0.465	0.476	0.480
80	0.191	0.439	0.451	0.447	0.367	0.363	0.449	0.458	0.484	0.491
85	0.144	0.431	0.446	0.449	0.352	0.357	0.451	0.463	0.479	0.483
90	0.080	0.420	0.449	0.451	0.335	0.345	0.448	0.458	0.473	0.479
95	0.003	0.401	0.451	0.454	0.306	0.336	0.452	0.460	0.465	0.474

Table-4.11: Minimum decision error values for double compressed JPEG images using different quality factors ($\mathcal{QF}_2$) versus the forensic detector provided in [146].

Quality	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
50	0.372	0.441	0.457	0.442	0.455	0.469	0.464	0.480	0.482	0.489
55	0.321	0.421	0.439	0.454	0.448	0.446	0.453	0.465	0.487	0.493
60	0.313	0.410	0.425	0.447	0.441	0.467	0.456	0.459	0.479	0.481
65	0.310	0.382	0.443	0.434	0.452	0.429	0.461	0.472	0.464	0.475
70	0.265	0.364	0.435	0.412	0.446	0.447	0.450	0.462	0.454	0.470
75	0.237	0.353	0.465	0.368	0.451	0.465	0.441	0.469	0.473	0.485
80	0.182	0.327	0.432	0.339	0.437	0.443	0.429	0.479	0.469	0.488
85	0.152	0.295	0.411	0.301	0.434	0.461	0.419	0.475	0.463	0.475
90	0.089	0.274	0.428	0.278	0.452	0.453	0.407	0.470	0.474	0.478
95	0.051	0.260	0.436	0.262	0.431	0.438	0.416	0.463	0.446	0.469

Table-4.12: Minimum decision error values for double compressed JPEG images using different quality factors ($\mathcal{QF}_2$) versus the forensic detector provided in [109].

Quality	$\mathcal{T}$	$\mathcal{FD}_{S_q}$ [151]	$\mathcal{FD}_{S_qS_b}$ [115]	$\mathcal{FD}_V$ [118]	$\mathcal{FD}_{S_u}$ [125]	$\mathcal{FD}_F$ [143]	$\mathcal{FD}_{Fan}$ [47]	$\mathcal{FD}_{Gur}$ [152]	$\mathcal{FD}_1$ Proposed	$\mathcal{FD}_2$ Proposed
50	0.391	0.427	0.435	0.457	0.431	0.449	0.447	0.465	0.468	0.472
55	0.365	0.430	0.447	0.451	0.438	0.457	0.450	0.457	0.457	0.470
60	0.323	0.403	0.449	0.436	0.441	0.453	0.453	0.452	0.460	0.469
65	0.288	0.362	0.436	0.410	0.446	0.450	0.442	0.448	0.461	0.475
70	0.232	0.347	0.431	0.403	0.430	0.445	0.434	0.441	0.442	0.458
75	0.201	0.341	0.426	0.392	0.435	0.446	0.439	0.451	0.454	0.461
80	0.154	0.315	0.417	0.369	0.427	0.441	0.427	0.443	0.459	0.464
85	0.128	0.298	0.420	0.351	0.442	0.439	0.413	0.445	0.453	0.458
90	0.079	0.287	0.412	0.328	0.434	0.429	0.422	0.436	0.446	0.452
95	0.024	0.273	0.438	0.292	0.448	0.437	0.409	0.432	0.440	0.447

It is worth mentioning that a higher minimum decision error value indicates that the anti-forensic approach is more effective at deceiving forensic detectors. Anti-forensic methods, on the other hand, cannot mislead forensic detectors with smaller levels of minimum decision error, as demonstrated in [137]. As a result, the suggested DFrCT-based anti-forensic method can successfully conceal traces of compression, fooling several JPEG compression forensic detectors.

4.3 Summary

This chapter discusses the JPEG anti-forensic approach, which hides compression artifacts in the DFrCT domain and deceive both scalar and machine learning-based forensic detectors. The suggested shifted block DFrCT method effectively conceals JPEG compression artifacts and numerous JPEG forensic detectors. The benefit of the provided methodology is that it has an extra fractional parameter, which increases its flexibility. Blocking artifacts are further reduced using TV-based deblocking. As a consequence, several variables for each examined image are utilized in this chapter to optimize the recommended JPEG anti-forensic approach, such as shifted block and fractional parameter. In comparison to previous anti-forensic approaches, the presented JPEG anti-forensic system delivers higher image quality and forensic undetectability. Furthermore, because it is capable of outperforming most forensic approaches, the proposed strategy has sparked a significant debate about the robustness of forensic techniques. Therefore, in the next chapter, further work is dedicated to project a counter JPEG anti-forensic scheme to expose the JPEG compression even when anti-forensic attacks are present.

CHAPTER 5

FORENSIC APPROACH TO COUNTER JPEG ANTI-FORENSICS

The JPEG compression anti-forensic framework designed in the last chapter is capable of misleading the majority of forensic detectors. Therefore, there is a need to extend the research work towards countering the anti-forensic techniques. On the basis of statistical analysis of second-order, this chapter proposes a counter JPEG anti-forensic technique, which reveals the artifacts generated by JPEG anti-forensics. In fact, the majority of current forensic works on JPEG compression detection focuses on the analysis of first-order statistical feature components. By using anti-forensic approaches, forensic detectors relying on first-order statistical analysis can be easily misled. To counter these anti-forensic attacks, it is necessary to do higher-order statistical analysis. Using a second-order statistical analysis based on MTPM, the traces left by the dithering operation of different anti-forensic methods are discovered in this chapter. The proposed second order feature can detect grainy noise caused by anti-forensic techniques dithering operation. The suggested forensic system consists of two steps: selecting a target difference image and generating second-order statistical features for both intra and inter-block DCT domains by evaluating Markov Transition Probability Matrices (MTPMs). When compared to other methods, experiments have shown that the suggested forensic method based on MTPM can detect traces of JPEG compression even when anti-forensic attacks are present.

5.1 Countering JPEG compression Anti-Forensics

A counter JPEG anti-forensic approach on the basis of statistical analysis of second-order of the footprints is created, as illustrated in Figure 5.1. Even when an anti-forensic attack is present, the MTPMs are used in a second-order statistical analysis to develop a detection feature. It's worth mentioning that when DCT is used to convert images from the spatial domain to the frequency domain, the correlation among neighbouring coefficients within the DCT block weakens. However, there is still a link between surrounding coefficients in the same block. In addition, the adjacent block DCT coefficients have a significant correlation. Furthermore, when the quantization loss is ignored, the pixels difference is found to be linearly related to the DCT coefficients acquired from the same places in successive DCT blocks. Even though the

quantization loss is irreversible and predictable, it has an impact on the dependency. The loss due to quantization and dependency are revealed as a result of the correlation between the identical positions in neighbouring DCT blocks. As a result of this, to detect these relationships, frequency domain features in the intra-block and inter-block domains are obtained. As shown in Figure 5.1, the proposed system consists of three steps: selecting a target difference image, evaluating intra-block and inter-block Markov transition matrices for DCT domains, and generating a mono-dimensional signal. To discriminate between JPEG compressed and original images, the generated mono-dimensional signal is fed to SVM classifier.

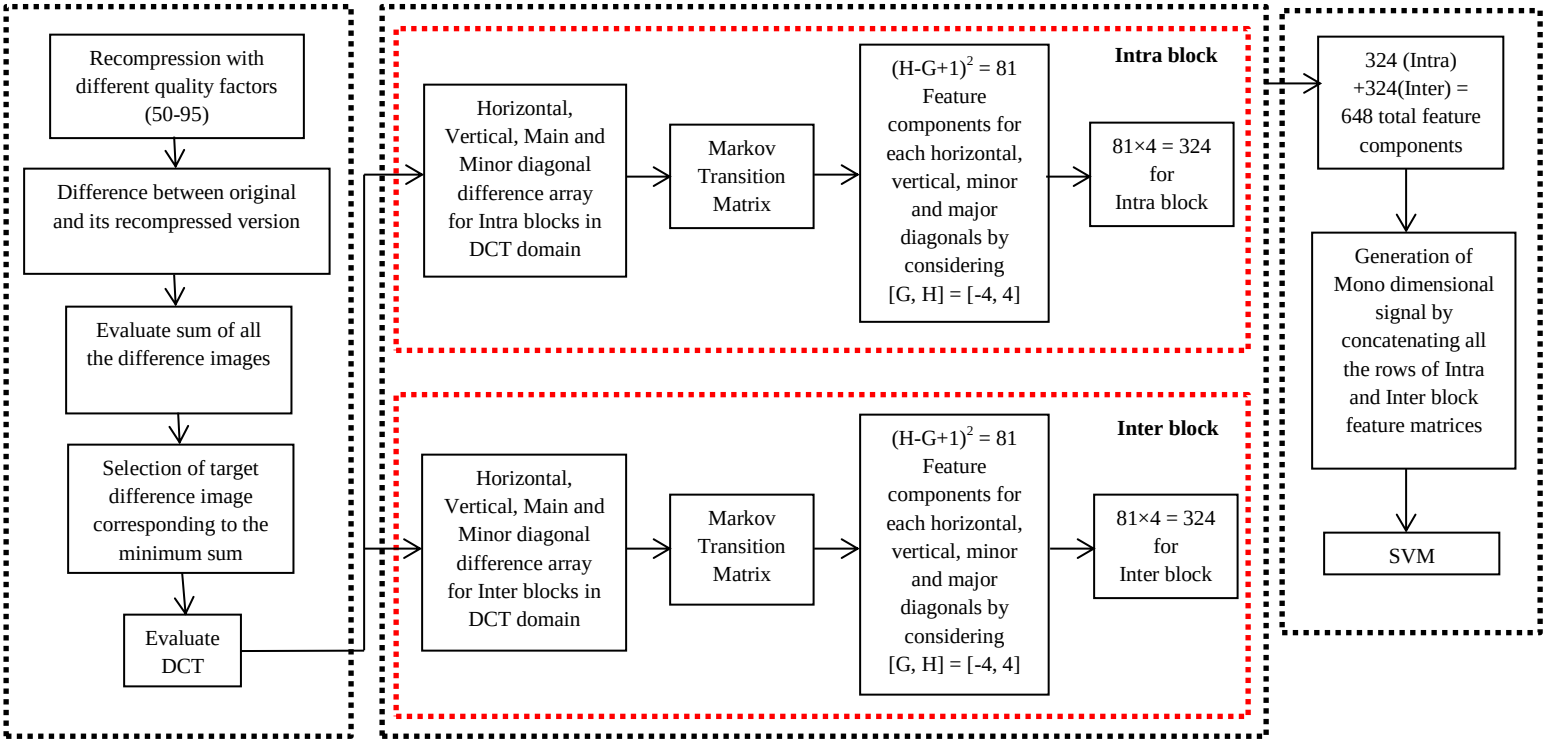


Figure 5.1: Proposed counter JPEG anti-forensic scheme.

5.1.1 Selecting Difference Image

The utilization of operations of image processing outcomes in the huge change in pixel values of original image. Consequently, preserving intrinsic statistics of the original image is a difficult challenge. Instead of considering the spatial domain, the difference domain is used to investigate the properties of neighbouring pixels in order to detect these changes. This is due to the explanation that the contents of the image are less affected by the difference domain. The image under consideration for inspection is largely compressed in JPEG format by considering a variety of quality variables ranging from 50 to 95. Subsequently, the change among the recompressed image and original image is then calculated. The difference between the considered image and its recompressed variants is computed. Then, we choose the difference image that corresponds to the least sum as our target image. Then, the target image is then subjected to DCT for further processing.

5.1.2 Evaluation of MTPMs in DCT domain

MTPM took advantage of the DCT coefficients' inter and intra-block correlation. Analyzing the DCT coefficients inside the same block yields the correlation of intra-block. Contrarily, DCT coefficients at the identical location of neighbouring blocks are used to calculate correlation of inter-block. The inconsistencies in the correlation of surrounding DCT coefficients are exploited using MTPM's second order statistical analysis. The 2-D DCT coefficients having an array size of 8×8 is obtained by processing the selected target difference image (I_{tar}) of dimension $m \times n$ as shown in Figure 5.2(a). $T'(f', e')$ denotes a 2-D DCT coefficient array with a total number of DCT blocks of $(m/8) \times (n/8)$. Afterward, the inconsistencies in the neighboring DCT coefficients correlation obtained in the difference domain is further highlighted by using difference DCT coefficient 2-D arrays along horizontal, vertical, main and minor diagonal directions as shown in Figure 5.3. To model these differential 2-D arrays, second order statistical study relying on the Markov random process is used.

In the horizontal and vertical directions, the MTPMs for intra-block adjacent DCT coefficients are estimated using (5.1.1) and (5.1.2), respectively. The features of MTPM with $\boldsymbol{\mathcal{P}}(T'(f' + 1, e') = v|T'(f', e') = u)$ and $\boldsymbol{\mathcal{P}}(T'(f', e' + 1) = v|T'(f', e') = u)$ as conditional distribution probabilities along horizontal and vertical directions, respectively for the coefficients pair (u,v)

are designated as $\boldsymbol{MTPM}_{intra,h}$ and $\boldsymbol{MTPM}_{intra,v}$. The function $\partial(a,b)=1$ for $a=b$, and $\partial(a,b)=0$, otherwise. The function $\partial(a,b)=1$ for $a=b$, and $\partial(a,b)=0$, otherwise. MTPMs are evaluated along main and minor diagonal difference arrays in a similar way [144].

$$\boldsymbol{MTPM}_{intra,h}(u,v)=\boldsymbol{\mathcal{P}}(T'(f'+1,e')=v|T'(f',e')=u)$$
$$=\frac{\boldsymbol{\mathcal{P}}(T'(f',e')=u,T'(f'+1,e')=v)}{\boldsymbol{\mathcal{P}}(T'(f',e')=u)}$$
$$=\frac{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1}\partial(T'(f',e'),u)\partial(T'(f'+1,e'),v)}{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1}\partial(T'(f',e'),u)} \quad (5.1)$$

$$\boldsymbol{MTPM}_{intra,v}(u,v)=\boldsymbol{\mathcal{P}}(T'(f',e'+1)=v|T'(f',e')=u)$$
$$=\frac{\boldsymbol{\mathcal{P}}(T'(f',e')=u,T'(f',e'+1)=v)}{\boldsymbol{\mathcal{P}}(T'(f',e')=u)}$$
$$=\frac{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1}\partial(T'(f',e'),u)\partial(T'(f',e'+1),v)}{\sum_{e'=1}^{T_{e'}-1}\sum_{f'=1}^{T_{f'}-1}\partial(T'(f',e'),u)} \quad (5.2)$$

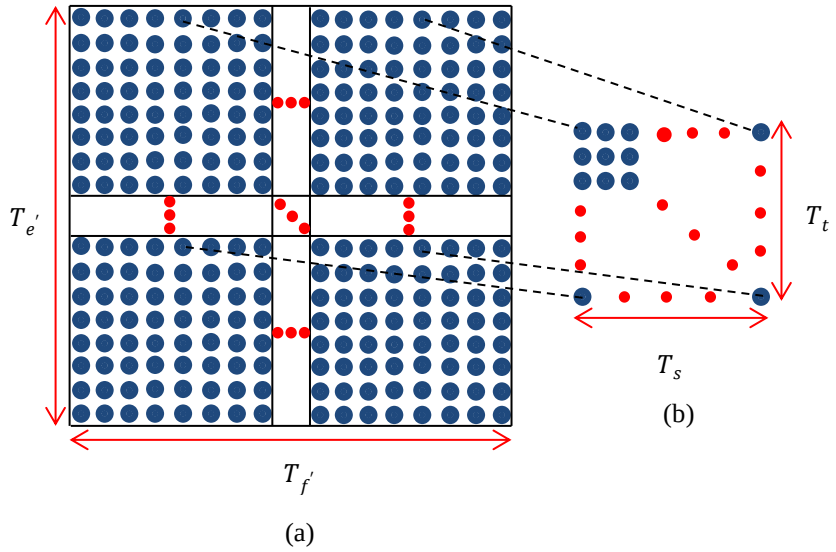


Figure 5.2 (a) DCT coefficients in a 2-D array, (b) Realisation of Mode (5) 2-D array.

Inter-block correlation can be shown along the modes of DCT coefficients, implying that coefficients at similar positions of adjacent 8×8 blocks can convey their frequency characteristics. Initially, 2-D arrays are constructed using the DCT coefficient 2-D array. As illustrated in Figure 5.3, the image's mode 2-D arrays are then employed to construct difference mode 2-D arrays in various orientations to represent the correlation of inter-block.

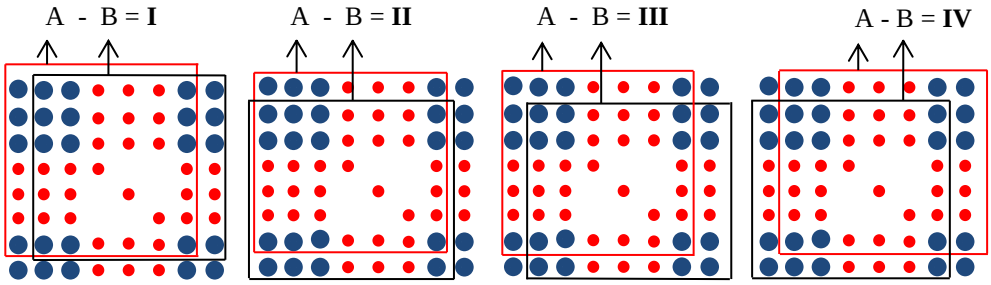


Figure 5.3: Horizontal (I), Vertical (II), Main diagonal (III), and Minor diagonal (IV) directions of a difference DCT/Mode 2-D array.

These difference mode 2-D arrays are then subjected to the Markov process. To construct the average transition probability matrix, each difference mode 2-D array is processed in all directions. Figure 5.2 (b) depicts the mode (5) 2-D array construction. $T_t = T_{e'}/8$ and $T_s = T_{f'}/8$ in vertical and horizontal directions, respectively, are the dimensions of each mode 2-D array. Because the DC component also known as mode 1 has no major effect on the results, it is not included in the calculations. As a result, for the considered image, only 63 mode 2-D arrays are produced. The mode coefficient in a mode 2-D array is described as $T^{(mode)}(s,t)$, such that $mode \in [2,64]$, $s \in [0, T_s - 2]$ and $t \in [0, T_t - 2]$. In four directions, the difference mode 2-D array is computed as [155]:

$$T_h^{(mode)}(s,t) = T^{(mode)}(s,t) - T^{(mode)}(s+1,t) \tag{5.3}$$

$$T_v^{(mode)}(s,t) = T^{(mode)}(s,t) - T^{(mode)}(s,t+1) \tag{5.4}$$

$$T_{d'}^{(mode)}(s,t) = T^{(mode)}(s,t) - T^{(mode)}(s+1,t+1) \tag{5.5}$$

$$T_{d''}^{(mode)}(s,t) = T^{(mode)}(s+1,t) - T^{(mode)}(s,t+1) \tag{5.6}$$

Eqs. (5.7) and (5.8) are used to calculate the MTPMs for inter-block neighbouring DCT coefficients in the horizontal as well as vertical direction, respectively. The coefficients pair MTPM features (v,u) conditional distribution probabilities in both horizontal and vertical directions $\boldsymbol{\mathcal{P}}(T_h(s+1,t) = v | T_h(s,t) = u)$ and $\boldsymbol{\mathcal{P}}(T_v(s,t+1) = v | T_v(s,t) = u)$ are denoted

by $\boldsymbol{MTPM}_{inter,h}$ and $\boldsymbol{MTPM}_{inter,v}$, respectively. For inter-block DCT coefficients, MTPM can be defined in a similar way for the main as well as minor diagonal difference arrays. Each MTPM is made up of $(H-G+1)^2$ elements, where u and v is in range $[G,H]$ Eq. (5.9) is used to compute a matrix with $(H-G+1)^2$ feature components. The inconsistencies introduced due to the modification of neighboring DCT coefficients correlation dominates near the origin. As a result, the range of u and v is considered to be $[-4,4]$, each MTPM giving 81 feature components. As a result, all of the MTPMs yield 648 feature components [155].

$$\boldsymbol{MTPM}_{inter,h}(u,v) = \boldsymbol{\mathcal{P}}(T_h(s+1,t)=v|T_h(s,t)=u)$$
$$= \frac{\boldsymbol{\mathcal{P}}(T_h(s,t)=u, T_h(s+1,t)=v)}{\boldsymbol{\mathcal{P}}(T_h(s,t)=u)}$$
$$= \frac{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_h^{(mode)}(s,t)=u)\partial(T_h^{(mode)}(s+1,t)=v)}{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_h^{(mode)}(s,t)=u)} \quad (5.7)$$

$$\boldsymbol{MTPM}_{inter,v}(u,v) = \boldsymbol{\mathcal{P}}(T_v(s,t+1)=v|T_v(s,t)=u)$$
$$= \frac{\boldsymbol{\mathcal{P}}(T_v(s,t)=u, T_v(s,t+1)=v)}{\boldsymbol{\mathcal{P}}(T_v(s,t)=u)}$$
$$= \frac{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_v^{(mode)}(s,t)=u)\partial(T_v^{(mode)}(s,t+1)=v)}{\sum_{t=1}^{T_t-2}\sum_{s=0}^{T_s-2}\sum_{mode=2}^{64}\partial(T_v^{(mode)}(s,t)=u)} \quad (5.8)$$

$$\boldsymbol{MTPM} = \begin{bmatrix} \boldsymbol{\mathcal{P}}(G|G) & \boldsymbol{\mathcal{P}}(G|G+1) & \cdots & \boldsymbol{\mathcal{P}}(G|H) \\ \boldsymbol{\mathcal{P}}(G+1|G) & \boldsymbol{\mathcal{P}}(G+1|G+1) & \cdots & \boldsymbol{\mathcal{P}}(G+1|H) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{\mathcal{P}}(H|G) & \boldsymbol{\mathcal{P}}(H|G+1) & \ldots & \boldsymbol{\mathcal{P}}(H|H) \end{bmatrix} \quad (5.9)$$

In the following section, the artifacts are highlighted by further processing these feature components explored by the MTPMs. As a result, an efficient second-order statistical feature is generated.

5.1.3 Generation of mono-dimensional signal based on statistical analysis of second order

In this section, we will look at how anti-forensic approaches affect MTPMs. The majority of anti-forensic approaches are rely on optimization techniques that aim to determine the best

mapping for recovering of the uncompressed original image statistics. This method involves shifting of pixels from one bin to another on the basis of maximum pixel distortion. Such anti-forensic attacks are capable of totally erasing the gaps present in the JPEG compressed image histogram. Despite the fact that the images histograms are identical whether they are uncompressed or processed anti-forensically but the MTPM still shows traces. We are searching for an MTPM-derived second-order statistical feature which can effectively distinguish between the uncompressed and anti-forensically processed images.

Uncompressed Lena image

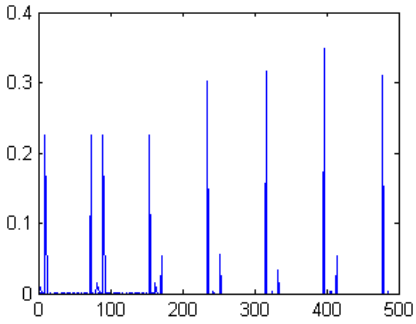
(a)

Image of Lena compressed in JPEG format with a quality of 50

(b)

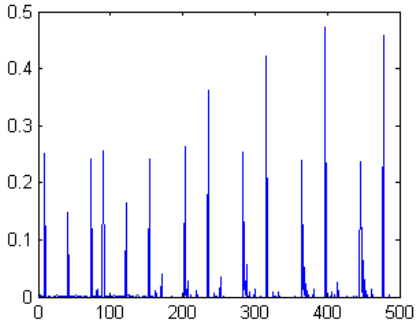
At a quality factor of 50, JPEG forgery ($\mathcal{F}D_{Fan}$)

(c)



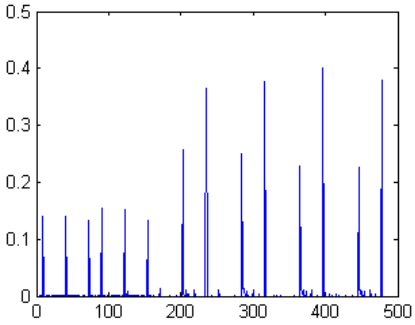
$\delta(n)$ for Lena uncompressed image

(d)



$\delta(n)$for Lena image compressed in JPEG with a quality of 50

(e)



$\delta(n)$ at 50 quality factor for Lena JPEG forgery ($\mathcal{F}D_{Fan}$)

(f)

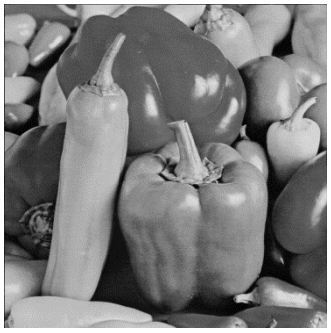


Image of Peppers uncompressed
(g)

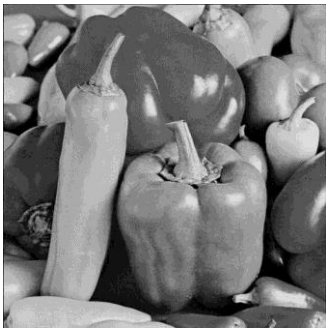
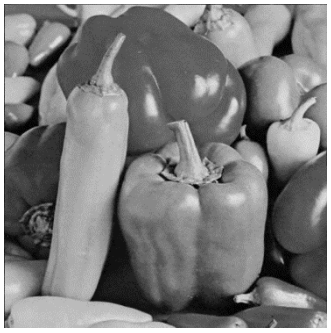
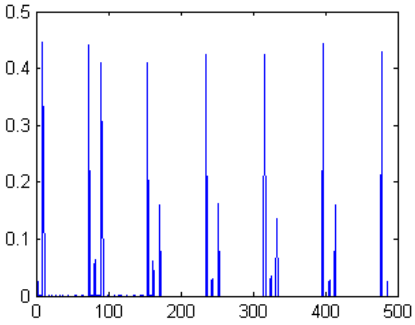


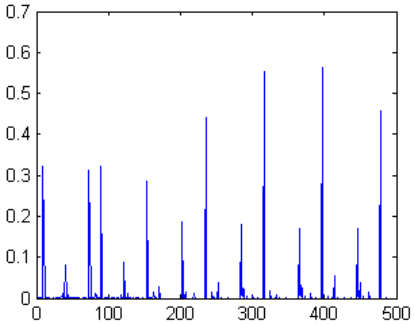
Image of peppers compressed in JPEG format with a quality of 50
(h)



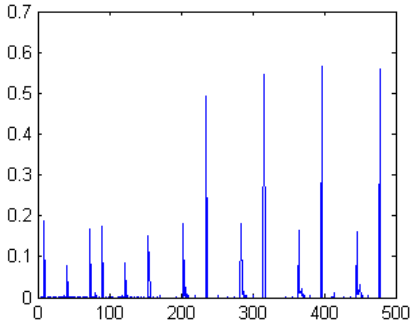
At a quality factor of 50, JPEG forgery ($\mathcal{F}D_{Fan}$)
(i)



$\delta(n)$ for the uncompressed image of Peppers
(j)



$\delta(n)$for image of Peppers encoded in JPEG with a quality of 50
(k)



$\delta(n)$ at 50 quality factor for Peppers JPEG forgery ($\mathcal{F}D_{Fan}$)
(l)

Figure 5.4: Uncompressed, JPEG compressed, and anti-forensically processed images of Lena and Peppers are revealed by (a), (b), (c), and (g), (h), (i) respectively. $\delta(n)$ for (a), (b), (c), and (g), (h), (i) are revealed by (d), (e), (f), and (j), (k), (l), respectively.

A mono-dimensional signal is obtained by analysing several properties depending on the MTPM of the considered image. Concatenation of the rows of intra-block and inter-block MTPMs yields this signal. Dithering artifacts occur while processing the image anti-forensically, according to the study. Let $\delta(n)$ denote a mono-dimensional signal based on MTPMs with a size of (1, 648). According to signal $\delta(n)$, a smooth behavior is revealed by an uncompressed image while a JPEG compressed image and an image modified using anti-forensics exhibit oscillatory behaviour, as shown in Figure 5.4. Figure 5.4 (e) and Figure 5.4 (k) reveal that oscillations in JPEG compressed images are higher than in images processed with anti-forensics, as illustrated in Figure 5.4 (f) and Figure 5.4 (l) respectively. It is due to the employment of anti-forensic methods for hiding artifacts of JPEG compression so as to trick the detectors used in forensic

investigation. However, this feature is effective at recognising the JPEG images that are altered anti-forensically. SVM is used for the identification of signals generated by uncompressed as well as anti-forensically processed images by using this mono-dimensional signal.

The proposed JPEG forensic technique's algorithm:

***Input*:**
I_{input}: JPEG compressed or Anti-forensically processed JPEG image.
***Output*:**
f: Mono-dimensional feature
***Parameters*:**
I_{diff}: Difference image
$I_{recompressed}$: Recompressed image
QF: Quality factor

begin
$[x, y] = size(I_{input})$;
$QF = 50{:}\,1{:}\,95$;
$I_{difference} = zeros(x, y, length(QF))$;
Initialize $count = 1$;
for $i = QF$ ***do***
$I_{recompressed} = recompress(I_{input}, i)$; % Recompression with different quality factors
$I_{diff}(:,:,c) = I_{input}(:,:) - I_{recompressed}(:,:)$;
$T_{span}(:,:,c) = sum(sum(I_{diff}(:,:,c)))$;
$count = count + 1$;
end
$[value, index] = min(T_{span})$;
$I_{selected} = I_{diff}(:,:,index)$; % Difference image is chosen relating to the minimum sum
$I_{dct} = abs(dct(I_{selected}))$;
$f1 = MTPM_{intra,h}(I_{dct})$; $f2 = MTPM_{inter,h}(I_{dct})$; $f3 = MTPM_{intra,v}(I_{dct})$; $f4 = MTPM_{inter,v}(I_{dct})$;
$f5 = MTPM_{intra,d'}(I_{dct})$; $f6 = MTPM_{inter,d'}(I_{dct})$; $f7 = MTPM_{intra,d''}(I_{dct})$; $f8 = MTPM_{inter,d''}(I_{dct})$;
$f = [f1;\ f2;\ f3;\ f4;\ f5;\ f6; f7; f8]$; % Compute the resultant feature vector
end

5.2 Experiment Results

The presented counter anti-forensic method is examined in this chapter to demonstrate its capacity to identify JPEG compression footprints even after anti-forensics have been applied by performing several tests on standard databases such as UCID and BOSSBase. The images in both datasets are compressed using a range of quality factors from $\{50, 51, 52, \ldots, 95\}$. After that, these compressed images are subjected to different JPEG anti-forensic techniques with the

purpose to develop JPEG forgery datasets. The evaluation is performed by considering the various SVM-based forensic detectors.

5.2.1 Comparison of SVM-based Forensic Detectors

The minimum decision error (P_e) is used as an assessment parameter against various forensic detectors in steganalysis approaches [153], [156]. ROC curves for various JPEG forensic detectors are first calculated using negative and positive cases. Negative cases are images that are authentic and uncompressed, whereas the positive cases are JPEG (anti-forensic) images. However, the anti-forensic technique dithering operation in the spatial domain generates an artificial or grainy noise. Even after using JPEG anti-forensic methods, aim of the presented approach is to find compression footprints. It is believed that the forensic analyst is familiar with both anti-forensic and forensic methodologies and when it comes to SVM-based detectors, a sequence of forged images can be used to train the detector. This is the worst-case situation for anti-forensic methods. Popular detectors on the basis of SVM such as K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} can effectively defeat JPEG anti-forensic techniques. It is difficult to deceive detector based on machine learning by anti-forensic techniques [157]. For anti-forensic techniques, this is the worst-case scenario; however, it is perfect for forensic techniques. SVM-based detectors are trained by considering each form of anti-forensic JPEG image. In steganalysis, detectors based on SVM such as K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} have very low values of minimum decision error and good detection accuracy. The current SRM-34,671 is only utilized in SVM on rare occasions due to its large feature dimensionality [130]. SRM-714 [130], an upgraded version of SRM-34,671, has reduced feature dimensionality but performs similarly to SRM-34,671. As a result, the proposed technique is compared to SRM-714 in order to make the comparison viable. To disguise the JPEG compression footprints, the DCT coefficients are modified on a wide scale. In the case of image steganalysis, the modification rate is considerable when DCT coefficients are changed (bits per pixel). By constructing JPEG forgeries with replacement procedure, the performance of the suggested methodology K_{MTPM} is evaluated. With a substitution rate varying from 0.05 to 1, the center portion of a certain image in uncompressed format is replaced with processed image using JPEG anti-forensics. The forensic examination is carried out using uncompressed and processed images both. LIBSVM [133] with a Gaussian kernel is used to train

the SVM classifier. SVM parameters are determined using a multiplicative grid and five-fold cross-validation [145].

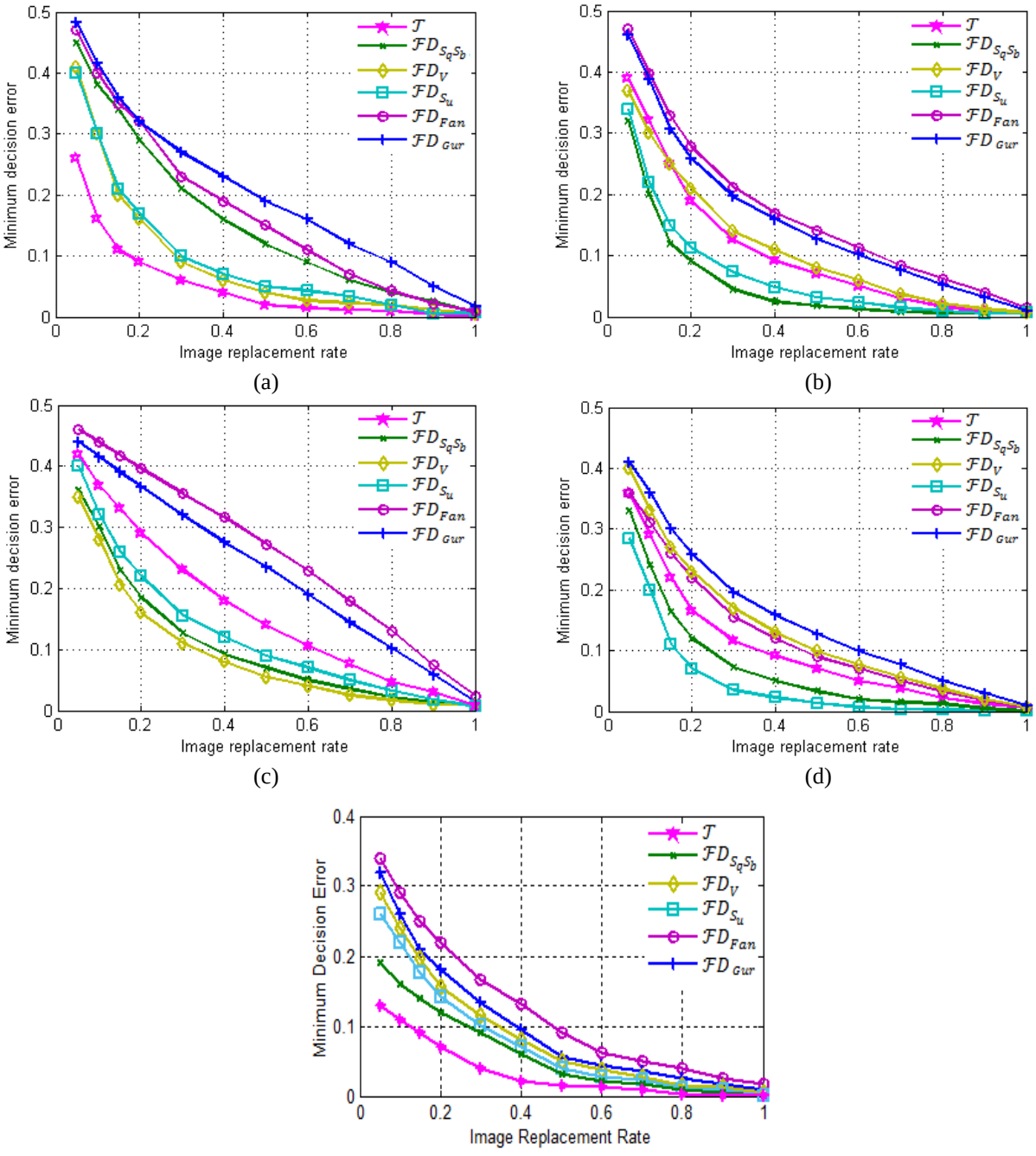


Figure 5.5: Using SVM-based detectors trained on the UCIDTrain dataset, by considering different image replacement rates against different forgeries, we calculated the minimum decision error. On the UCIDTest dataset, the results are obtained. (a) K_{Li}^{S100} [122], (b) K_{SPAM}^{S686} [145], (c) K_{AR}^{S10} [128], (d) K_{SRM}^{S714} [130], (e) Proposed (K_{MTPM}).

Figure 5.5 depicts the values of minimum decision error for several anti-forensic methods based on image replacement rate. The proposed methodology K_{MTPM} as shown in Figure 5.5(e) has outperformed Figure 5.5 (a) K_{Li}^{S100}, Figure 5.5 (b) K_{SPAM}^{S686}, Figure 5.5 (c) K_{AR}^{S10} and Figure 5.5 (d) K_{SRM}^{S714} by providing lower minimum decision error values against several approaches of anti-forensics. The proposed approach aims to distinguish among anti-forensically processed and compressed images. In forensic undetectability terms the techniques $\mathcal{F}D_{Fan}$ and $\mathcal{F}D_{Gur}$ outperforms the other anti-forensic techniques. This is because JPEG forgeries are created using explicit DCT histogram smoothing in JPEG anti-forensic approaches [47] and [152]. This smoothing causes the image statistics to change significantly. When the replacement rate is 0.10, the anti-forensic approach provided in [142] yields a high minimum decision error for existing SVM-based detectors. As a result, creating a forgery is as simple as exchanging a 112×160 size block for a 384×512 size UCID dataset image. The forger will produce a number of forgeries by substituting the 112×160 block, for example, in the image the forger will easily substitute the head of one individual. When attempting to make an entire JPEG image appear uncompressed, anti-forensic techniques have a difficult time in fooling machine learning detectors. JPEG anti-forensics is still used in a variety of scenarios, for example, concealing image splicing and double compression footprints. However, the proposed counter method has been enhanced for all anti-forensic approaches, which results in low values of minimum decision error, including 0.10, as shown in Figure 5.5. When compared to other techniques, the value of minimum decision error for $\mathcal{F}D_{Gur}, \mathcal{F}D_{v}, \mathcal{F}D_{Fan}$ is quite high. This is due to the explicit smoothing of the histogram. It's worth mentioning that a greater minimum decision error value indicates lower forensic detectability. Smaller minimum decision error values indicate improved forensic detection.

5.2.2 Counter Anti-Forensics of DJPG compression

The counter anti-forensic scheme is further validated in this section by testing it on anti-forensically processed DJPG compressed images. The effectiveness of the present forensic method and as well as the forensic detectors [146] and [109] is computed using various anti-forensic schemes. Images are compressed twice in double JPEG compression, first with the QF_1 and then with QF_2. During double JPEG compression, image cropping and content changes are possible. On JPEG images compressed with quality factor QF_1, current anti-forensic approaches

are used. According to the testing conditions, after using the anti-forensic process, the forged JPEG image can be left unused or cropped using a random grid shift. Finally, by compressing resultant image with QF_2, double JPEG compressed anti-forensic image is obtained.

5.2.2.1 Counter Anti-Forensics of NA-DJPG compression

The presented counter anti-forensic scheme is further explored to counter the NA-DJPG compression anti-forensics. Using an effective threshold detector, the integer periodicity map of DC coefficients' non-uniformity is determined in [109]. The image is first chosen from UCID dataset and compressed with QF_1. After that, the image is cropped with $0 \leq i, j \leq 7$ and random shift $(i, j) \neq (0, 0)$. The cropped image is then compressed again with QF_2, resulting in a NA-DJPG compressed image. Afterwards compression with quality factor QF_1, anti-forensics is performed. Using the method of [128], images from the UCID dataset are used to create various forms of JPEG forgeries. Because the anti-forensic approach takes a long time to compute only half of the images in the UCIDTest dataset are taken into account with 100 possible quality factor combinations i.e $QF_1 \; and \; QF_2 \in \{50, 55, 60, 65, 70, 75, 80, 85, 90, 95\}$ [152].

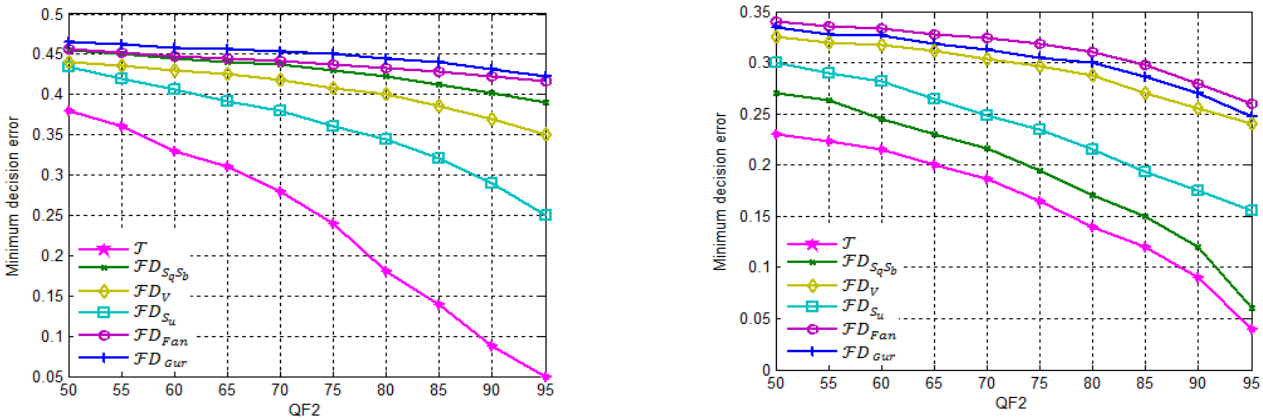


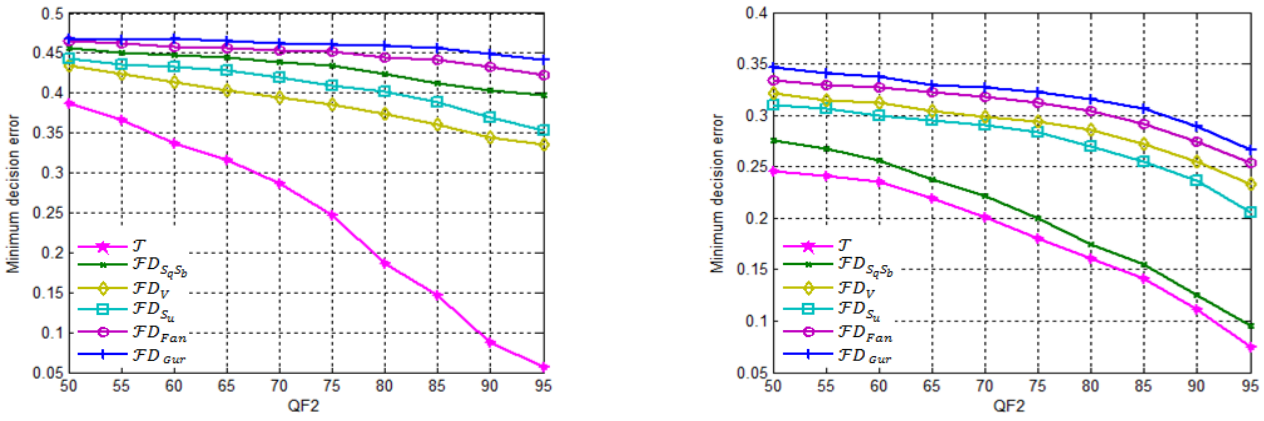
Figure 5.6: Testing on various types of forgeries, the minimum decision error is obtained using different QF_2 values against (a) NA-DJPG detector, (b) Proposed scheme K_{MTPM} on UCID dataset.

The proposed forensic detector (K_{MTPM}) and the NA-DJPG detector [109] are used to simultaneously analyze single and double compressed JPEG images. The average P_e for several types of forgeries using different QF_2 values is shown in Figure 5.6. When checked against the NA-DJPG detector, due to explicit histogram smoothing the anti-forensic approaches $\mathcal{FD}_{Gur}$ and $\mathcal{FD}_{Fan}$ demonstrate strong forensic undetectability [109]. The anti-forensic approach $\mathcal{FD}_{Fan}$

proposed in [47] successfully fools the majority of current JPEG forensic detectors. With a minimum decision error value of 0.5 , $\mathcal{FD}_{Fan}$ effectively fools the NA-DJPG detector [109]. This is because the NA-DJPG detector cannot detect integer periodicity. The suggested methodology will also reveal gaps in the DCT domain that are only partly filled. For various quality factor QF_2 values, the proposed forensic technique (K_{MTPM}), as shown in Figure 5.6, offers lower minimum decision error values. This demonstrates that the suggested method outperforms the current double compression forensic method [109] as tested against a variety of anti-forensic methods.

5.2.2.2 Counter Anti-Forensics of Aligned DJPG compression

The detection of A-DJPG anti-forensics is also of great significance in forensic examination. Pevný and Fridrich [128] generated a 144-dimensional feature vector from low-frequency DCT histograms. For categorization of single and DJPG compressed images, this feature vector is given into SVM. Penvy and Fridrich examine 9 low-frequency AC sub-bands while constructing the feature vector, and then, for each low-frequency sub-band, create a 16-bin histogram. Images from the UCIDTrain dataset were compressed to create the A-DJPG compressed images dataset with quality factor QF_1 and then compressing them again with QF_2, such as $QF_1 \neq QF_2$. As a result, half of the UCIDTest dataset images is considered, this case contains 90 different combinations for which JPEG forgeries of various types are produced.



(a) (b)

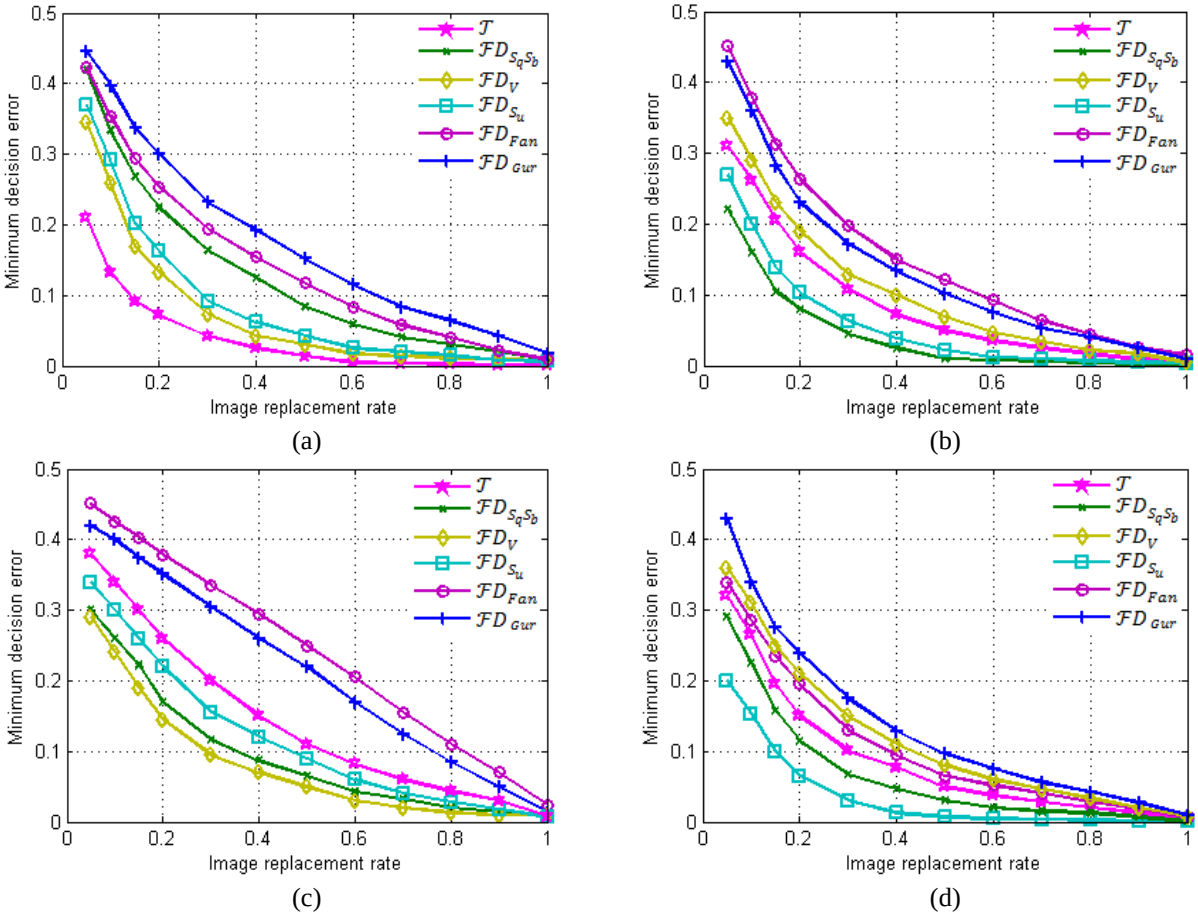
Figure 5.7: Testing on various types of forgeries, the minimum decision error is obtained using different QF_2 values against (a) A-DJPG detector, (b) Proposed scheme K_{MTPM} on UCID dataset.

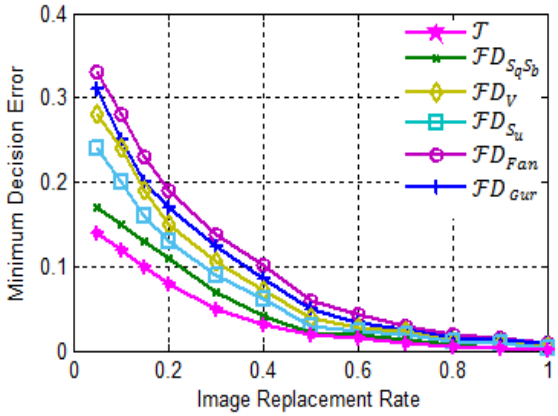
In comparison to [146], the proposed JPEG forensic strategy was tested against a number of well-known anti-forensic techniques, offers lower values of minimal decision error as shown in

Figure 5.7. In terms of minimum decision error, the proposed forensic methodology outperformed previous methods. It is important to note that forensic approaches with lower minimum decision error values are more successful.

5.2.3 Experiment Results Obtained on Bossbase Dataset

Performance analysis on the BOSSBase image dataset [137] is used to further validate the proposed forensic approach. On the BOSSBase dataset, P_e for different anti-forensic approaches are shown in Figure 5.8. using varying image replacement rates versus SVM-based detectors K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686}, K_{SRM}^{S714}, and K_{MTPM}.





(e)

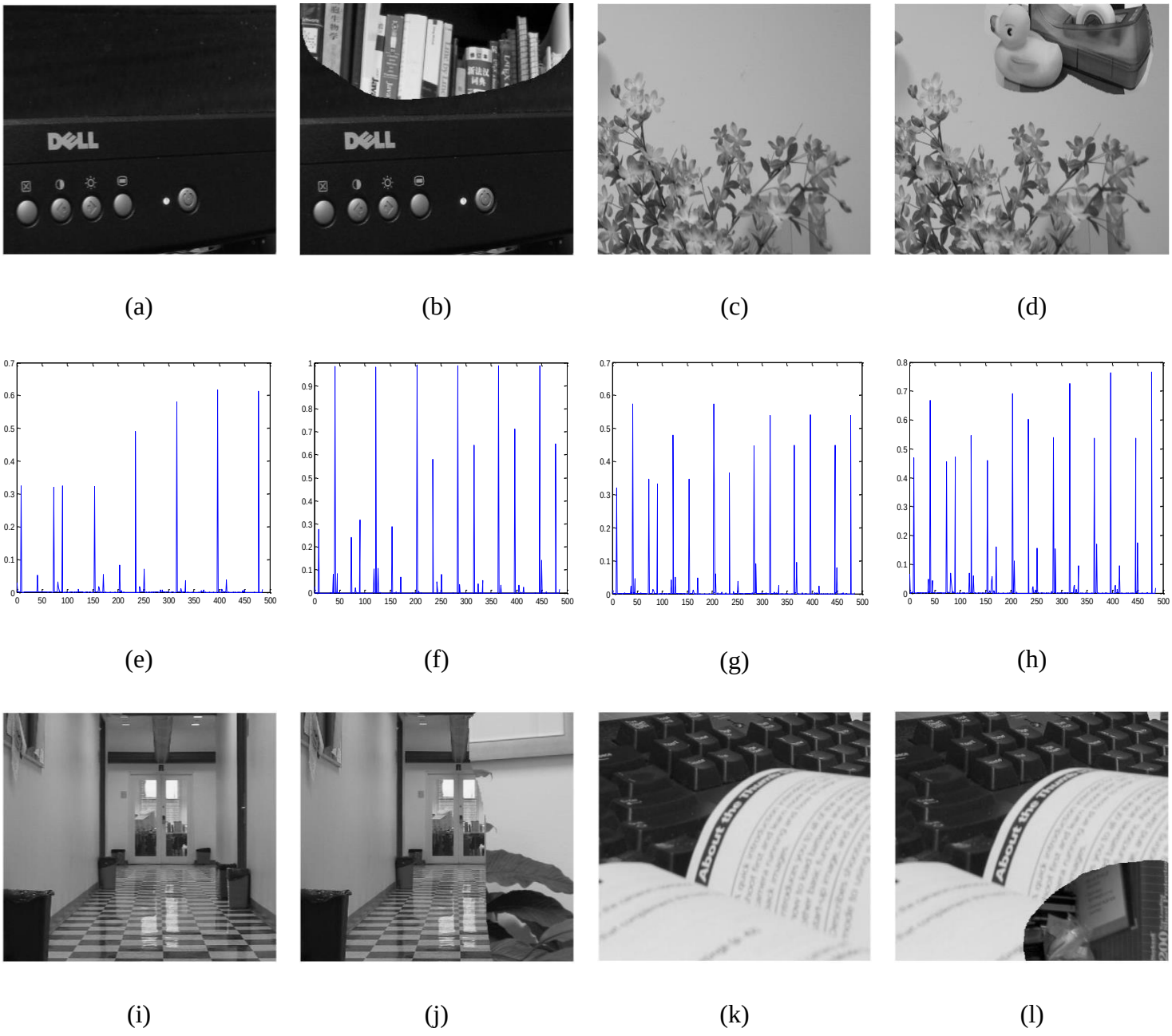
Figure 5.8: Using SVM-based detectors trained on the Bossbase dataset, by considering different image replacement rates against different forgeries, we calculated the minimum decision error. On the Bossbase dataset, the results are obtained. (a) K_{Li}^{S100} [122], (b) K_{SPAM}^{S686} [145], (c) K_{AR}^{S10} [128], (d) K_{SRM}^{S714} [130], (e) Proposed (K_{MTPM}).

The suggested forensic technique (K_{MTPM}) based on statistical analysis of second order improves outcomes in the detection of all the considered JPEG anti-forensic techniques by providing smaller minimum decision error values. The outcomes attained on the UCID database are fairly comparable to the findings attained on the BOSSBase database, as shown in Figure 5.5 and Figure 5.8. In addition, the dimensionality curse is less likely to affect SVM classifiers [154]. As a result, the SVM classifier's performance is less affected by the number of images in the dataset. Furthermore, it's worth noting that BOSSBase dataset's minimum decision error values are very identical to those of the UCID dataset images.

5.3 Evaluation of proposed scheme on spliced images

The majority of image splicing methods are optimization-based, with the goal of determining the optimum mapping to recover the statistics of original image. The inconsistencies near the edges in spliced images, there is a difference in the intensity level. There is a relation between the spliced and original parts because of these inconsistencies. The spliced and genuine images may be distinguished using this relationship. These inconsistencies in the altered images may be assessed using the proposed method, which is based on second-order statistical analysis. Figure 5.9 depicts the monodimensional signal for several spliced and original images. The analysis of signal $\delta(n)$ in Figure 5.9 reveals that an authentic image has smooth behaviour, whereas a spliced image with splicing technique has oscillating behaviour, as illustrated in Figure 5.9 (f),

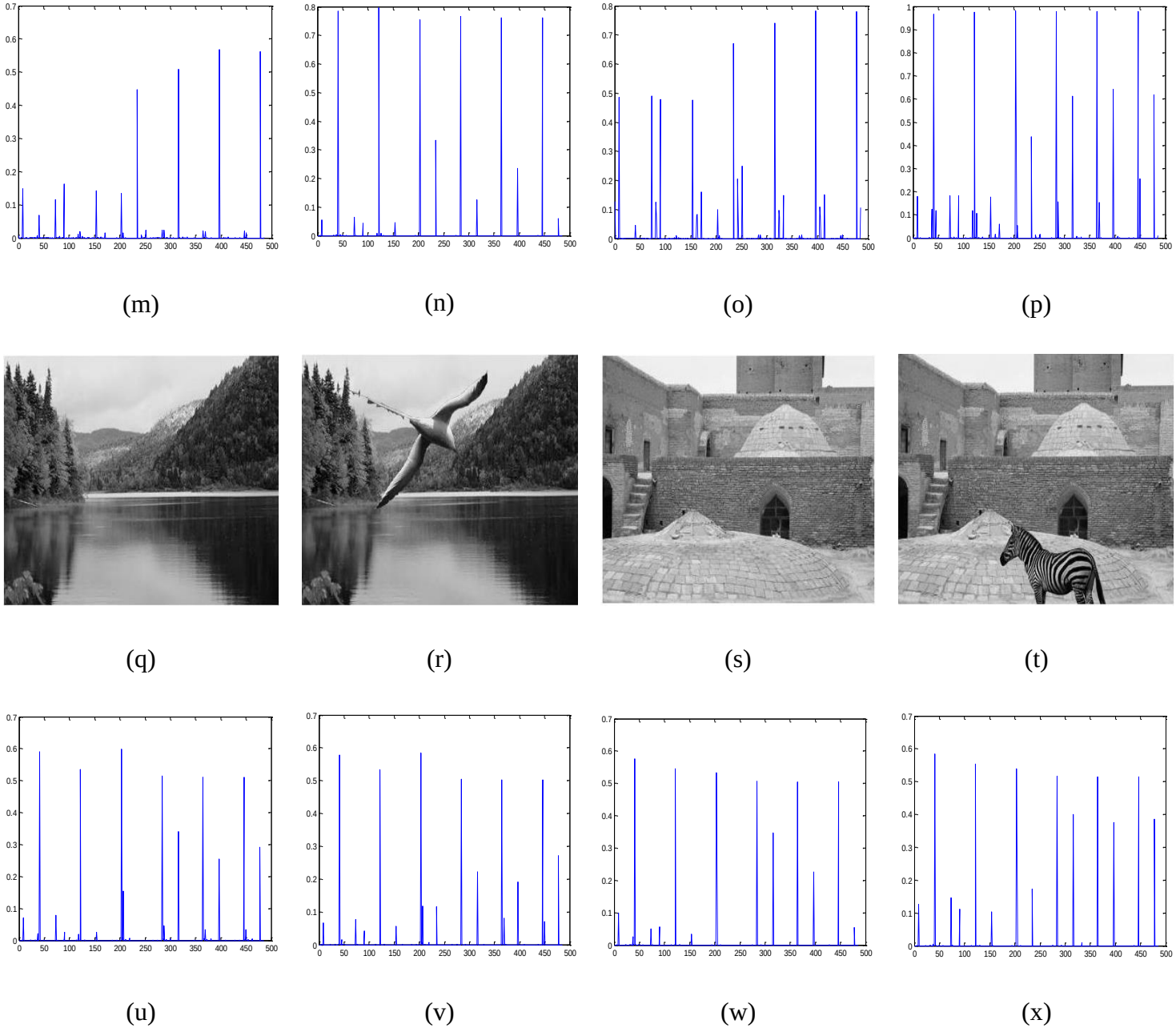
(h), (n), (p), (v), and (x). Figure 5.9 further illustrates that between authentic and spliced images, the oscillations of the mono-dimensional signal $\delta(n)$ are obviously different. As a result, it is evident that the suggested feature can efficiently recognize spliced images.



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

(e) (f) (g) (h)

(i) (j) (k) (l)



(m) (n) (o) (p)

(q) (r) (s) (t)

(u) (v) (w) (x)

Figure 5.9: Uncompressed authenticate images are denoted by (a), (c), (i), (k), (q), (s), while the spliced images are denoted by (b), (d), (j), (l), (r), (t). The resultant signals $\delta(n)$ for the uncompressed authenticate and spliced images are (e), (g), (m), (o), (u), (w) and (f), (h), (n), (p), (v), (x), respectively.

5.3.1 Experiment Results Obtained on CASIA v1.0 and Columbia Datasets

Several experiments using standard datasets including CASIA v1.0 [139] and the Columbia database [140] are conducted are used to evaluate the suggested forensic approach. The CASIA dataset contains 800 authentic photos and 921 altered images, which can be used to detect manipulation [139]. There are 363 photos in total in the Columbia dataset, which are in BMP and TIFF formats, of which 183 are genuine and the rest are manipulated [140]. However, in both datasets, the number of altered images is higher than the number of genuine images. As a result, a random selection of images is used for detection in order to achieve a balance between genuine and manipulated photos. 70% of the images in the proposed study are utilized for training, while 30% are utilized for testing. The performance of the classifier concerning the testing data is summarized by a confusion matrix.

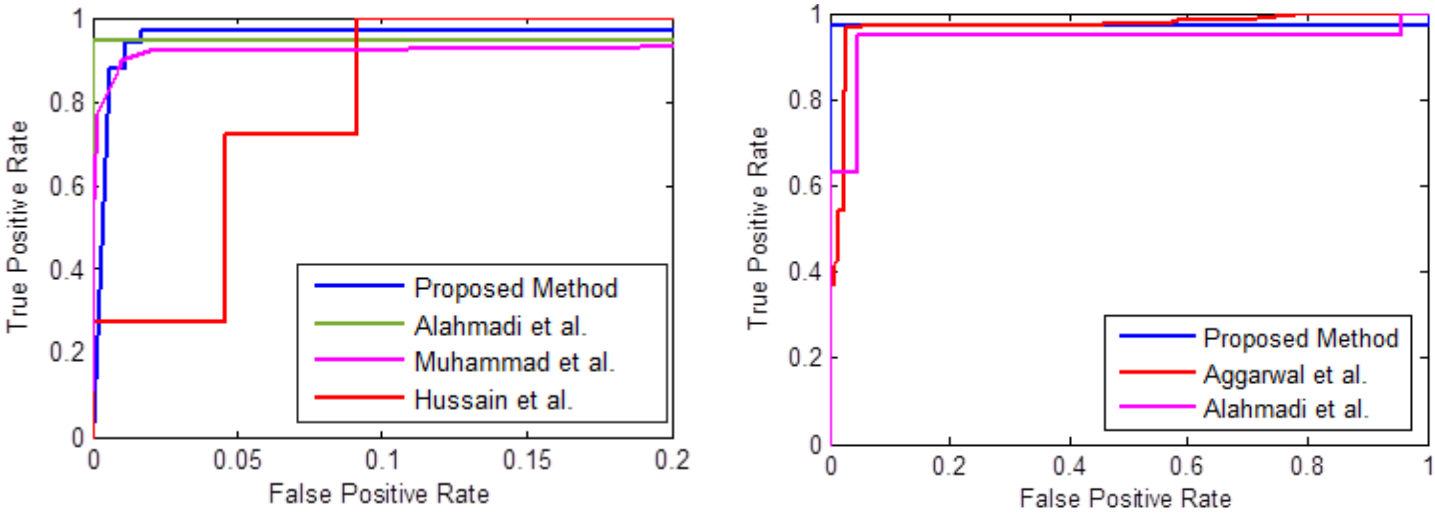
Table-5.1: Confusion matrices for the respective datasets.

CASIA v1.0	**Predicted Negative**	**Predicted Positive**
Actual Negative	236	4
Actual Positive	2	238

Columbia	**Predicted Negative**	**Predicted Positive**
Actual Negative	53	1
Actual Positive	1	53

For example, the CASIA v1.0 dataset has 800 genuine and 921 altered images. To maintain the balance, the experimentation includes 800 authentic and 800 manipulated images, for a total of 1600 images in CASIA v1.0. The classifier is trained with 1120 images and tested with 480 images, according to the 70:30 training and testing proportions. Similarly, the Columbia dataset is utilized to train the classifier, with 252 images used for training and 108 pictures used for testing. Hence, the confusion matrix is formed on the basis of 480 and 108 images to envisage the accuracy of the classifier by relating actual and predicted classes. The confusion matrix for both the CASIA v1.0 and Columbia datasets can be seen in Table 5.1.

The effectiveness of the suggested strategy is further proven using the ROC curve, by taking into account a variety of existing strategies [158 – 162]. The ROC curve depicts the classification system performance. The suggested scheme maximum performance is depicted by the ROC curve towards the upper left corner. Figure 5.10 (a) shows the curves of ROC for the CASIA v1.0 compared with [158 – 160] and Figure 5.10 (b) shows the comparison of ROC curves for the Columbia dataset with [161 – 162].



(a) (b)

Figure 5.10: ROC curves for various approaches assessed on (a) CASIA v1.0 dataset and (b) Columbia dataset.

Figure 5.10 (a) and (b) show that for the suggested approach the ROC curve is closer to the upper left corner, indicating that it is more accurate than previous methodologies. Furthermore, the experimental findings show that statistical feature of second-order derived from MTPM surpasses previous approaches in both the intra-block and inter-block DCT domains. On the CASIA v1.0 and Columbia datasets, the accuracy was 98.75% and 98.15%, respectively. As a result, the suggested approach effectively distinguishes between genuine and spliced photos.

Table-5.2: Run time analysis of the proposed technique on both datasets.

Datasets	Image Size	Total number of images	Running Time (secs/image)
CASIA v1.0	**384×256**	1721	0.438
Columbia	**757×568 to 1152×768**	363	2.364 to 2.839

Moreover, majority of methods do not implement run-time analysis, as they, are not robust against post-processing operations. Instead, as demonstrated in Table 5.2, by confirming performance through run-time analysis, the proposed technique avoids these limitations.

5.4 Summary

In this chapter, by taking into account second-order statistical analysis based on MTPMs, a counter JPEG anti-forensic technique is implemented. The suggested feature can identify grainy noise caused by anti-forensic methods dithering operation. Extensive experimental study has proven the capabilities of the suggested forensic approach. Experiments demonstrate that the presented methodology outperforms existing strategies in countering various techniques by lowering the minimum decision error values. 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

EXPOSING JPEG COMPRESSION FOOTPRINTS USING SECOND ORDER STATISTICAL ANALYSIS

In this chapter, the counter JPEG anti-forensic method presented in last chapter is further examined to improve its capability in the detection of numerous anti-forensic attacks. The second-order Markov Transition Probability Matrices (MTPMs) statistics are used to model the underlying intra-block and inter-block dependencies of JPEG quantized DFrCT coefficients. The DFrCT approach utilizes a fractional parameter to the suggested method to increase its efficiency. Moreover, the experimental results illustrate that the proposed technique outperforms numerous existing methods.

6.1 Detection approach for JPEG compression Anti-Forensics

Majority of current compression detection methods depend on the image histogram to examine first-order statistics. Anti-forensic methods may effectively confuse these detection techniques. Subsequently, a statistical analysis of higher-order is needed to evaluate this issue. The MTPM is the subject of statistical investigation of second-order as shown in Figure 6.1. It is significant that when the images are transformed from spatial domain to frequency domain with DFrCT transformation, the correlation between the adjacent coefficients within the DFrCT block is noticeable. Moreover, there is a strong correlation between the adjacent block DFrCT coefficients. Furthermore, the difference in DFrCT coefficients obtained from the same locations in neighbouring DFrCT blocks has a direct effect on the pixels comparison, while the quantization loss is ignored. Despite the fact that loss due to quantization is expected to be irreversible, it has an effect on the dependency. Thus, the dependency and loss due to quantization are expressed in this way because of the correlation between same locations in adjacent blocks of DFrCT. On account of this information, to expose these dependencies the frequency domain features of the inter and intra-block are extracted. As shown in Figure 6.1, there are three stages of the proposed approach which incorporates: target difference image selection, assessment of (MTPMs) in DFrCT domain, and generation of mono-dimensional

signal. Furthermore, to distinguish between compressed and uncompressed JPEG images, an SVM classifier is utilized for classification.

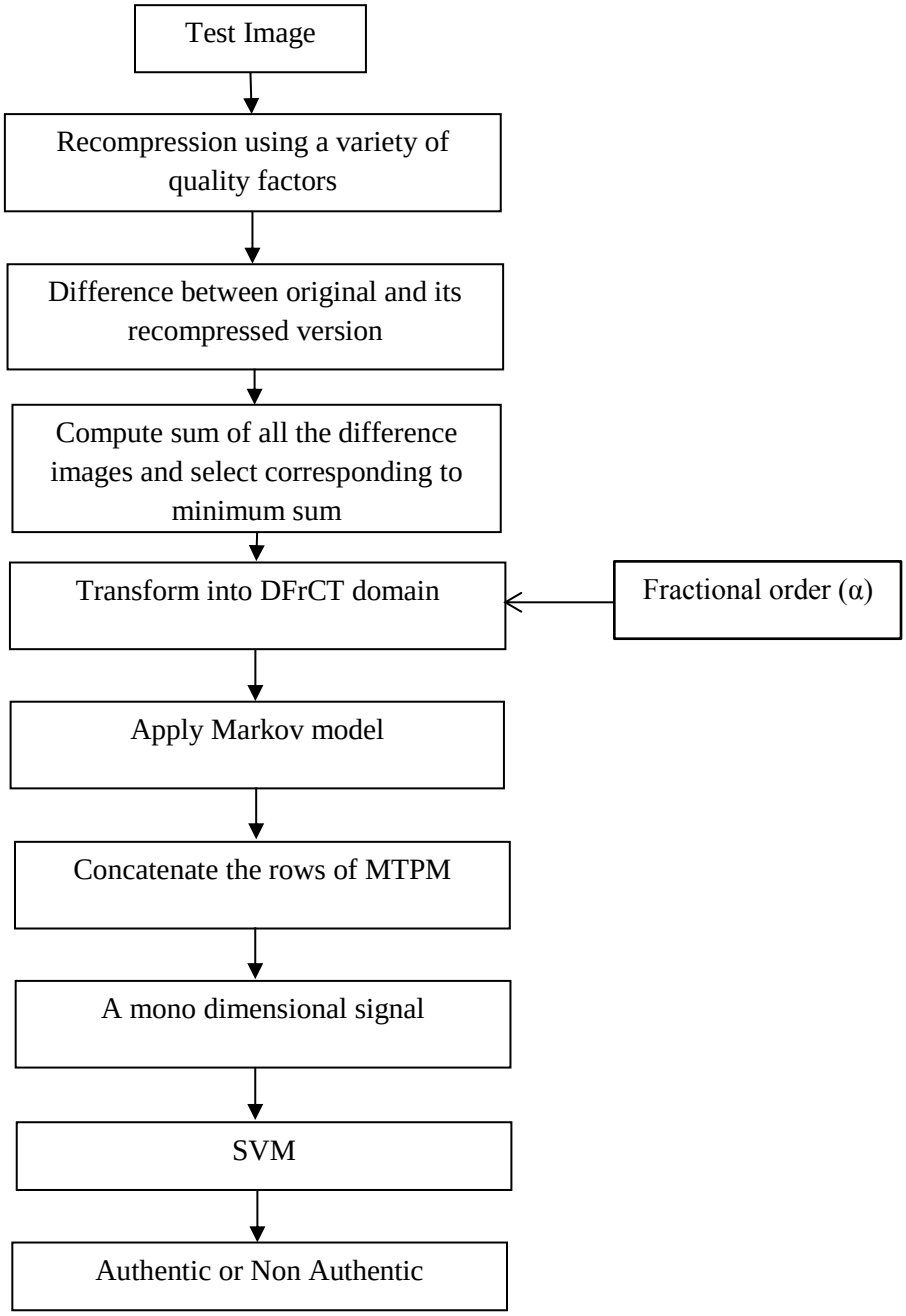


Figure 6.1: Sketch of the proposed algorithm.

6.1.1 Generation of mono-dimensional signal based on MTPMs in DFrCT domain

This section investigates the anti-forensic techniques effect on MTPMs. The majority of anti-forensic approaches are rely on optimization techniques that aim to determine the best mapping for recovering of the uncompressed original image statistics. This method involves shifting of pixels from one bin to another on the basis of maximum pixel distortion. Such anti-forensic attacks are capable of totally erasing the gaps present in the JPEG compressed image histogram. Despite the fact that the images histograms are identical whether they are uncompressed or anti-forensically processed but the MTPMs still shows traces. We are searching for an MTPM-derived second-order statistical feature which can effectively distinguish between the uncompressed and anti-forensically processed images.

Uncompressed Lena image

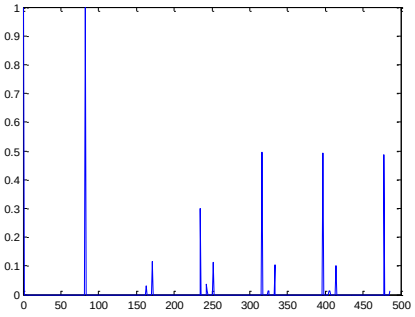
(a)

Image of Lena compressed in JPEG format with a quality of 50

(b)

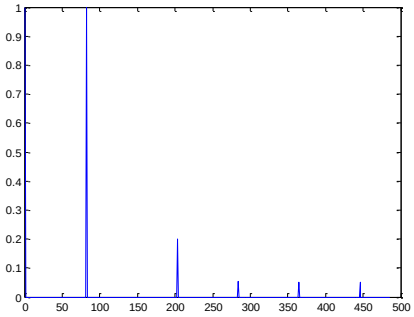
At a quality factor of 50, JPEG forgery ($\mathcal{FD}_{Fan}$)

(c)



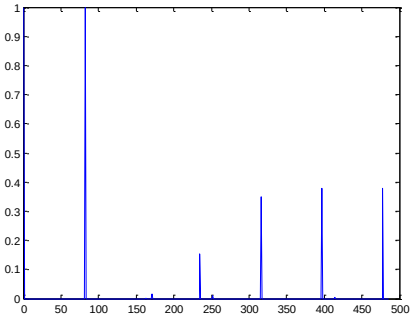
$\delta(n)$ for Lena uncompressed image

(d)



$\delta(n)$for Lena image encoded in JPEG with a quality of 50

(e)



$\delta(n)$ at 50 quality factor for Lena JPEG forgery ($\mathcal{FD}_{Fan}$).

(f)

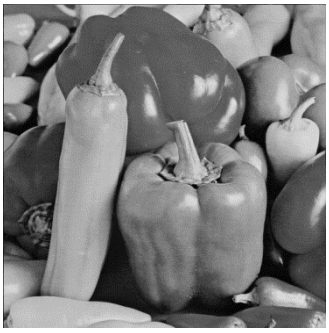


Image of Peppers uncompressed

(g)

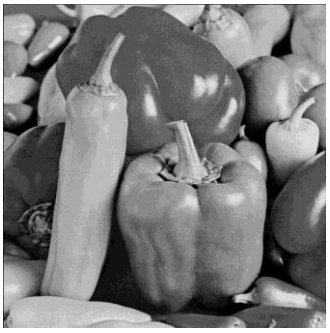
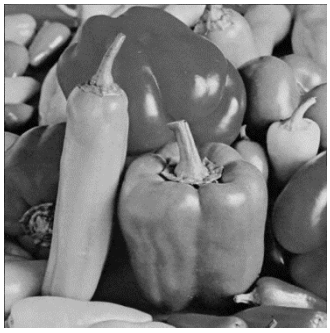


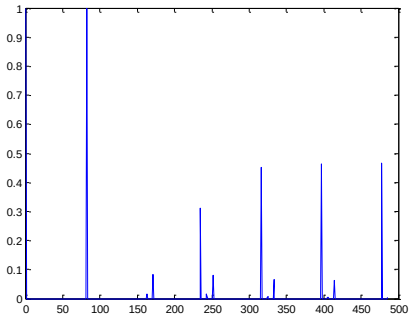
Image of peppers compressed in JPEG format with a quality of 50

(h)



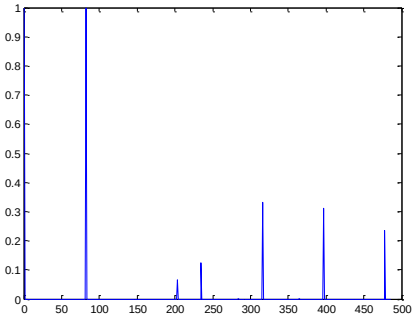
At a quality factor of 50, JPEG forgery ($\mathcal{FD}_{Fan}$)

(i)



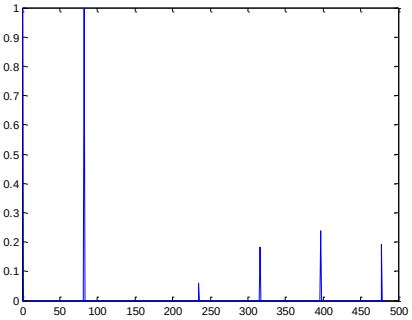
$\delta(n)$ for Peppers uncompressed image

(j)



$\delta(n)$for Peppers image encoded in JPEG with a quality of 50

(k)



$\delta(n)$ at 50 quality factor for Peppers JPEG forgery ($\mathcal{FD}_{Fan}$).

(l)

Figure 6.2: Uncompressed, JPEG compressed, and anti-forensically processed images of Lena and Peppers are revealed by (a), (b), (c), and (g), (h), (i) respectively. $\delta(n)$ for (a), (b), (c), and (g), (h), (i) are revealed by (d), (e), (f), and (j), (k), (l), respectively.

A mono-dimensional signal is obtained by analysing several properties depending on the MTPM of the considered image. Concatenation of the rows of intra-block and inter-block MTPMs yields this signal. Dithering artifacts occur while processing the image anti-forensically, according to the study. Let $\delta(n)$ denote a mono-dimensional signal based on MTPMs with a size of (1, 648). According to signal $\delta(n)$, a smooth behavior is revealed by an uncompressed image while a JPEG compressed image and an image modified using anti-forensics exhibit oscillatory behaviour, as shown in Figure 6.2. Figure 6.2 (e) and Figure 6.2 (k) reveal that oscillations in JPEG compressed images are higher than in images processed with anti-forensics, as illustrated in Figure 6.2 (f) and Figure 6.2 (l), respectively. It is due to the employment of anti-forensic methods for hiding artifacts of JPEG compression so as to trick the detectors used in forensic investigation. However, this feature is effective at recognising the JPEG images that are altered anti-forensically.

6.2 Experimental Results

This section evaluates the suggested counter JPEG anti-forensic scheme performance against different types of anti-forensic schemes and several comparisons are made to validate its authenticity.

6.2.1 Evaluation of proposed approach by considering SVM-based forensic detectors

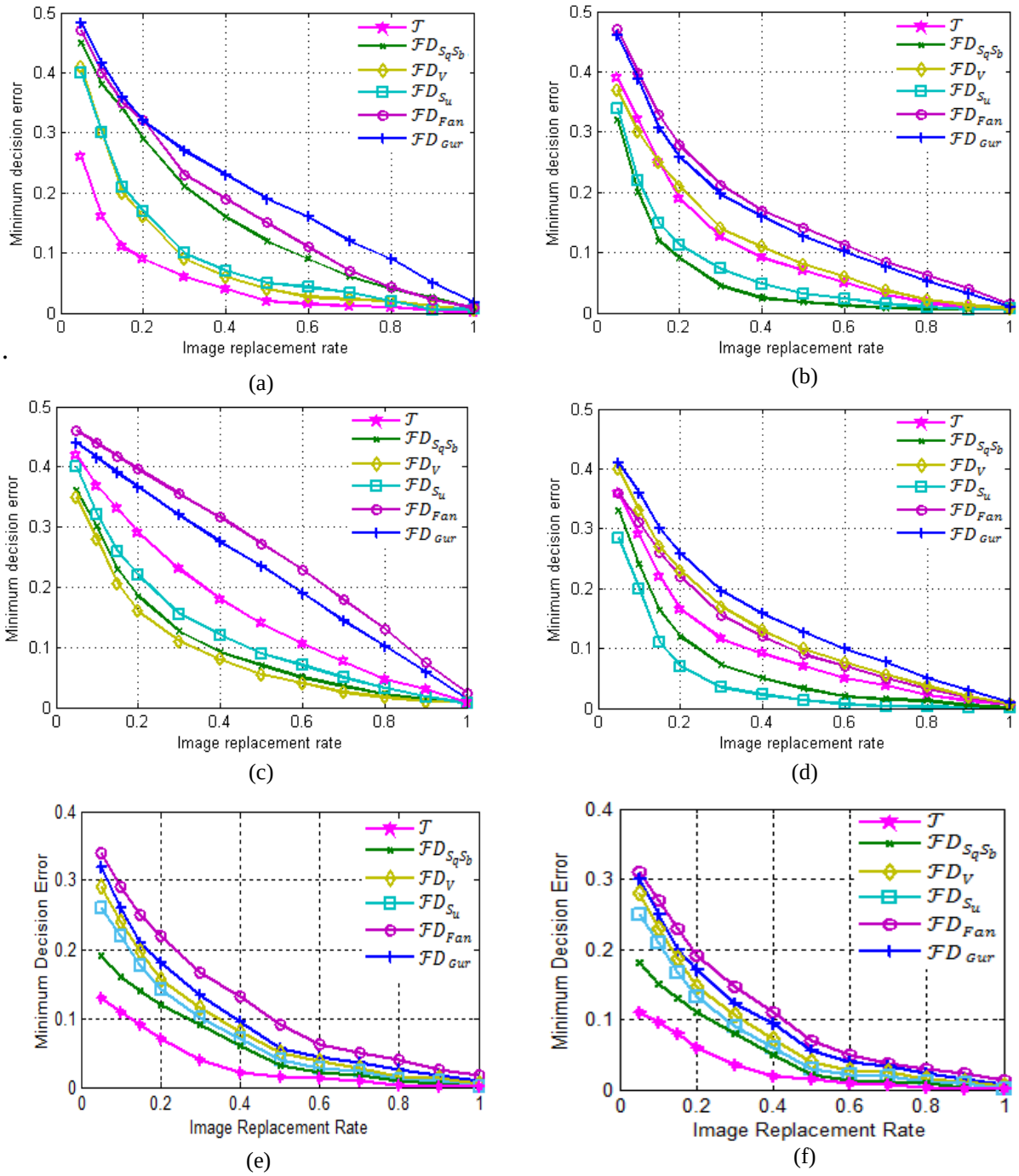
As shown in Fig. 1, there are three stages of the proposed approach which incorporates: target difference image selection, assessment of (MTPMs) in the DFrCT domain, and in third stage mono-dimensional signal generation. To categorize between JPEG compressed and original images, the SVM classifier is fed with the generated mono-dimensional signal. The proposed methodology is evaluated by using the minimum decision error (P_e) as an evaluation metric. When comparing the output of forgeries, the minimum decision error (P_e) is used as an assessment parameter against various forensic detectors in steganalysis approaches [153], [156]. ROC curves for various JPEG forensic detectors are first calculated using negative and positive cases. Negative cases are pictures that are authentic and uncompressed, whereas the positive cases are JPEG (anti-forensic) images. However, the anti-forensic technique's dithering operation in the spatial domain generates an artificial or grainy noise. Even after using JPEG anti-forensic methods, aim of the presented approach is to find compression footprints.

It is believed that the forensic analyst is familiar with both anti-forensic and forensic methodologies and in the case of SVM-based detectors, a sequence of forged images can be used to train the detector. For anti-forensic procedures, this is the worst-case scenario. SVM-based detectors are widely used such as K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} can effectively defeat JPEG anti-forensic techniques. Anti-forensic techniques have a difficult time fooling detectors based on machine learning [157]. For anti-forensic techniques, this is the worst-case scenario, However, it's perfect for forensic techniques. In steganalysis, detectors based on SVM such as K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686} and K_{SRM}^{S714} have very low values of minimum decision error and good detection accuracy. By constructing JPEG forgeries with replacement procedure, the performance of the suggested methodology K_{MTPM} is evaluated. With a substitution rate varying from 0.05 to 1, the center portion of a certain image in uncompressed format is replaced with processed image using JPEG anti-forensics. The forensic examination is carried out using

uncompressed and processed images both. LIBSVM [133] with a Gaussian kernel is used to train the SVM classifier. SVM parameters are determined using a multiplicative grid and five-fold cross-validation [145].

6.2.1.1 Experimental results obtained on UCID dataset

Uncompressed images and with corresponding anti-forensic counterparts are used to train SVM classifiers in this section. For forensic testing, these classifiers use the images provided by the UCIDTest. Figure 6.3 depicts the values of minimum decision error for several anti-forensic methods based on image replacement rate. The suggested methodology K_{MTPM} has outperformed (a) K_{Li}^{S100}, (b) K_{SPAM}^{S686}, (c) K_{AR}^{S10} and (d) K_{SRM}^{S714} by providing lower minimum decision error values versus several approaches of anti-forensics, as revealed in Figure 6.3 (e) and (f). With a step size of 0.01 'a' is changed from zero to one throughout the investigation. For all of the images analysed, the proposed technique produces good results with fractional parameter 'a' ranging from 0.9 to 0.99. However, when the value of fractional parameter is 0.97, the best outcomes are attained. The effectiveness of the proposed technique is further investigated through a comparison of DCT and DFrCT based forensic approaches. DFrCT provides an additional parameter $\alpha = a\pi/2$ in which 'a' varies from zero to one. In forensic undetectability terms, the techniques $\mathcal{FD}_{Fan}$ and $\mathcal{FD}_{Gur}$ exceed the other anti-forensic techniques. This is because JPEG forgeries are created using explicit DCT histogram smoothing in JPEG anti-forensic approaches [47] and [152]. This smoothing causes the image statistics to change even more. When the replacement rate is 0.10, the anti-forensic approach provided in [142] yields a high minimum decision error for existing SVM-based detectors. As a result, creating a forgery is as simple as exchanging a 112×160 block size for a UCID dataset image of size 384×512. The forger will produce a number of forgeries by substituting the 112×160 block. For example, in the image the forger will easily substitute the head of one individual. When attempting to make an entire JPEG image appear uncompressed, anti-forensic techniques have a difficult time in fooling machine learning detectors. When compared to other techniques, the value of minimum decision error for $\mathcal{FD}_{Gur}, \mathcal{FD}_{v}, \mathcal{FD}_{Fan}$ is quite high. This is due to the explicit smoothing of the histogram. It's worth mentioning that a greater minimum decision error value indicates lower forensic detectability. Smaller minimum decision error values indicate improved forensic detection.

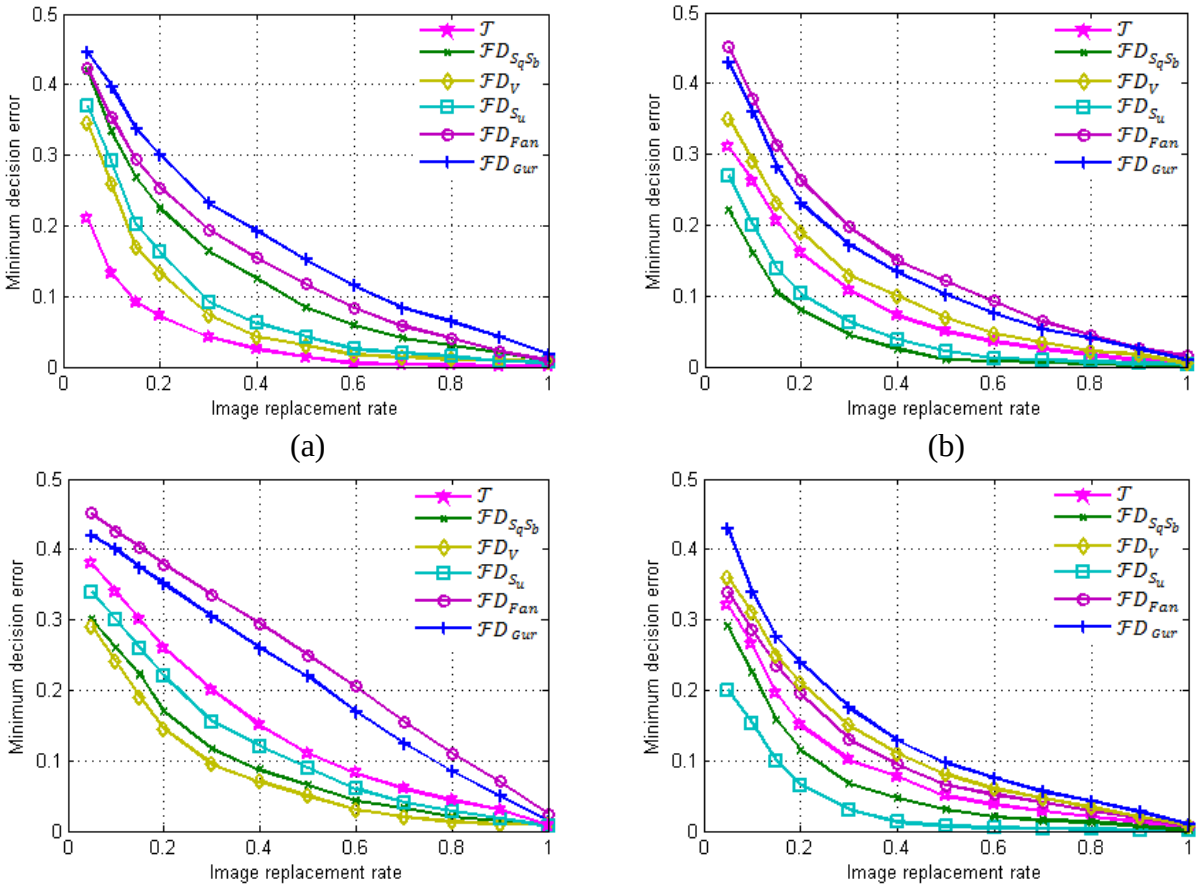


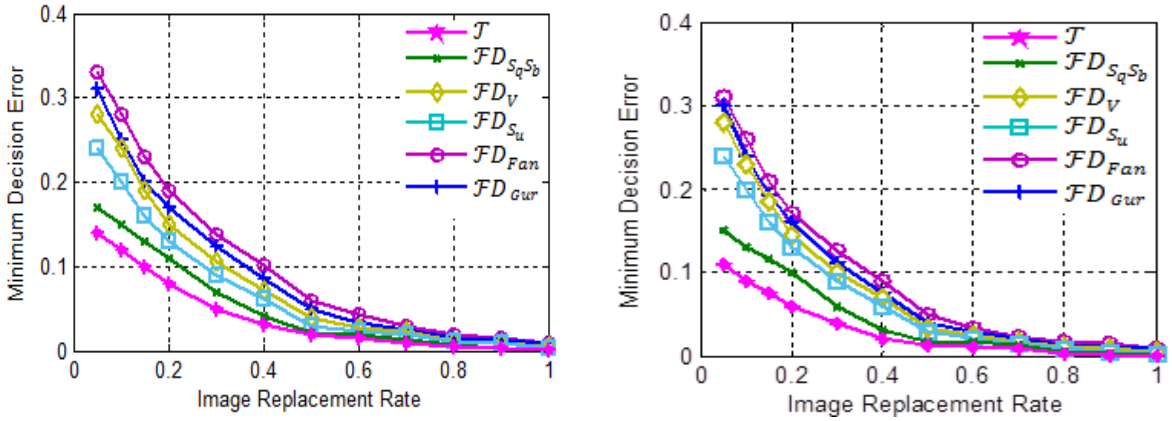
(a) (b) (c) (d) (e) (f)

Figure 6.3: Using SVM-based detectors trained on the UCIDTrain dataset, using different image replacement rates against different forgeries, we calculated the minimum decision error. On the UCIDTest dataset, the results are obtained. (a) K_{Li}^{S100} [122], (b) K_{SPAM}^{S686} [145], (c) K_{AR}^{S10} [128], (d) K_{SRM}^{S714} [130], (e) Proposed (K_{MTPM}) at 'a' $= 1$, (f) Proposed (K_{MTPM}) at 'a' $= 0.97$.

6.2.1.2 BOSSBase dataset based experimental results

In this section, performance analysis on the BOSSBase image dataset [137] is used to further validate the proposed forensic approach. BOSSBase dataset original raw images are transformed into 8-bit grayscale PGM images using the UFRaw utility after being converted into PPM format. For forensic testing, each original high-resolution grayscale BOSSBase image is cropped into a sub-image of 512×512. To test detectors base on SVM from the BOSSBase image database, we selected 5000 test images and the remaining images as training images. Afterwards, these images are treated using a variety of anti-forensic approaches to provide datasets of processed images for evaluation. The BOSSBase image testing and training datasets have been prepared using the same technique as used for UCID images. On the BOSSBase dataset, the values of minimum decision error for several JPEG anti-forensic approaches using various image substitution rates against K_{Li}^{S100}, K_{AR}^{S10}, K_{SPAM}^{S686}, K_{SRM}^{S714}, and K_{MTPM} detectors are seen in Figure 6.4.





(e) (f)

Figure 6.4: Using SVM-based detectors trained on the Bossbase dataset, using different image replacement rates against different forgeries, we calculated the minimum decision error. On the Bossbase dataset, the results are obtained. (a) K_{Li}^{S100} [122], (b) K_{SPAM}^{S686} [145], (c) K_{AR}^{S10}[128], (d) K_{SRM}^{S714} [130], (e) Proposed (K_{MTPM}) at 'a' $= 1$, (f) Proposed (K_{MTPM}) at 'a' $= 0.97$.

The suggested forensic technique (K_{MTPM}) based on statistical analysis of second order improves outcomes in the identification of the JPEG anti-forensic approaches by providing lower P_e values. The outcomes attained on the UCID database are fairly comparable to the findings attained on the BOSSBase database, as shown in Figure 6.3 and Figure 6.4. The proposed forensic method objective is to discriminate among uncompressed and images which are processed anti-forensically. The fractional parameter of DFrCT is modified in steps of 0.01 from 0 to 1, throughout the investigation. For all of the images analysed, the proposed technique produces good results with values of fractional parameter ranging from 0.9 to 0.99. However, where the 'a' is 0.97, the best results are achieved. In addition, the dimensionality curse is less likely to affect SVM classifier [154]. As a result, the SVM classifier performance is less affected by the number of images in the dataset. Furthermore, the BOSSBase dataset minimum decision error values are very identical to those of the UCID dataset images.

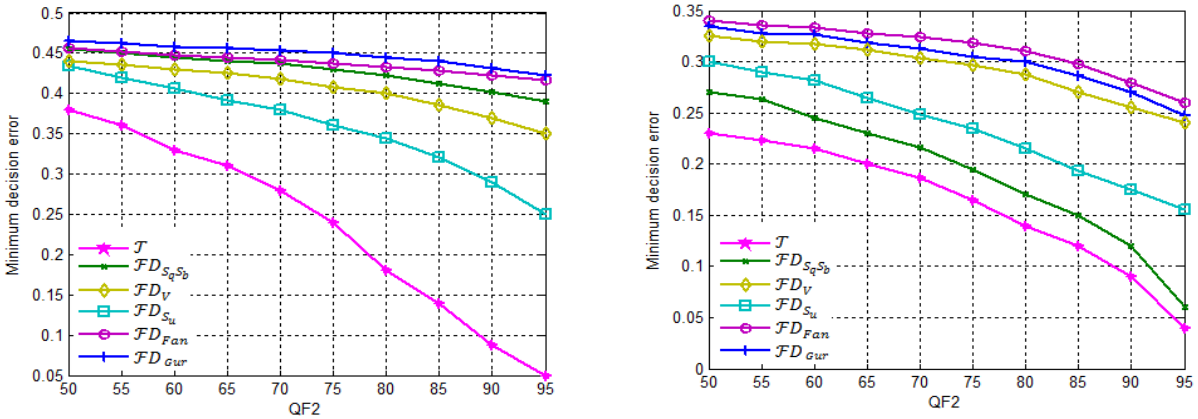
6.2.2 Performance analysis of double JPEG compression

The proposed forensic technique was tested on anti-forensically processed images that were double JPEG compressed to further confirm its viability. The effectiveness of the presented forensic method and as well as the forensic detectors [109] and [146] is computed using various anti-forensic schemes.

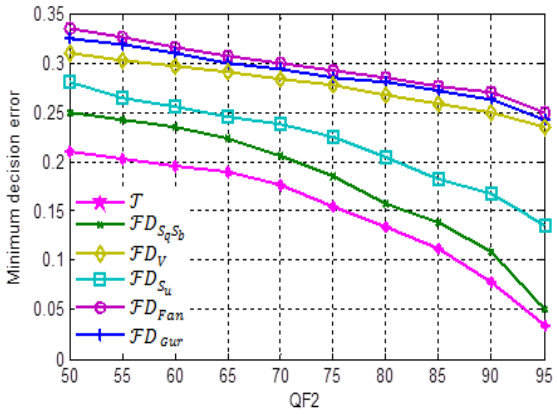
6.2.2.1 Evaluation on Non-aligned JPEG compressed images

Images are compressed twice in double JPEG compression, first with QF_1 and then with QF_2. During double JPEG compression, image cropping and content changes are possible. On JPEG images compressed with quality factor QF_1, current anti-forensic approaches are used. According to the testing conditions, after using the anti-forensic process, the forged JPEG image can be left unused or cropped using a random grid change. Finally, by compressing resultant image with QF_2, double JPEG compressed anti-forensic image is obtained.

The average of minimum decision error with different QF_2 values is shown in Figure 6.5 against various types of forgeries. When checked against the NA-DJPG detector, due to explicit histogram smoothing, the anti-forensic approaches $\mathcal{FD}_{Gur}$ and $\mathcal{FD}_{Fan}$ demonstrate strong forensic undetectability [109]. The anti-forensic approach $\mathcal{FD}_{Fan}$ proposed in [47] successfully fools the majority of current JPEG forensic detectors. With a value (approx.) 0.5 of minimum decision error, $\mathcal{FD}_{Fan}$ effectively fools the NA-DJPG detector [109]. The suggested forensic methodology will also reveal gaps in the DFrCT domain that are only partly filled. For various quality factor QF_2 values, the proposed forensic technique (K_{MTPM}), as shown in Figure 6.5, offers lower minimum decision error values. This demonstrates that the suggested method outperforms the current double compression forensic method [109] against a variety of anti-forensic methods.



(a) (b)



(c)

Figure 6.5: Testing on various types of forgeries by evaluating minimum decision error for different QF_2 values against (a) NA-DJPG detector, (b) Proposed scheme K_{MTPM} at 'a' $= 1$ and (c) Proposed scheme K_{MTPM} at 'a' $= 0.98$, on UCID dataset.

6.2.2.2 Evaluation on Aligned JPEG compressed images

Images from the UCIDTrain dataset were compressed to create the A-DJPG compressed images dataset with quality factor QF_1 and then compressing them again with QF_2, such as $QF_1 \neq QF_2$. In comparison to [146], the introduced JPEG forensic approach offers lower P_e values against several existing anti-forensic methods, as shown in Figure 6.6. The DFrCT fractional parameter is modified in steps of 0.01 from 0 to 1 in this entire analysis of the proposed technique. For all of the images considered, the proposed method produces good results with 'a' ranging from 0.9 to 0.99. However, whether it comes to JPEG compressed images that are aligned and non-aligned, the best results are obtained at fractional orders of and 0.97 and 0.98, respectively. In terms of minimum decision error, the proposed forensic methodology outperformed previous methods. It is important to note that forensic techniques with lower minimum decision error values are more effective.

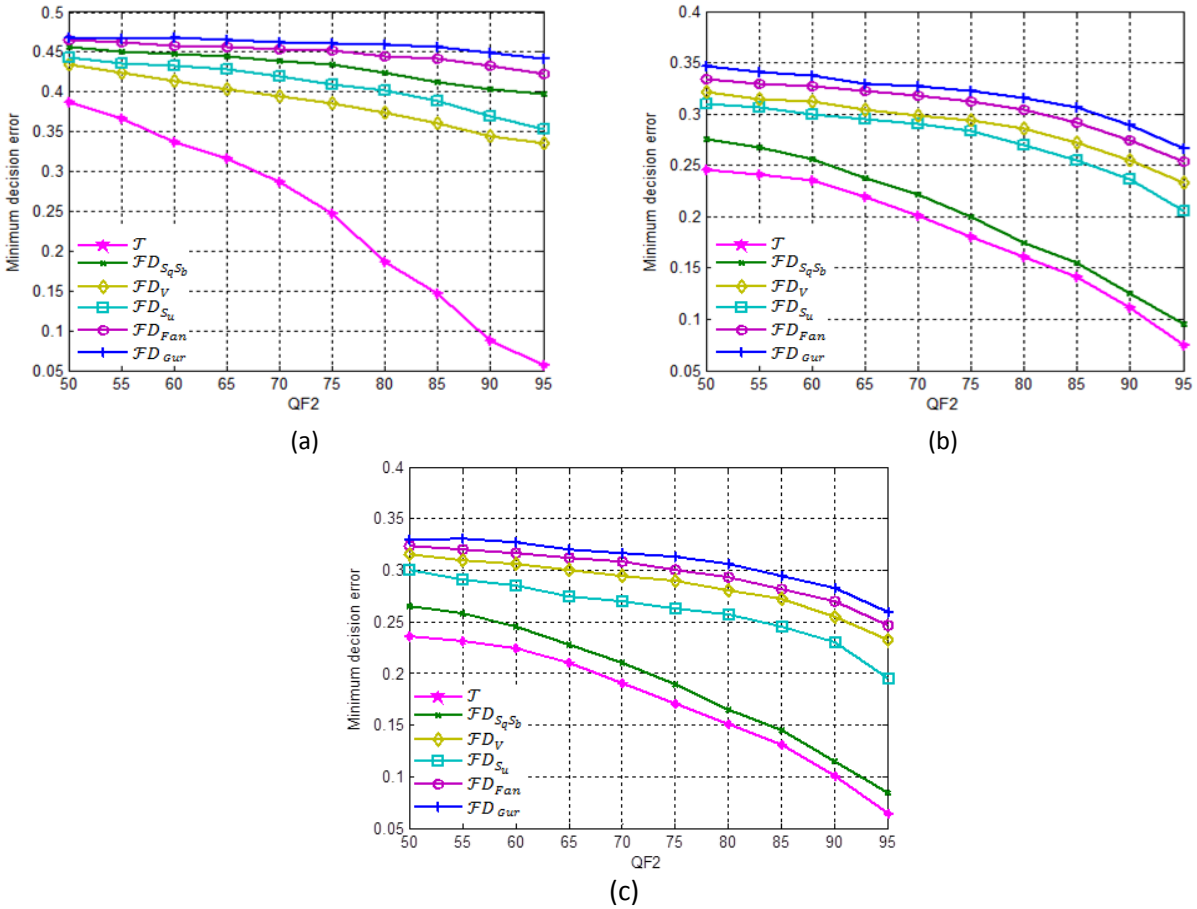


Figure 6.6: Testing on various types of forgeries, the minimum decision error is obtained using different QF_2 values against (a) A-DJPG detector, (b) proposed scheme K_{MTPM} at 'α' $= 1$ and (c) proposed scheme K_{MTPM} at 'α' $= 0.97$, on UCIDTest dataset.

6.3 Summary

By using anti-forensic methods, forensic detectors on the basis of first-order statistical analysis can easily mislead. To address these anti-forensic techniques, a statistical analysis of higher-order is necessary. The JPEG forensic methodology is described in this chapter, which can expose compression artifacts in the DFrCT domain. The proposed approach which is the combination of MTPM and DFrCT, conducted a statistical analysis of higher-order to detect the footprints produced by various anti-forensic methods. The proposed method also has the benefit of providing variable parameter "α" of DFrCT to improve its flexibility. When compared to current techniques, the proposed forensic technique potential is validated by comprehensive experimental results.

CHAPTER 7

CONCLUSIONS AND FUTURE SCOPE

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

7.1 Conclusions

JPEG is a widely used compression format in various cameras and image processing softwares. The presence of digital images in an inappropriate manner on social networking sites inspires the researchers to work for the enhancement of forensic investigation methods in order to determine the validity of digital images. On the other hand, expert anti-forensic strategies are required to challenge and aid in the advancement of forensic procedures. As a result, a JPEG anti-forensic technique is developed, which conceals compression artifacts in the DCT domain and thereby deceives forensic detectors. The use of a shifted block DCT technique allowed the employment of a non-adaptive dithering model to introduce dithering noise. In the second stage, the outcome of this shifted block DCT technique is further processed using a TV-based deblocking technique to remove blocking artifacts left behind after JPEG compression in the spatial domain. The results show that the proposed strategy outperforms existing strategies with a very low computational cost

The further research is dedicated to design an enhanced JPEG anti-forensic technique to remove the blocking artifacts introduced by JPEG compression. Therefore, a methodology is provided that can trick forensic detectors rely on scalars and machine learning by concealing compression artifacts in the DFrCT domain. JPEG compression artifacts are well hidden by using the shifted block DFrCT method. The suggested approach benefits from the addition of a fractional parameter, which increases its flexibility for more improvement. Blocking artifacts are further reduced using TV-based deblocking. As a result, for optimization of the recommended approach, this strategy contains different variables for each considered image, such as fractional parameter

and shifted block. The proposed JPEG anti-forensic scheme provides enhanced image visual quality as compared to the existing approaches with high PSNR, SSIM values and better forensic undetectability on UCID and BOSSBase datasets. Moreover, as compared to state-of-the-art approaches, the suggested JPEG anti-forensic approaches provide a superior balance between image quality and forensic undetectability. Furthermore, the proposed methodology has raised an important question about the reliability and security of forensics methods.

The analysis of JPEG anti-forensics reveals the limitations of existing forensic detectors. Actually, the first-order statistical feature component analysis is the main focus of existing forensic work on JPEG compression detection. By using anti-forensic approaches, forensic detectors relying on first-order statistical analysis can be readily misled. To counter these anti-forensic tactics, it is necessary to do a statistical analysis of higher-order. To address this problem, this study provides a second-order statistical analysis-based counter JPEG anti-forensic method (MTPMs) in DCT and DFrCT domain. Selection of the target difference image, evaluation of MTPMs, and MTPMs are used to generate second-order statistical features are the three steps of the suggested framework. The impacts of JPEG anti-forensics dithering operation are investigated in the first step by examining variance inconsistencies along the diagonals. Following that, in the second step, MTPMs are examined to detect grainy noise added during dithering process. The final step is to create an optimum second-order statistical feature and feed it to the SVM classifier. The results based on UCID and BOSSBase databases, showed that the suggested MTPMs based forensic detector is quite effective even when anti-forensic attacks are present. Moreover, the multi-purpose nature of the proposed counter JPEG anti-forensic scheme is confirmed when evaluated on spliced images considering CASIA v1.0 and Columbia datasets. When compared to current approaches, the ability of the proposed forensic methodology is validated by thorough experimental research, which shows that it outperforms many anti-forensic methods in terms of detection. In this research work, some useful observations were made which will be very helpful to the researchers who wish to show the classification between original and modulated regions in the forged images.

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 anti-forensics and forensics:

- An anti-forensic framework for JPEG compression is proposed to disguise the existing scalar and SVM-based forensic detectors. When this framework is evaluated on UCID dataset, 98.58% of the images are classified as not JPEG compressed.
- Furthermore, an improved anti-forensic framework for JPEG compression based on DFrCT is proposed. When this framework is tested on the UCID dataset, it finds that 98.93% of the images are classified as not JPEG compressed.
- Moreover, the proposed approach efficiently hides the JPEG compression artifacts and provides better performance in comparison to the existing techniques in terms of image visual quality and forensic undetectability.
- A counter JPEG anti-forensic technique is proposed on the basis of Markov Transition Probability Matrices (MTPMs) based second order statistical analysis by revealing the artifacts introduced during the JPEG anti-forensics
- The proposed counter JPEG anti-forensic technique is explored in both DCT and DFrCT domain to find its applications in the detection of JPEG compression forensics. The proposed framework provides better detection results against various anti-forensic attacks when compared to the existing techniques in terms of lower minimum decision error values.

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 helpful to the researchers who wish to show the classification between pure and modulated regions in the forged images.

7.3 Future Scope

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

- A better restoration of DCT coefficients histogram can be achieved to make the presented JPEG anti-forensics framework more robust.
- In the future, a forensic technique that is robust against anti-forensic attacks can be developed based on the findings in the experimental results section.

- The presented counter JPEG anti-forensic technique can be further investigated to discover its applications for other image processing operations. Also, it can be extended to color images.
- In future CNN can be used to improve the anti-forensic and forensic techniques.

References

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

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

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

[4] W. S. Lin, S. K. Tjoa, H. V. Zhao, and K. J. R. Liu, "Digital image source coder forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 3, pp. 460-475, 2009.

[5] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Investig.*, vol. 10, no. 3, pp. 226-245, 2013.

[6] O. M. Al-Qershi and B. E. Khoo, "Enhanced block-based copy-move forgery detection using k-means clustering," *Multidimens. Syst. Signal Process.*, vol. 30, no. 4, pp. 1671-1695, 2019.

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

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

[9] H. Farid, "*Digital Image Forensics*," https://farid.berkeley.edu/downloads/tutorials/digital imageforensics.pdf, 2012.

[10] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 450-461, 2007.

[11] G. Singh, "Top 33 Photo editing apps-Best photo apps," Available: https://www.pixpa.com/blog/photo-apps.

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

[13] 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.

[14] R. Saracco. (2018). *IEEE future directions* [Online]. Available: https://cmte.ieee.org/futuredirections/2018/08/23/6953.

[15] S. Walia and K. Kumar, "Pragmatical Investigation of Frequency-Domain and Spatial-Structure Based Image Forgery Detection Methods," *Int. J. Comput. Intell. IoT*, vol. 1, no. 2, pp. 240-245, 2018.

[16] X. Y. Wang, C. Wang, L. Wang, L. X. Jiao, H. Y. Yang, and P. P. Niu, "A fast and high accurate image copy-move forgery detection approach," *Multidimens. Syst. Signal Process.*, vol. 31, no.3, pp. 857-883, 2020.

[17] "FaceApp," Available: https://www.faceapp.com.

[18] F. Luan, S. Paris, E. Shechtman, and K. Bala, "Deep photo style transfer," in *Proc. 2017 Int. Conf. Comp. Vis. Patt. Recog.*, 2017, pp. 6997-7005.

[19] A. Akula, A. Singh, R. Ghosh, S. Kumar, and H. K. Sardana, "Target recognition in infrared imagery using convolutional neural network," in *Proc. Int. Conf. Comp. Vis. Image Process.*, 2016, pp. 25-34.

[20] A. Singh and P. K. Jain, "A compartive study of SVD and ICA for target detection in through-the-wall radar images," in *Proc. 11th Int. Conf. Indus. Inf. Syst.*, 2016, pp. 608-613.

[21] T. J. Afullo, "Global Information and Africa: the telecommunications infrastructure for cyberspace," *Libr. Manag.* vol. 21, no. 4, pp. 205–214, 2000.

[22] A. Kamilaris and A. Pitsillides, "Mobile Phone Computing and the Internet of Things: A Survey," *IEEE Internet of Things Journal*. vol. 3, no. 6, pp. 885-898, 2016.

[23] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," *IEEE Access*, vol. 6, pp. 20596-20608, 2018.

[24] A. K. Jain, S. C. Sharma, R. Jha, and K. Manoj, "Effect of congestion on the performance of IEEE 802.11 network," *Int. J. Inf. Commun. Technol.*, vol. 1, no. 3/4, pp. 318-328, 2008.

[25] M. Alibakhshikenari, B.S. Virdee, C.H. See, F. Falcone, and E. Limiti, "Study on isolation improvement between closely-packed patch antenna arrays based on fractal metamaterial electromagnetic bandgap structures," *IET Microwaves, Antennas Propag.*, vol. 12, no. 14, pp. 2241-2247, 2018.

[26] Y. Wang *et al.*, "Fixed frequency reuse for LTE-advanced systems in local area scenarios," in *Proc. VTC Spring 2009 - IEEE 69th Vehicular Tech. Conf.*, 2009, pp. 1-5.

[27] A. V. Vanmali and V. M. Gadre, "Visible and NIR image fusion using weight-map-guided Laplacian–Gaussian pyramid for improving scene visibility," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 42, pp. 1063-1082, 2017.

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

[29] 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.

[30] 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.

[31] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 4, pp. 857-867, 2010.

[32] T. H. Park, J. G. Han, Y. H. Moon, and I. K. Eom, "Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain," *Eurasip J. Image Video Process.*, vol.1, pp. 1-10.

[33] G. Cao, Y. Zhao, R. Ni, and H. Tian, "Anti-forensics of contrast enhancement in digital images," in *Proc. 12th ACM Workshop Multimed Security*, 2010, pp. 25-34.

[34] 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.*, 2013, pp. 8682–8686.

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

[36] 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.

[37] 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.*, 2013, pp. 3043–3047.

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

[39] 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.

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

[41] 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.*, 2008, pp. 803–808.

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

[43] Y. Kim, J. W. Soh, and N. I. Cho, "AGARNet: Adaptively Gated JPEG Compression Artifacts Removal Network for a Wide Range Quality Factor," *IEEE Access*, vol. 8, pp. 20160-20170, 2020.

[44] E. A. Armas Vega, E. González Fernández, A. L. Sandoval Orozco, and L. J. García Villalba, "Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression," *IEEE Access*, vol. 8, pp. 11815-11823, 2020.

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

[46] 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.*, 2013, pp. 3058–3062.

[47] 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 Secur.*, vol. 9, no. 8, pp. 1211–1226, 2014.

[48] W. Fan, K. Wang, F. Cayre, and 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.*, 2010, pp. 1694–1697.

[49] 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.

[50] P.Y. Lin. (2009). *Basic image compression algorithm and introduction to JPEG standard* [Online]. Available: http://disp.ee.ntu.edu.tw/meeting.

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

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

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

[54] 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.

[55] T. K. Boehme and R. Bracewell, "The Fourier Transform and its Applications," vol. 31999, pp. 267-272, 1986, New York: McGraw-Hill.

[56] R. Saxena and K. Singh, "Fractional Fourier Transform: A Review," *IETE J. Educ.*, vol. 48, no.1, pp. 13-29, 2007.

[57] V. Namias, "The fractional order fourier transform and its application to quantum mechanics," *IMA J. Appl. Math.*, vol. 25, no. 3, pp. 241-265, 1980.

[58] S. C. Pei, and M. H. Yeh, "Discrete fractional Fourier transform," in *1996 IEEE Int. Symp. on Circ. and Syst. the World. ISCAS 96*, pp. 536-539, 1996.

[59] M. H. Yeh and S.C. Pei, "Improved discrete fractional Fourier transform," *Opt. Lett.*, vol. 22, no. 14, pp. 1047–1049, 1997.

[60] S. C. Pei, M. H. Yeh, and C. C. Tseng, "Discrete fractional Fourier transform based on orthogonal projections," *IEEE Trans. Signal Process.*, vol. 47, no. 5, 1335-1338, 1999.

[61] N. Goel and K. Singh, "A modified convolution and product theorem for the linear canonical transform derived by representation transformation in quantum mechanics," *Int. J. Appl. Math. Comput. Sci.*, vol. 23, no. 3, 685-695, 2013.

[62] K. Singh and R. Saxena, "Performance of discrete fractional Fourier transform classes in signal processing applications," *Dr. Diss.*, 2006.

[63] H. M. Ozaktas, O. Ankan, M. Alper Kutay, and G. Bozdagi, "Digital computation of the fractional fourier transform," *IEEE Trans. Signal Process.*, vol. 44, no. 9, 2141-2150, 1996.

[64] B. Santhanam and J. H. McClellan, "The discrete rotational fourier transform," *IEEE Trans. Signal Process.*, vol. 44, no. 4, 994-998, 1996.

[65] M. H. Yeh and S. C. Pei, "A method for the discrete fractional Fourier transform computation," *IEEE Trans. Signal Process.*, vol. 51, no. 3, 889-891, 2003.

[66] S. C. Pei and J. J. Ding, "Closed-form discrete fractional and affine fourier transforms," *IEEE Trans. Signal Process.*, vol. 48, no. 5, 1338-1353, 2000.

[67] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 2002, 2nd edition (*Beijing: Publishing House of Electronics Industry*).

[68] S. C. Pei and M. H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Trans. Signal Process.*, vol. 49, no. 6, pp. 1198-1207, 2001.

[69] M. F. Gerek, and O. N. Erden, "The discrete fractional cosine transform," in *Proc.* IEEE Balkan Conf. Sig. Process. Commun. Circ. Syst., 2000, pp. 1-4.

[70] A. W. Lohmann, D. Mendlovic, Z. Zalevsky, and R. G. Dorsch, "Some important fractional transformations for signal processing," *Opt. Commun.*, vol. 125, no. 1-3, 1996, pp.18-20.

[71] M. Arora and K. Singh "An improved algorithm for the detection of diabetes using Iris Images," *Dissertation*, 2016.

[72] N. Jindal and K. Singh, "Joint image compression-encryption using discrete fractional transforms," *Imaging Sci. J.*, vol. 62, no. 5, pp. 265-272, 2014.

[73] M. Arora, K. Singh, and G. Mander, "Discrete fractional cosine transform based online handwritten signature verification," in *Proc. 2014 Recent Adv. Eng. Comput. Sci. (RAECS)*, 2014, pp. 1-6.

[74] S. M. Qi, B. Z. Li, and H. Sun, "Image watermarking via fractional polar harmonic transforms", *Jour. of Elect. Imag.*, vol. 24, no.1, pp. 1–12, 2015.

[75] G. Cariolaro, T. Erseghe, and P. Kraniauskas, "The fractional discrete cosine transform," *IEEE Trans. Signal Process.*, vol. 50, no. 4, pp. 902-911, 2002.

[76] M. J. Narasimha and A. M. Peterson, "On the Computation of the Discrete Cosine Transform," *IEEE Trans. Commun.*, vol. 26, no. 6, pp. 934-936, 1978.

[77] J. Wu, L. Zhang, and N. Zhou, "Image encryption based on the multiple-order discrete fractional cosine transform," *Opt. Commun.*, vol. 283, no. 9, pp. 1720-1725, 2010.

[78] 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.

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

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

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

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

[83] 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.

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

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

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

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

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

[89] 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*, 2012, pp. 1810–1814.

[90] 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 Secur.*, vol. 9, no. 11, pp. 1933–1942, 2014.

[91] 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.

[92] 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.

[93] 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*, 2015, pp. 1–5.

[94] 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.*, 2015, pp. 1–5.

[95] 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.*, 2011, pp. 25–30.

[96] 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.

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

[98] B. Mahdian and S. Saic, "Detecting double compressed JPEG images," in *Proc. Int. Conf. Image Crime Detect. Prevent.*, 2009, pp. 1–6.

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

[100] 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, 2006, pp. 423–435.

[101] 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.*, 2001, pp. 264–271.

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

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

[104] 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.*, 2007, pp. 217–220.

[105] 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.*, 2010, pp. 1687–1690.

[106] 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.*, 2008, pp. 803–808.

[107] 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 Secur.*, vol. 6, no. 2, pp. 396–406, 2011.

[108] 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.*, 2010, pp. 434–437.

[109] 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.

[110] 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.

[111] 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.*, 2011, pp. 2444–2447.

[112] A. Singh, G. Singh, and K. Singh, “A Markov based image forgery detection approach by analyzing CFA artifacts,” *Multimed. Tools Appl.*, vol. 77, no. 21, 28949-28968, 2018.

[113] G. Singh and K. Singh, “Digital image forensic approach based on the second-order statistical analysis of CFA artifacts,” *Forensic Sci. Int. Digit. Investig.*, vol. 32, 200899, 2020.

[114] 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, 1-14, 2015.

[115] 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.*, 2010, pp. 2109–2112.

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

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

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

[119] C. Jung, L. Jiao, H. Qi, and T. Sun, "Image deblocking via sparse representation," *Signal Process. Image Commun.*, vol. 27, no. 6, 663-677, 2012.

[120] Q. B. Do, A. Beghdadi, and M. Luong, "A new adaptive image post-treatment for deblocking and deringing based on Total Variation method," in *Int. Conf. on Info. Sci., Sign. Process. and their Appl.*, 2010, pp. 464-467.

[121] F. Alter, S. Durand, and J. Froment, "Deblocking DCT-based compressed images with weighted total variation," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2004, pp. 1-4.

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

[123] 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*, 2018, pp. 656–672.

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

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

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

[127] 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.

[128] 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.

[129] 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*, 2016, pp. 1–6.

[130] 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.

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

[132] 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.

[133] 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.

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

[135] 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.

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

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

[138] 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, 2015.

[139] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," *2013 IEEE China Summit Int. Conf. Sig. Inf. Process.*, 2013, pp. 422-426.

[140] Y. F. Hsu and S. F. Chang, "Detecting image splicing using geometry invariants and

camera characteristics consistency," in *Proc. IEEE Int. Conf. Multimed. Expo*, 2006, pp. 549-552.

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

[142] 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.

[143] 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.*, 2013, pp. 3058–3062.

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

[145] 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.

[146] 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.

[147] A. Banerji and A. M. Ghosh, *Multimedia Technologies*. New Delhi, India: Tata McGraw Hill, 2010.

[148] 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.

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

[150] A. Kumar, A. Kansal, and K. Singh, "An improved anti-forensic technique for JPEG compression," *Multimed. Tools Appl.*, vol. 78, no. 18, pp. 25427-25453, 2019.

[151] 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.*, 2010, pp. 1694–1697.

[152] G. Singh and K. Singh, "Improved JPEG anti-forensics with better image visual quality and forensic undetectability," *Forensic Sci. Int.*, vol. 277, pp. 133-147, 2017.

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

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

[155] Y. Q. Shi, C. Chen, and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," in *Proc. Int. Workshop Inf. Hiding,* 2006, pp. 249-264.

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

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

[158] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal, Image Video Process.*, vol. 11, pp. 81-88, 2017.

[159] G. Muhammad, M. H. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Mach. Vis. Appl.*, vol. 25, pp. 985-995, 2014.

[160] M. Hussain, S. Q. Saleh, H. Aboalsamh, G. Muhammad, and G. Bebis, "Comparison between WLD and LBP descriptors for non-intrusive image forgery detection," in *Proc. 2014 IEEE Int. Symp. Innovations Intell. Syst. Appl. (INISTA),* 2014, pp. 197-204.

[161] S. Agarwal and S. Chand, "Texture operator based image splicing detection hybrid technique," in *Proc. 2016 Second Int. Conf. Comput. Intell. Commun. Tech. (CICT),* 2016, pp. 116-120.

[162] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in *Proc. 2013 IEEE Global Conf. Sig. Inf. Process.*, 2013, pp. 253-256.

VITA

Amit Kumar was born in Amritsar, Punjab, India in 1989. He received B. Tech in Electronics and Communication Engineering from Amritsar College of Engineering and Technology, Amritsar, Punjab, India in 2011. He received M. Tech degree in Electronics and Communication Engineering from AKTU, India in 2015. He is presently working towards the Ph.D. degree in the Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab, India. His research interests include signal processing and image processing. His email id is amitkatyal101@gmail.com.