Improved Copy-Move Forensics Techniques for Digital Video

A thesis submitted

in fulfillment of the requirement for the award of degree

of

Doctor of Philosophy

Submitted by

Gurvinder Singh

Registration Number: 951606008

Under the Supervision of

Dr. Kulbir Singh

Professor, ECED

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY

PATIALA-147004

FEBRUARY 2022

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "**Improved Copy-Move Forensics Techniques for Digital Video**", for the award of degree of **Doctor of Philosophy** in Electronics and Communication Engineering Department (ECED), Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision and guidance of Dr. Kulbir Singh, Professor, ECED, Thapar Institute of Engineering and Technology, Patiala.

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

Date: 07/11/2022

Gurvinder Singh.

Gurvinder Singh

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

Date: 07/11/2022.

Dr. Kulbir Singh
Professor, ECED
TIET, Patiala,
Punjab, India

ACKNOWLEDGEMENTS

First and foremost, I bow down to the Almighty GOD for always showering His blessings on me. I am indebted to Him for his benevolence that held me in the moments of despair and inspired me to move forward by enlightening my thoughts with His wisdom. It is solely His grace that guided me from the very inception to the completion of this research work.

I would like to express my sincere, humble and immense gratitude to my supervisor **Dr. Kulbir Singh**, Professor, Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala for his guidance, valuable advice, supervision, support, motivation and kindness throughout this research work. The completion of the research work carried out in this thesis is attributed to extensive guidance from my supervisor. I thanks to **Dr. Kulbir Singh** for convincing me to go down this road and never letting me go off track with his intriguing ideas. I am thankful to **Dr. Kulbir Singh** for his enthusiastic supervision, untiring efforts, constructive criticism, and beneficial remarks during inspiring discussions helped a lot in the accomplishment of this thesis.

I thanks to **Dr. Neeru Jindal**, Assistant Professor, Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala for her valuable advice, support and motivation during my research work.

I am highly grateful to **Dr. Alpana Agarwal**, Head of Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala for her continuous support and encouragement in my research work. I would like to thank **Dr. Anil Kumar Verma**, Professor, Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala for his guidance and cooperation. Moreover, I would also like to express sincere gratitude to my doctoral committee members **Dr. Vinay Kumar**, Associate Professor, **Dr. Amit Mishra**, Assistant Professor in Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala, and **Dr. Sunil Kumar**, Associate Professor in Electrical and Instrumentation Engineering Department, Thapar Institute of Engineering and Technology, Patiala for their valuable suggestions during my entire research.

I am also immensely thankful to my fellow researchers, Dr. Gurinder Singh, Dr. Kanwarpreet Kaur, Amit Kumar, Navneet Kaur at Thapar Institute of Engineering and Technology, Patiala

for helping me throughout my research. The acknowledgment would be incomplete if i do not express my gratitude to the non-teaching staff of the department for their help during the course of this study.

I would like to thank my family members for their love, affection, encouragement, and support. I also owe the completion of this work to my dearest parents Mr. Anup Singh and Mrs. Kuldeep Kaur who supported me in all pursuits of life by learning from past experiences. I also thanks to my wife Mrs. Rupinder Kaur who always motivated me to move ahead with a positive attitude towards life. I am also thankful to my brother Mr. Tejinder Singh and sister-in-law Mrs. Harmeet Kaur for their encourage and support. Lastly, I would like to acknowledge the love of my daughters Divjot Kaur, Tanmeet Kaur, niece Japleen Kaur and nephew Prabhnoor Singh who give me happiness moments with their naughty activities.

Gurvinder Singh

ABSTRACT

There are a lot of editing tools, software and devices like mobile phone, digital cameras, digital camcorders, etc., that are easily used to manipulate the contents of authentic digital videos without leaving behind any footprints. During manipulation, any frame or region of digital video is altered with Copy-Move (CM) forgery, which results in forged digital videos with Copy-Move Frame Duplication (CMFD), Copy-Move Region Duplication (CMRD), and Chroma Key Foreground (CKF) forgeries. Due to these forgeries, it becomes more difficult to detect the authenticity of digital videos through the eyes. Therefore, it is essential to ensure digital videos' reality in this real-world scenario. There are several existing techniques for detecting these forgeries in digital videos in the literature. However, these existing techniques have suffered from several limitations for detecting the CMFD, CMRD and CKF forgeries in digital videos.

In this thesis, work has been done to improve the detection of CMFD, CMRD and CKF forgeries in digital videos. In the presented work of CMFD forgery detection, the proposed approach has detected duplicated frame sequence at long continuous locations as well as at many different locations with different lengths of frame sequence in the digital videos using Correlation Coefficients (CC) and also detected the frame sequences which are duplicated from other digital videos with Coefficient of Variation (CV). Thus, it is observed that the presented work is more effective for detecting frame duplications in large and small frame sequences with higher detection accuracy (DA) in digital videos than the existing techniques.

The limitation of detecting the less number of duplicated frames has been removed in multiple CMFD forgery detection approach. This presented work is based on Equal Central Block Variance (ECBV), which has efficiently detected multiple frame duplications in the digital videos such as single frame duplication (SFD) in the entire digital video, repetition of a frame (RF) in the form of sequence, shuffled frame sequence (SFS) and disorder frame sequence (DFS). By comparing the results, it has been found that early and effective detection with higher DA and minimum execution time achieved in different digital video cases by multiple CMFD forgery detection approach.

In the presented work for detecting CMRD forgery, the CMRD forgery detection approach has detected rectangular and square shape regular region duplications and irregular region duplications with many irregularities within the same frames and from the other frames of the digital videos. This presented work is based on CC and CV to detect regular and irregular region duplications in digital videos. From its comparison with existing techniques, it has been noticed

that the proposed approach provides more effective performance with higher DA in digital videos taken from the SULFA dataset and downloaded from the internet.

The drawback of detecting small duplicated regions in the digital videos has been eliminated in the proposed multiple CMRD forgery detection approach based on Histogram Equalization (HE) and block filtering. This presented work has effectively detected single and multiple CMRD forgeries with different region sizes such as 3× 3, 4× 4, 8×8, 16×16, 24× 24, and 32× 32 in the digital videos. It is observed by comparing this work with the existing techniques that it provides better results on detecting single and multiple CMRD forgeries with different region sizes in the digital videos than others.

There are very few existing techniques for detecting CKF forgery in the literature. In this thesis, the CKF forgery detection approach has been seen this forgery based on Frame Edge Identification (FEI) in the digital videos. The proposed method has identified and detected CKF forgery within the edge frames. This approach has also isolated this forgery from the authentic part of the edge frame with localization and tracking in each frame of the forged digital video. This presented work has performed more efficiently on the digital videos with different cases taken from the SULFA dataset. This work has provided adequate robustness against various attacks. It has also implemented digital videos, which are downloaded from the internet. The experimental results indicate higher DA with lower execution time and better robustness than existing techniques.

LIST OF PUBLICATIONS

Published Journal Publications:

[P.1] G. Singh and K. Singh, "Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation," *Multimedia Tools and Applications*, vol. 78, pp. 11527–11562, 2019, doi: 10.1007/s11042-018-6585-1 **(SCI Indexed, Impact Factor 2.75)**

[P.2] G. Singh and K. Singh, "Chroma key foreground forgery detection under various attacks in digital video based on frame edge identification," *Multimedia Tools and Applications*, vol. 81, pp. 1419–1446, 2022, doi: 10.1007/s11042-021-11380-3 **(SCI Indexed, Impact Factor 2.75)**

Communicated Journal Publications:

[C.1] G. Singh and K. Singh, "Multiple Copy-Move Forgery Detection in Digital Video Frames and Regions," *Journal of Signal Processing Systems*. **(SCI Indexed, Impact Factor 1.348)**

[C.2] G. Singh and K. Singh, "Copy-Move Video Forgery Detection Techniques: A Systematic Survey with Comparisons, Challenges and Future Directions," *Wireless Personal Communications*. **(SCI Indexed, Impact Factor 1.671)**

LIST OF ACRONYMS AND ABBREVIATIONS

CM	Copy-Move
CKF	Chroma Key Foreground
CMFD	Copy-Move Frame Duplication
CMRD	Copy-Move Region Duplication
CC	Correlation Coefficients
CV	Coefficients of Variation
ECBV	Equal Central Block Variance
HE	Histogram Equalization
FEI	Frame Edge Identification
DCT	Discrete Cosine Transformation
LBP	Local Binary Pattern
HOG	Histogram of Oriented Gradients
HSV	Hue-Saturation-Value
SURF	Speeded Up Robust Features
FLANN	Fast Library for Approximate Nearest Neighbours
DWT	Discrete Wavelet Transform
LSB	Least Significant Bit
RGB	Red Green Blue
SIFT	Scale-Invariant Feature Transform
CNN	Convolutional Neural Network
2D-CNN	2 Dimensional-Convolutional Neural Network
3D-CNN	3 Dimensional-Convolutional Neural Network
SSIM	Structural Similarity Index
MSE	Mean Square Error
PR	Precision Rate
RR	Recall Rate
DA	Detection Accuracy
F1	F1 Score
F2	F2 Score
FPR	False Positive Rate

FNR	False Negative Rate
TPR	True Positive Rate
TNR	True Negative Rate
SULFA	Surrey University Library for Forensic Analysis
2D	Two Dimensional
3D	Three Dimensional
ROC	Receiver Operating Characteristic
QF	Quantization Factor
SFD	Single Frame Duplication
SFS	Shuffled Frame Sequences
RF	Repetition of a Frame
DFS	Disordered Frame Sequences

GLOSSARY OF SYMBOLS

$\alpha(.)$	Normalizing scale factor
u	Horizontal spatial frequency for integers $0 \leq u < 8$
v	Vertical special frequency for integers $0 \leq v < 8$
$D_{u,v}$	DCT coefficients
$d_{x,y}$	Pixel intensity value at coordinates (x, y)
$cos(.)$	Cosine function
$\sum_{(.)}$	Summation function
exp (.)	Exponential function
$\overrightarrow{p}, \overrightarrow{q}$	Vectors
$p_{(.)}$	Element of vector $\overrightarrow{p}$
$q_{(.)}$	Element of vector $\overrightarrow{q}$
$A_{(.)}$	Element of one-dimensional vector
$\mu_{(.)}$	Mean of vector
H(.)	Hessian matrix
I	Integral image
δ	Scale
X	a point of I at scale δ
$\frac{\partial^2}{\partial X^2}$	Gaussian second order derivative
L (.)	Convolution of $\frac{\partial^2}{\partial X^2}$ with I at a point X
v	Four-dimensional descriptor vector
dx	Wavelet response in horizontal direction
dy	Wavelet response in vertical direction
|dx|	Absolute value of the response dx
|dy|	Absolute value of the response dy
G_{ab}	Smooth frame with pixel co-ordinators (a, b)
(2c+1) × (2c+1)	Gaussian filter kernel size
σ	Standard deviation
|G|	Gradient magnitude
$K_{G(.)}$	Kernel for the gradient

$G_{(.)}$	Gradient
$\lvert G_{(.)} \rvert$	Magnitudes of $G_{(.)}$
arctan	Arctangent function
θ	Angle of direction of the edge
$g(.)$	Grayscale Image
$m_{(.)}$	Number of pixel
M	Total number of pixels
K	Highest gray level
$p(.)$	Probability
μ	Mean
C_0	Background class
C_1	Object class
ω_0	Probability of C_0
ω_1	Probability of C_1
μ_0	Average gray level of C_0
μ_1	Average gray level of C_1
μ_t	Total average gray level of $g(.)$
T	Gray level for threshold
$\in$	Set membership
T'	Optimal threshold
σ^2 (T)	The between-class variance at T
$\arg \max_{1 \le T < K}$	Arguments of the maxima
$P_L(.)$	Probability density function
$C_L(.)$	Cumulative density function
$F_{(.)}$	Pixel intensity level from 0 to G
$n_{(.)}$	Total number of pixels for calculating $P_L(.)$
Y	Output image
T"	Threshold for getting Y in HE
$\forall$	Universal quantification
μ_m	Average pixel value of m region,
μ_n	Average pixel value of n region

$\sigma^2_{(.)}$	Variance
σ_{mn}	Covariance of m and n regions
K_1 and K_2	Constants
P *and* Q	Blocks for calculating MSE
$R \times R$	Size of P and Q
(d, e)	Pixel co-ordinates of P and Q
$*$	Convolution operation
$\times$	Multiplication
R, *G* and *B*	Red, Green, and Blue channels of RGB frame
I_L	Luminance component.
l	Length of a digital video
n	Length of a frame sequence
av	Average of calculated variances
f_T	Total number of frames
f_N and f_{N+1}	Two consecutive frames
f_P	RGB difference frame obtained by f_{N+1}-f_N
f_Q	Another RGB difference frame obtained by f_N -f_{N+1}
f_D	Combined RGB difference frame
$r(.)$	Rate of large edge pixel difference values
$\sum Q_n$	Sum of large edge pixel difference values of n^{th} edge frame
N_n	Total number of edge pixel difference values of n^{th} edge frame

LIST OF FIGURES

LIST OF TABLE

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

This chapter provides a brief introduction of basic concepts that are the foundation to enhance the interest for diving into the depths of the research work conducted in this thesis. It deals with the essential terms related to digital video forensics, different kinds of digital video forgery and Copy-Move forgery in the real world scenario.

1.1 Preamble

Due to the growth in multimedia technology, the availability of internet and video capturing devices such as mobile phones, digital cameras, digital camcorders and CCTV has been increased. The memorable moments of life are captured in these devices' digital videos and images. These digital videos and images represent effective communication over social media [24]. Traditionally, it has been ensured that the running digital video in TV news or published photographs in newspapers has been recognized with certification of faithfulness. Also, the recording of surveillance video has been represented as evidence in a court of law [27]. However, in recent years, there have been many video editing tools, software, and devices utilized to manipulate the contents of original digital videos for making forged digital videos. A particular object or event is concealed in these forged digital videos without leaving behind any footprints [84]. These manipulations provide more difficulty for detecting the authenticity of digital videos. Therefore, a tool is required to expose the authenticity of digital videos in the real world scenario.

1.2 Digital Video Forensics

Digital Video Forensics is a field that deals with the investigation of the authenticity of digital videos. It provides a tool to expose the malicious manipulation in digital videos [50], [86]. The maximum research work has been devoted to analyzing still digital images in the last decade. However, in the last few years, researchers have focused on detecting digital video forgery. Digital video forgery means manipulating the authentic contents of digital video to make forged digital video [48], [87], and [103]. The advancement in digital video processing tools technology makes tampering easy and faster. Digital Video Forensics plays a crucial role to identify such aggressive manipulations which are purely indistinguishable to human eyes.

1.2.1 Types of Digital Video Forgery

The following types of digital video forgery are shown in Figure 1.1 [86].

(a) Intra-frame Forgery

(b) Inter-frame Forgery

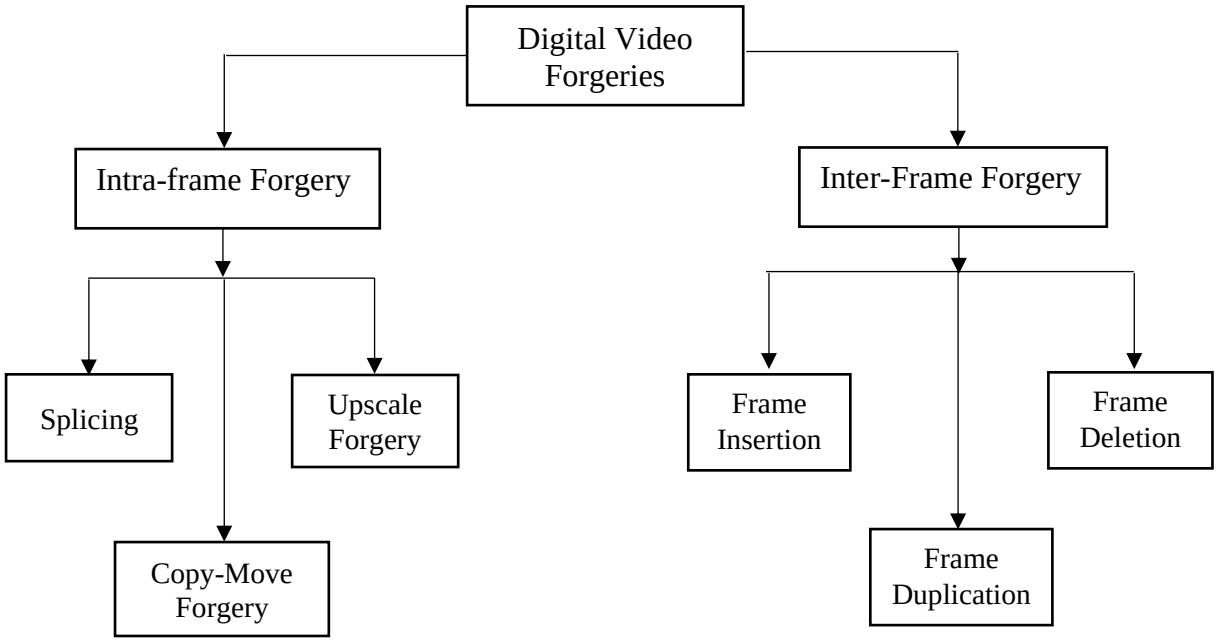


Figure 1.1: Types of Digital Video Forgery

1.2.1.1 Intra-frame Forgery

In an intra-frame forgery, the authentic contents of individual frames are altered in the digital video. When any part is added to a frame, it provides an internal disturbance between the part of the authentic frame and pastes one, i.e. the original pixel alignment gets changed. Sometimes, the added parts may be of any shape and can be presented at any location of the frame [27], [50], [84], and [86]. This type of forgery is also known as spatial tempering in digital videos. Following are the different categories of intra-frame forgery in digital videos, as shown in Figure 1.1.

1.2.1.1.1 Splicing

In this forgery, a frame is copied from one frame and then added to any other frame. This resultant frame becomes a spliced frame in the digital video [80] and [125]. An example of splicing in a digital video is shown in Figure 1.2, in which frame one and frame 2 indicate the authentic frames of two different digital videos, and the spliced frame is made by merging these two frames [88].

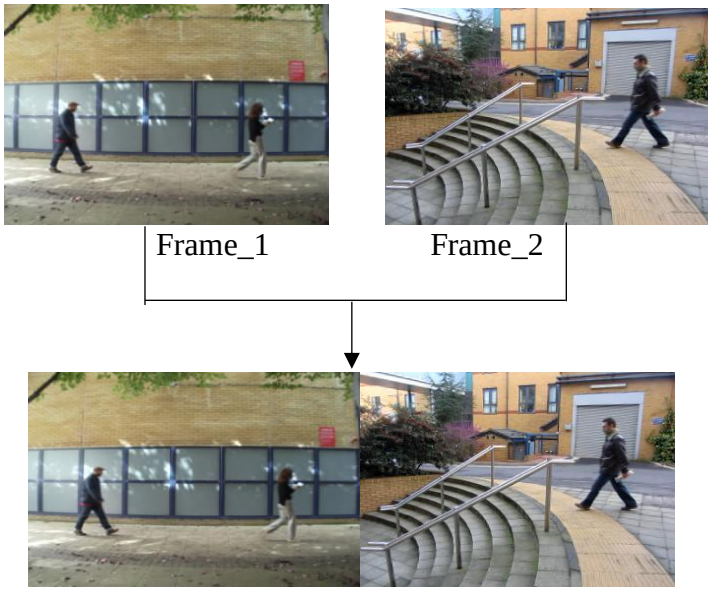
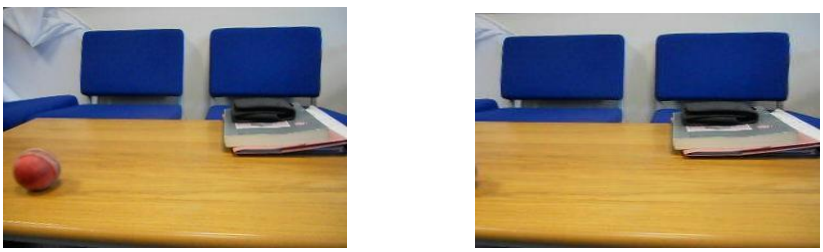


Figure 1.2: Example of Splicing forgery in the digital video

1.2.1.1.2 Upscale Crop

In this type of forgery, the outermost frame section is cropped in an upscale crop to eliminate the evidence of crime occurrence in the digital video [88]. Then, this manipulated frame is enlarged to retain the resolution across the digital video. The example of an upscale crop is shown in Figure 1.3, in which (a) indicates the authentic frame of a digital video and (b) shows the forged frame with upscale crop forgery [30].



(a) Authentic frame (b) Frame after Upscale Crop forgery (A ball is removed)

Figure 1.3: Example of Upscale Crop forgery

1.2.1.1.3 Copy-Move Forgery

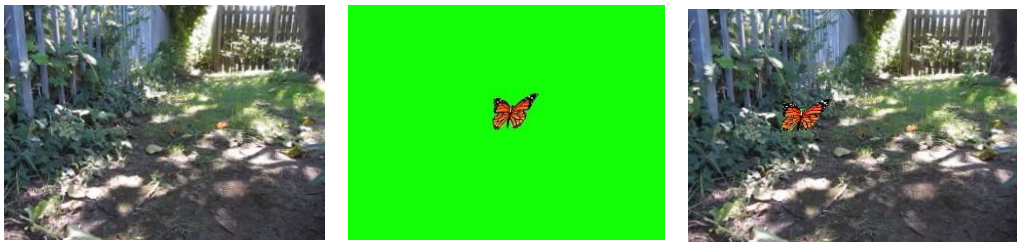
Copy-Move (CM) forgery is a forgery in which a region of frame is copied and moved to another location of the frame in the digital video [27], [50], [84], and [86]. This forgery is made with different shapes and sizes within the frame. This resultant frame becomes a region duplicated frame in the digital video. This duplication is also known as Copy-Move Region

Duplication (CMRD) forgery. An example of CMRD is shown in Figure 1.4, in which (a) indicates the authentic frame of a digital video and (b) shows CMRD forgery in the frame.

(a) The authentic frame (b) CMRD forgery

Figure 1.4: Example of CMRD forgery in the digital video

The chroma keying is another example of CM forgery. A foreground of a green screen video frame is copied and then moved to any location of frame of another natural digital video [5], [51], [89], and [118]. Figure 1.5 shows the chroma key foreground (CKF) forgery in the frame in which (a) indicates the authentic frame of a natural digital frame, (b) shows the authentic frame of a green screen digital video and (c) shows the CKF forgery in the frame [93].



(a) An authentic frame of a natural digital video (b) Authentic frame of a green screen digital video (c) CKF Forgery

Figure 1.5: Example of CKF forgery in the digital video

1.2.1.2 Inter-frame Forgery

Inter-frame forgery means manipulating frames or frame sequences within the digital video. In this forgery, a set of frames are copied from one location and inserted at another location into the digital video [27] and [86]. Figure 1.6 shows the different ways of inter-frame forgery in digital video. This forgery aims to hide any captured event of the digital video. In a digital video, the relation between adjacent frames is quite the same, which makes it a difficult task to detect the affected frame sequences in the digital video. This type of forgery is also known as temporal tempering in digital videos. This forgery is further divided into the following different categories [86].

1.2.1.2.1 Frame Insertion

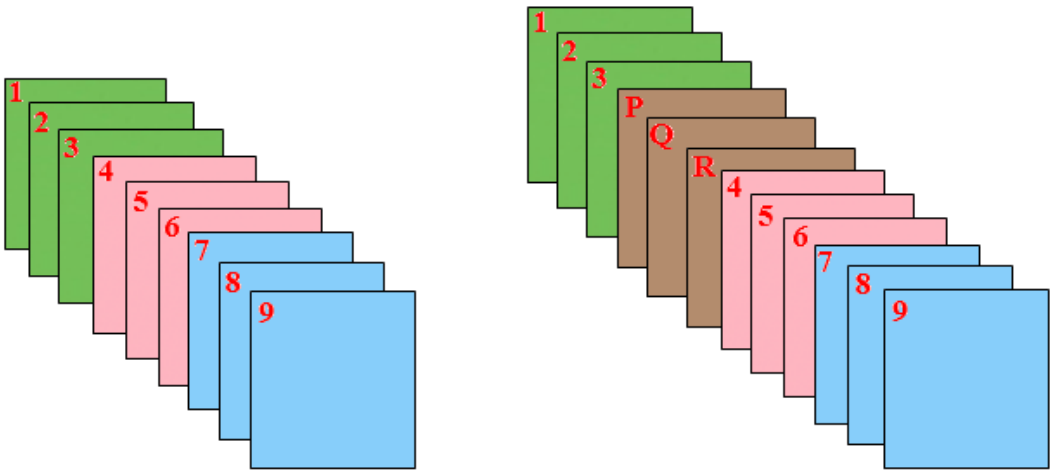
Several frames are copied from other digital videos in this forgery and moved to a natural digital video, as shown in Figure 1.6 (b) [126]. Sometimes, these copied frames are resized to keep the equal characteristics of digital video. The frame rate of forged digital video is the same as that of authentic digital video, but the total number of frames increases in the forged digital video [28].

1.2.1.2.2 Frame Deletion

In this type of forgery, some frames are removed to delete the information in the digital video, as shown in Figure 1.6 (c). Therefore, the total number of frames decreases in the forged digital video compared to authentic digital video [90], [111], and [119].

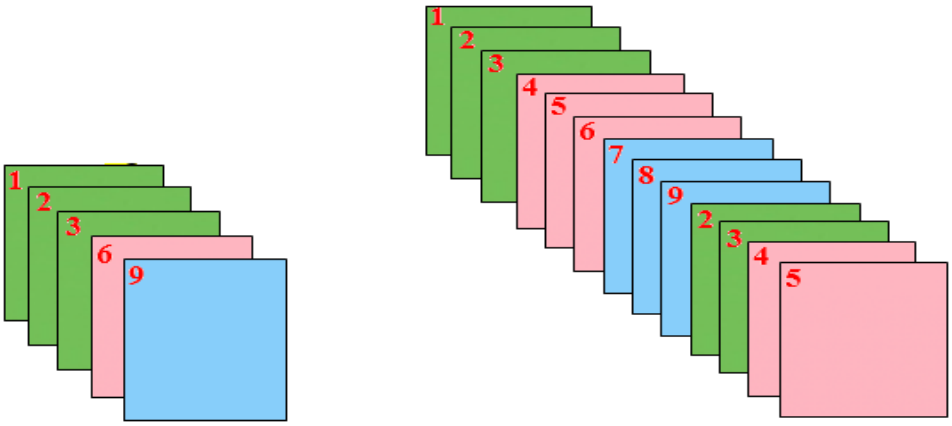
1.2.1.2.3 Frame Duplication

In frame duplication forgery, the number of frames is copied in the form of frame sequence and moved copied frame sequence at other locations of the digital video, as shown in Figure 1.6 (d). This forgery is generally used to hide the significant proofs from the digital video [20], [31], [52], and [53]. During criminal cases in courtrooms, a convict can be proved as an innocent and guiltless person in front of a court if the convict succeeds to show his/her proof by submitting a spoofed digital video as evidence [47], [54], and [91]. This duplication is also known as Copy-Move Frame Duplication (CMFD) forgery.



(a) (b)

Figure 1.6: (a) Authentic frame sequence (b) Frame Insertion forgery



(c) (d)

Figure 1.6: (c) Frame Deletion forgery (d) Frame Duplication forgery

1.3 Basics of CM Forgery

Today, CM forgery is the most frequently encountered forgery in digital videos. It has been prepared by duplicating an object or a frame in the frame sequence of digital video [76] and [55]. When several frame sequences are replicated within the digital video, it creates CMFD forgery [91]. On the other side, while objects are introduced in the frame sequence to generate more objects or hide any particular region inside the frame, it makes CMRD forgery [32]. Similarly, the duplication of foregrounds from a green screen digital video to other natural digital video spreads CKF forgery over social media. These forgeries make it a great challenge to identify the authenticity of digital videos in the real world scenario. During forgery creation, there are some footprints left behind in the digital video. These footprints differentiate the authentic and forged digital videos by CM forgery detection techniques [35].

1.3.1 CM Forgery Detection Techniques

In the history of digital video forensics, researchers have classified CM forgery detection techniques into two forms: active technique and passive technique [27], [50], [84], and [86].

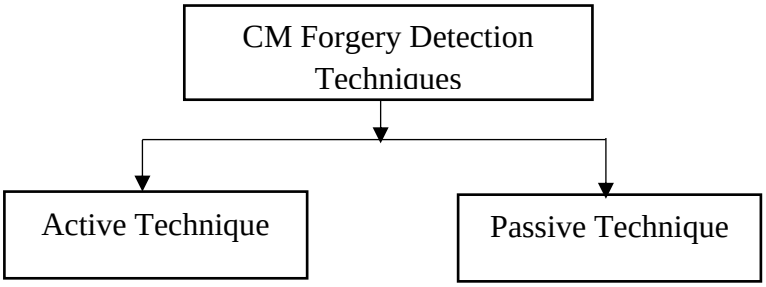


Figure 1.7: Types of CM forgery Detection Techniques

1.3.1.1 Active Technique

The active technique is one in which an additional material like a digital signature or digital watermark has been added during digital video creation so that the authenticity of the digital video contents can be verified [27] and [84]. A digital signature is dependent on the public key encryption. A private key is utilized to translate the hashed form of the frame. This translated form makes a unique "signature" for the frame. For the decryption process, a public key is used to decrypt the signature [50]. A watermark is also inserted in the image or code into the frame. This watermark is used to verify the authenticity of the digital video. However, it has been observed that only watermark is not enough to verify the authenticity because multiple watermarks could be inserted into the digital video frame. It has also been noticed that these watermarks are not more suitable for protecting and verifying the authenticity of the digital videos [86]. Besides, this technique has a few limitations such as (i) anybody can manipulate the digital video contents during the watermark insertion, (ii) the manipulations in digital video's contents can be done before encryption, and (iii) there is a need of hardware for inserting the watermark or signature in digital videos. Therefore, this technique has narrow applications [86] and [103].

1.3.1.2 Passive Technique

On the other side, in passive technique, the authenticity of the digital videos are identified without inserting any material and using any hardware. This technique extracts the internal features of a digital video for detecting CM forgery. The statistical or mathematical characteristics of digital video are changed with any kind of manipulations [50]. These changed characteristics assist the researchers for detecting CM forgery in the digital video. Therefore, this technique is more effective than active technique [86], [103]. This technique also analyses forgery localization which depends on feature statistics of the digital video. Therefore, the algorithms and methods of forgery detection and localization in the digital video are based on statistical or mathematical characteristics [87]. Over the years, researchers have used various kinds of such expressive features to detect CM forgery. The signs of forgery in the digital video contents reveal the specific artifacts in one or more features. Therefore, the occurrence of forensics artifacts helps the investigators as evidence of content manipulating operation in the digital videos [86], [87].

1.4 Need for digital video forgery identifications

There are following points for the need of digital video forgery identification:

1. The flow of fake information through the forged digital videos in the multimedia creates a lot of confusion between people. Therefore, in order to escape from spreading any confusion through the forged digital videos, it is more need of identification of authentic/ forged digital videos in the real-world scenario.
2. The forged digital videos are raised several disputes and contradiction issues by distributing these videos over the social media. These disputes and issues lost the peace of mind which provides bad outcomes on the social media. Hence, there is a great requirement of detection of digital video forgery to prevent such types of disputes and contradiction issues.
3. Today, due to easily available video editing tools and software, each human has a capability of manipulating the digital videos according his/her own choice. Thus, the forged digital videos can also be represented as fake evidence in the sight of court which may lead to a wrong conviction. So, the need of digital video forgery identification is going to increase.
4. For the security purpose of digital videos, the digital video forgery detection techniques are much required to prevent the forgery in digital videos' frames and their regions. These techniques can provide a great assistance to identify and trace the area from where a part of digital videos has been stolen, copied and distributed.
5. While the forgery is created in the digital videos, then it results in some artifacts in the frame of digital videos. The detection and analysis of artifacts help the investigator to discover the authenticity of a digital video. Thus, there is a lot of need for the digital video forgery identification.

1.5 Present challenges in digital video forgery detection:

There are present challenges in digital video forgery detection which has been described as below:

- The existing techniques are required to detect the frame duplication if a copied set of frames are shuffled or reversed on different position in the digital video.
- The performance is decreased if number of duplicated frames is less than length of duplicated frame sequence.
- Change in bit rate and quantization scale ratio effect the performance.

- It is difficult to detect the too small size forged regions in the digital video.
- It is challenging task for the researchers to detect the forgery in digital videos with several types of noise. Because these noise effect all pixel intensities of the frame.

1.6 Requirement of the future research:

The requirement of the future research is discussed as follow:

- Robustness: In the future research, it is a most requirement of robustness in the digital video detection techniques because various attacks and a number of environmental conditions affect the pixel of each frame of digital videos during the making forged digital videos and capturing the digital videos. The attacks and environmental conditions decrease the performance of digital video forgery detection techniques. Therefore, the work on robustness is required in the future research.
- Machine learning techniques: Researchers have presented a number of statistical methods for detecting forgery in the digital videos. Now, it is required to detect digital video forgery using machine learning techniques. In the machine learning techniques, the machine learning (ML) and deep learning (DL) models are applied for the digital video forgery detection. These techniques are need a huge amount of data and are also capable of automatically learning the complex features/artifacts for the detection of digital video forgery. This encourages the researchers to design the automated technique for the digital video forgery detection.
- Digital Video Frame Count: Most of the passive techniques depend on the numbers of frame duplicated in case of Copy-Move Frame Duplication (CMFD) detection. These techniques have not capability for CMFD detection in the digital video when the digital video frame count is less than a certain threshold.
- Digital Video Detection and Localization: A single type of forgery has been identified and localized in the digital videos by most of passive techniques. At the same time, these techniques have not capability to detect the multiple forgeries such as splicing, upscale crop, frame replication, frame mirroring etc.) in the digital video.
- Digital Video Background: There are many forgery detection techniques which are designed to detect the forgery in a digital video having a static background. However, there are a few techniques which expose the forgery in digital video having a moving background. Thus, it becomes an issue on which the researchers can do more work.

1.7 Motivation

The main use of CM forgery detection is to determine the authenticity of digital video contents. Most of the research work has been done for detecting CM forgery on still digital images. Today, every person can edit the digital video due to which controversial issues and several disputes are increased in the real world scenario. In contrast, these forged digital videos are posted over the social media. The detection of CM forgery is increasing day by day for the security of digital videos [36], [127]. Therefore, the research work has focused on detecting CM forgery in the digital videos. However, there are few existing techniques for detecting CM forgery in duplicated frames and regions of the digital videos. During forgery creation in the digital video, many frames or any part of the frame are copied and moved to other locations within the digital video, resulting in CMFD and CMRD artifacts. The detection and analysis of both duplications assist the investigator in finding the authenticity of a digital video.

CMFD forgery detection techniques such as [6], [56], [106], [112], and [120] are the motivation behind the presented work for detecting CMFD forgery in the digital videos. Most of these techniques have been detected the CMFD forgery within a small frame sequence of the digital video at only one location. Then, what will be happened while several events in a digital video are lost at different locations. Moreover, there are various frame duplications in the digital videos that have limited the detection of these techniques. Therefore, it motivated to carry out the research work for accurate detection of CMFD forgery in the digital videos.

The inspiration of research work for detecting CMRD forgery was got by the work of [7], [8], [67], [92], [94] and The study of these works reveals many aspects that can improve the detection of CMRD forgery within different shapes and locations in the digital videos. Furthermore, this research work can extend for detecting CMRD forgery within different sizes in the digital videos. So, a proposed approach is devoted to improving the detection of CMRD forgery in the digital videos.

There are very few techniques [5], [51], [89], and [118] which have been encouraged to enhance the accuracy for CKF forgery detection in the digital videos. It is observed from the study of these techniques that their detection accuracy is quite low and is also not immune against the attacks. It has motivated to provide the robustness under various attacks. Therefore, the research is inspired to design an approach for increasing the detection and immune against various attacks.

1.8 Contribution of Work

The major contributions of this thesis can be summarized as follows:

(i) An approach is proposed to detect CMFD forgery in the digital videos. In this work, a long duplicated frame sequence at the continuous location and the number of duplicated frame sequences with different lengths at different locations are detected in the digital videos. Several frame sequences duplicated from other digital videos with different resolutions are also detected in this work.

(ii) A proposed approach detects multiple CMFD forgeries in the different kinds of digital videos. In this work, the proposed approach detects single duplicated frame in the entire digital video, repetition of a frame in the form of sequence, shuffled frame sequences, and disorder frames in the sequences.

(iii) CMRD forgery is detected in the digital videos by the proposed approach. In this work, the regular and irregular region duplications are detected within the same frame and from another frame of the digital videos.

(iv) The proposed approach detects single and multiple CMRD forgeries in the digital videos. In this work, single and multiple duplicated regions of different region sizes such as 3×3, 4×4, 8×8, 16×16, 24×24, 32×32 are detected in the digital videos.

(v) CKF forgery is detected in the digital videos by the proposed approach. In this work, CKF forgery is detected in different circumstances within different digital videos. CKF forgery is also isolated and differentiated from the authentic foregrounds of the digital videos. Also, this proposed approach detects the CKF forgery within the digital videos under various attacks to provide better robustness.

1.9 Thesis Organization

The flow of the work carried out in this thesis is summarized in the following manner:

Chapter 1 presents the introduction of Digital Video Forensics, types of digital video forgery, CM forgery, CM forgery detection techniques, motivation behind the research work, contributions of work and thesis organization.

Chapter 2 provides a comprehensive review of related literature to give background information about detection of CMFD, CMRD and CKF forgeries in the digital videos. Based on literature review, the research gaps are discussed and research objectives are defined.

Chapter 3 presents CMFD forgery detection approach for detecting the duplicated frame sequence in the digital videos. This approach is based on Correlation Coefficients (CC) and Coefficients of Variation (CV). It has detected the duplicated frame sequences at continuous and different locations within the digital videos. Different evaluation parameters confirm the performance of the presented approach. The comparison with the existing techniques is also made in this chapter.

Chapter 4 focuses on the multiple CMFD forgery detection approach based on Equal Central Block Variance (ECBV) for detecting the multiple CMFD forgeries in the digital videos. Different kinds of digital videos are used to observe the performance of the presented approach. This presented approach is evaluated on different parameters and compared with the existing techniques in this chapter.

Chapter 5 deals with the CMRD forgery detection approach for detecting the duplicated regions in the digital videos. This approach has detected regular and irregular duplicated regions within the same frame and from another frame in the digital videos. The evaluation of this approach has been accomplished with several performance parameters. Moreover, the potential of the proposed approach is established against state-of-the-art existing approaches.

Chapter 6 presents a technique based on Histogram Equalization (HE) for detecting single and multiple CMRD forgeries of different region sizes in the digital videos. This chapter explores the capability of the presented technique for detecting the smallest duplicated region in the digital video. This technique has effectively performed on the digital videos for evaluating different parameters. Furthermore, the proposed technique is also compared with existing techniques.

Chapter 7 provides the CKF forgery detection approach that detects CKF forgery in the digital videos. This approach is based on Frame Edge Identification (FEI). This chapter also presents the ability of the proposed approach to work under various attacks in the digital videos. Different parameters have also been evaluated for the performance of the presented approach in the digital videos. Besides, its performance is compared against state-of-the-art existing approaches.

Chapter 8 provides the thesis's conclusion and the possible future scope in the area of presented work.

CHAPTER 2

LITERATURE SURVEY

This chapter is dedicated to studying and analyzing the literature's fundamental concepts related to CM forgery detection in the digital videos. It provides information associated with the presented research work's terms, functions, and methods. Furthermore, various performance metrics are also discussed to evaluate CM forgery detection techniques. Besides, this chapter covers the motivation, research gaps, objectives, and research methodology.

2.1 Context of CM Forgery Detection in Digital Videos

In the past, the video running in TV news or a photograph published in daily newspapers assured the integrity of visual and pictorial data. Similarly, in a court of law, the recording of surveillance video was considered authentic proof [27], [86]. However, due to the easy availability of video editing tools and low cost devices, the authentic video contents can be easily manipulated for concealing any object or event of video files without leaving behind any footprints. These digital videos can be easily manipulated so that they appear as authentic video content [48]. Therefore, digital forensics exposes these manipulations in still photographic data and digital videos. Most of the research work of CM forgery detection has been dedicated to analyzing still digital images. Now the research work of CM forgery detection has been focused on digital videos for identifying the malicious manipulations in video data [87].

At present, CM forgery is a most frequently encountered forgery in digital video forensics in the real world scenario. CM forgery aims to hide the entire information within the digital video [84]. Such kinds of digital videos are mostly used as evidence in the court of law. CM forgery manipulates the digital videos with CMFD and CMRD forgeries. CMFD forgery duplicates the frame sequences of captured events in the digital video [112] whereas, CMRD forgery duplicates a particular frame region in the digital video [94]. Thus, CM forgery manipulates the digital video's frames and regions. CM forgery has also extended itself to CM forgery. The foreground objects are copied from a video frame sequence with a constant backing color background and moved to another natural digital video [5]. Due to these forgeries, it has become a great challenge to identify the authenticity of digital video through eyes in the real world scenario. There are some existing techniques for detecting these forgeries, but these techniques have several limitations. Therefore, there is a need to remove the limitations of existing techniques and enhance the early and accurate detection of CM forgery in frames and regions

of the digital videos to provide better results during the investigation. Hence, this approach is considered in this research work.

2.2 Feature Selection Techniques for CM forgery Detection

The feature selection techniques depend on the internal characteristics of frames in the digital video because CMF disturbs the characteristics of video frames and provides some kind of static and temporal artifacts in the digital videos. The following techniques have been developed in the literature for the detection of CM forgery in the digital videos.

(a) Block similarity analysis techniques

(b) Key point feature techniques

2.2.1 Block similarity analysis techniques

In these techniques, each digital video frame is divided into overlapping or non-overlapping blocks to detect CM forgery in the digital videos. Then these blocks are used to extract the features using the following different techniques.

2.2.1.1 Discrete Cosine Transformation (DCT) Based Technique

In this technique, each digital video frame is converted from spatial domain to frequency domain. The frequency-domain removes the high frequency components and highlights the low frequency components for detecting the forgery. The DCT is given as follows [33]:

$$D_{u,v} = \frac{1}{4}\alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} d_{x,y}\ cos\left[\frac{(2x+1)u\pi}{16}\right] cos\left[\frac{(2x+1)v\pi}{16}\right] \quad (2.2.1)$$

where, u is horizontal spatial frequency for integers $0 \leq u < 8$, v is vertical special frequency for integers $0 \leq v < 8$, $d_{x,y}$ is pixel intensity value at coordinates (x, y), $D_{u,v}$ is DCT coefficients at coordinates (u, v), and

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{If u =0} \\ 1 & \text{Otherwise} \end{cases}$$ is a normalizing scale factor for making transformation.

There are the following steps for the implementation of DCT on an image:

1. The image is broken into 8×8 blocks.

2. DCT is designed to work on the pixel intensity values whose range lies from -128 to 127. Therefore, each pixel intensity value of each block is subtracted from 128.
3. Now, DCT is performed by accomplishing the matrix multiplication such as

$$D = TMT'$$

4. The matrix 'D' consists of 64 DCT coefficients which are represented by C_{ij}. Here, the values of i and j varies from 0 to 7. C_{00} is top-left coefficient which correlates to low frequencies of block of original image. While going from C_{00} to C_{77}, the DCT coefficients correlate to higher-to-higher frequencies. C_{77} corelates the highest frequencies.
5. After that, quantization process has been done. Each element of matrix D is divided by corresponding element of quantization matrix for rounding to the nearest integer value.

$$C_{i,j} = \text{round}\left(\frac{D_{i,j}}{Q_{i,j}}\right)$$

6. For reconstruction of given image, each element of C is multiplied with the corresponding element of quantization matrix.

$$R_{i,j} = Q_{i,j} \times C_{i,j}$$

7. After that, inverse DCT of R matrix is taken and add 128 to each element for getting the original image.

$$N = (T'RT) + 128$$

He *et al.* [33] presented a method based on DCT. Firstly, the frames are divided into overlapping/ non-overlapping blocks using a fixed-size sliding window. This window moves from top-left to bottom-right by one pixel along the direction. The pixel intensity values in each block are stored in a row. A matrix is formed with these rows corresponding to each block. Then lexicographical sorting is used to detect the matched blocks. This type of method is also known as exact match method. Lukas *et al*. [57] provided a method in which DCT is applied on each block for calculating the corresponding DCT coefficients. The quantization process with suitable Q factor is used to get better results. These calculated DCT coefficients are stored in row vector for each frame block. Then these feature vectors are stored in a matrix. The performance of Lexicographical sorting over this matrix is used to detect the similar blocks with the help of shift vectors. This method has a disadvantage that it cannot distinguish between huge similar areas on the digital video frame. However, Li *et al.* [58] provided a method to detect the duplicated frames in the digital videos based on fingerprints in digital video sub-

sequence. In this method, DCT coefficients of the frames of video sub-sequences have been used to extract these fingerprints. It has focused on improving fingerprints in video sub-sequences so that similar video sub-sequences can be detected. This method has not detected the frame duplication at different locations in the digital videos. Xu *et al.* [118] provided an approach to identify the effects of CKF in the digital video. The authors have extracted the features of quantization of DCT coefficients for detecting the CKF forgery in the digital videos. The DA of this approach is quite low. Therefore, there is a need to increase DA for detecting CKF forgery in the digital videos. Furthermore, Bozkurt *et al.* [6] described a method for detecting the forged frames in the digital video. This method has extracted binarized DCT features from the frames and represented their similarity. This method has not worked to detect frame duplication of different frame sequences in the digital video. Fadl *et al*. [25] described a technique for detecting the frame duplication in the digital videos based on the standard deviation of residual frames. Standard deviation of residual frame has been used to select few frames, whereas other frames have been ignored in this technique representing a static scene. After that, the entropy of DCT coefficients has been computed to represent its discriminating feature for each selected residual frame. Then, analysis of subsequence feature has been used to detect the duplicated frames in the digital videos.

2.2.1.2 Correlation Based Technique

There are some techniques based on CC for the detection of CM forgery in the digital videos. Wang *et al.* [112] have provided two methods. The first method is used to detect the frame duplication typed forgery in digital videos. The second is used to identify the region duplication within the digital video frames using spatial and temporal correlation features. The detection of duplicated frames is based on the correlation between all frames of the digital videos. The duplicated frames are detected by comparing the CC of a video subsequence using threshold. There is a scope to increase the detection accuracy. The CC is given as below:

$$\mathrm{CC}\,(\overrightarrow{p},\overrightarrow{q}) = \frac{\sum_i (p_i - \mu_p)(q_i - \mu_q)}{\sqrt{\sum_i (p_i - \mu_p)^2 \sum_i (q_i - \mu_q)^2}} \tag{2.2.2}$$

where, p_i is element of vector $\overrightarrow{p}$, q_i is element of vector $\overrightarrow{q}$, μ_p is mean of vector $\overrightarrow{p}$, μ_q is mean of vector $\overrightarrow{q}$ and $\mathrm{CC}\,(\overrightarrow{p},\overrightarrow{q})$ is correlation coefficient.

In the second method, a pair of frames have been taken to estimate a spatial offset corresponding to a duplicated region between them. This method has used phase correlation for this estimation. For each spatial offset, the correlation between the frames has been found to determine an offset value for a duplicated region in the digital video frame. These methods have not detected the

region duplication from other frame and frame duplication at different locations. However, Hsu *et al*. [32] described an approach for the region duplication detection. The correlation of noise residue is used as features to identify the forged regions in the video using Gaussian Mixture Model. This approach has found optimal threshold value based on the estimated parameters using Bayesian classifier. It has worked only on static background videos.

Moreover, Singh *et al*. [91] provided an approach for detecting the frame duplication forgery in the digital video. This approach has used correlation between suspicious frames as a feature. This approach fails when frame duplication has been done in different order and different frame sequences. Bagiwa *et al.* [5] designed a technique for detecting CKF in the digital video. This technique has analyzed the correlation of blurring artifacts for detecting the forged foreground in the current frame of the digital video. There is a scope to increase its DA.

There are following steps to calculate the correlation coefficients.

1. Calculate the mean $\bar{x}$ of all of the first coordinates of the data x_i.
2. Calculate the mean $\bar{y}$ of all of the second coordinates of the data y_i
3. Calculate s_x standard deviation of all of the first coordinates of the data x_i.
4. Calculate s_y standard deviation of all of the second coordinates of the data y_i.
5. Calculate $(z_{xi}) = {(x_i - \bar{x})}/{s_x}$ for each x_i.
6. Calculate $(z_{yi}) = {(y_i - \bar{y})}/{s_y}$ for each y_i.
7. Perform the multiplication of corresponding values as $(z_{xi}) \times (z_{yi})$.
8. Add the products from step 7.
9. Divide the sum by n – 1, where n is the total number of points in a data sequence.

The result of this is the correlation coefficient r. For example, data is given as [x=1, 2, 4, 5] and [y=1, 3, 5, 7]. Now, the mean of x and y are $\bar{x}$ = 3 and $\bar{y}$ = 4. The standard deviation s_x = 1.83 and s_y = 2.58.

10. The sum of the products in the rightmost column is 2.969848. Here, n-1= 4-1=3. Therefore, the sum of the products is divided by 3 which results the correlation coefficient value is 2.969848/3 = 0.989949.

2.2.1.3 Histogram of Oriented Gradients (HOG) Based Technique

In some techniques, HOG features have been used to detect CM forgery in the digital videos. Firstly, a frame is represented by a set of local histograms. These histograms are used to count

the occurrences of gradient orientation in a region of frame. The region of frame is known as cell whose size may vary. Now, for extracting HOG features, the gradients of a frame are computed by making a histogram of orientation at each cell. Then, the histogram, which is obtained from each cell of a frame-block, is normalized for getting the HOG descriptor of that block.

Subramanyam *et al.* [92] provided a method based on HOG feature matching and properties of video compression for the detection of CM forgery. In this, the RGB frame is converted into the grayscale frame for gradient computing by convolving the frame with horizontal and vertical masks [1 0 1] and $[-1\ 0\ 1]^{T,}$ respectively. The orientation is calculated at each pixel using the ratio of gradients in horizontal and vertical directions. Then the frame is divided into overlapping blocks L × L which are further divided into M × M cells. Each pixel of cell calculate its weighted vote which is gradient magnitude at that pixel. HOG features, extracted from each cell of each block, are matched with extracted HOG features of remaining blocks for the detection of CMRD in the digital videos. It does not detect region duplication from other frame of the digital video. Also, this method does not detect the frame duplication of different frame sequences in the digital video.

Furthermore, Lin *et al.* [52] provided a technique for detecting the duplicated frames in the digital videos. This technique consists of candidate clip selection, spatial correlation calculation and frame duplication classification. The histogram difference of two adjacent frames has been computed to find the duplicated candidates in the temporal domain.

A block-based algorithm has also been used to measure the similarity between the query clip and the candidate one in this technique. This technique cannot detect the shuffled and disorder frame sequence in the digital videos. Zhao *et al.* [130] presented a method for detecting inter-frame forgeries in the digital videos. This method uses Hue-Saturation-Value (HSV) color histogram comparison and Speeded Up Robust Features (SURF) feature extraction. These have been organized with Fast Library for Approximate Nearest Neighbours (FLANN) matching for its double-checking. In this, H-S and S-V color histograms have been calculated for each digital video frame. The similarities between histograms have been compared for detecting and localizing the tampered frames.

There are following steps for calculating the HOG features as below:

1. Firstly, take the input image for the calculation of HOG features and resize this image into an image of 128×64 pixels for getting better results.

2. Now calculate the gradient of image. The gradient is obtained by combining magnitude and angle from that image. Considering a block of 3x3 pixels, first G_x and G_y is calculated for each pixel using following eq.

$$G_x\ (r,c) = I(r,c+1) - I(r,c-1)$$

$$G_y\ (r,c) = I(r-1,c) - I(r+1,c)$$

where r, c refer to rows and columns

After calculating G_x and G_y , magnitude and angle of each pixel is calculated using the formulae as mentioned below:

$$\text{Magnitude} = \sqrt{G_x^2} + G_y^2 \quad \text{and}$$

$$\text{Angle} = |tan^{-1}(G_y / G_x)|$$

3. After getting the gradient of each pixel, the blocks are made by dividing the gradient matrices into 8x8 cells. Now, a 9-point histogram is calculated for each block. This 9-point histogram generates a histogram having 9 bins. Each bin has an angle range of 20 degrees. Each of these 9-point histograms can be plotted as histograms with bins which show the intensity of the gradient in that bin. There are 64 different values in a block for which the following calculation is performed. As 9 point histograms are using here. Hence,

Number of bins=9 (ranging from $0^0\ to\ 180^0$)

Step size ($\Delta\theta$) = 180^0/ Number of bins = 20^0

Each j^{th} bin, bin will have boundaries from:

$$\Delta\theta.\,j, \Delta\theta.\,(j+1)$$

Value of the centre of each bin will be:

$$C_j = \Delta\theta.\,(j+0.5)$$

4. In a block, the j^{th} bin will be calculated for each cell, then the value will be provided to j^{th} and$(j+1)^{th}$ bin respectively. This value is given as follow:

$$j = \lfloor(\frac{\theta}{\Delta\theta} - \frac{1}{2})\rfloor$$

$$V_j = \mu[\left(\frac{\theta}{\Delta\theta} - \frac{1}{2}\right)]$$

$$V_{j+1} = [\mu.\frac{\theta - c_j}{\Delta\theta}]$$

5. An array is taken as a bin for a block and values of V_j and V_{j+1} is added in the array at the index of j^{th} and$(j+1)^{th}$ bin calculated for each pixel.

6. The resultant matrix after the above calculations will have the shape of 16×8×9.

7. When the histogram computation is completed for all blocks, then 4 blocks are clubbed together to make a new block (2x2) from the 9 point histogram matrix. This clubbing is finished in an overlapping manner with a stride of 8 pixels. For all 4 cells in a block, all 9 point histograms are concatenated for each constituent cell to make a 36 feature vector. f_b is a feature vector.

8. Values of f_b for each block is normalized by the L2 norm:

$$\text{fbi} \leftarrow \frac{\text{fbi}}{\sqrt{||\text{fbi}|+\quad \epsilon|^2}}$$

Where ε is a small value added to the square of f_b in order to avoid zero division error.

9. To normalize, the value of k is first calculated as below:

$$k = \sqrt{b_1^2 + \quad b_2^2 \quad + \quad + \ldots\ldots\ldots + \quad b_{36}^2}$$

$$\text{fbi} = \left[\left(\frac{b_1}{k}\right) + \left(\frac{b_2}{k}\right) + \left(\frac{b_3}{k}\right) \ldots\ldots\ldots\ldots \left(\frac{b_{36}}{k}\right)\right]$$

10. This normalization is completed for reducing the effect of changes in contrast between images of the same object. A 36 point feature vector is collected from each block. There are 7 blocks in the horizontal direction and there are 15 blocks in the vertical direction. Therefore, the total length of HOG features will be 7×15 × 36 = 3780. Thus, HOG features of the selected image are calculated.

2.2.1.4 Discrete Wavelet Transform (DWT) Based Technique

In this technique, the frames have been extracted from digital video and converted into grayscale frames by Karthikasini *et al.* [47]. DWT decomposes these grayscale frames into four-level decomposition for getting the wavelet coefficients. The shrinkage filter is applied on the high frequency wavelet coefficients to perform the threshold. This threshold produces the new low-frequency coefficients, which are useful for reconstructing the frame using inverse

DWT. This reconstructed frame is a de-noised frame that is subtracted from the grayscale frame to get the noise residue. This process is repeated for all frames of the digital video. The noise residue video frames are divided into several blocks. Then, noise correlation values at block level are calculated for finding the similarities between blocks.

Yadav *et al*. represents a method for detecting the CMRD which is based on DWT. In this method, for making a reduced dimensional representation, DWT is applied to the input image. Then, the overlapping blocks are obtained by dividing the image. After sorting these blocks, the duplicated blocks are detected. Thus, the CMRD has been detected on the lowest level image representation using DWT. Li et al. provided a technique for the detection of duplicated regions based on DWT and Singular Value Decomposition (SVD). In this technique, DWT tis used to decompose the image into four sub-images for getting Lower sub band. The most of the information is available in this band only. SVD is used for reducing the dimension in this area. After that, lexicographical sorting is implemented to detect the forged area.

Zhang et al. described a DWT based scheme for detecting the CMRD forgery in which the DWT is used to reduce the dimension of input image. Then, phase correlation is applied to compute the spatial offset between regions. After that, pixel based matching algorithm is implemented to detect forgery. Zimba et al. presented a technique in which DWT is applied on the input image to reduce its dimension. In this technique, a suitable size block is moved to form overlapping blocks over the low-frequency band of the image. Then, PCA is applied to each block for reducing the dimension of the feature vector. After lexicographically sorting of blocks, the normalized shift vector and offset frequency are calculated. This offset frequency is subjected to morphological processing to find the forgery. Fattah et al. presented a method for the detection of CMRD forgery which is based on 2D DWT. In this method,2D DWT is implemented on input image, Then, DWT coefficients are gathered from LL band. This band is splitted containing overlapping and non-overlapping blocks. Candidate blocks are selected from non-overlapping blocks. Overlapping blocks are compared with the selected candidate blocks using Euclidean distance for detecting CMRD forgery.

2.2.1.5 Local Binary Pattern (LBP) Based Technique

Local Binary Pattern is a common texture descriptor used to investigate the CM forgery in the digital videos by Kharat *et al*. [47]. It is robust against the monotonic illumination changes and variation in contrast. However, it is sensitive to noise and small fluctuations in gray-level. Saddique *et al.* [95] has presented a robust texture descriptor named Chrominance value of Consecutive frame Difference and Discriminative Robust Local Binary Pattern (CCD-DRLBP)

which provides both texture and edge information into a representation. This representation indicates discontinuities and inconsistencies in the form of edges, lines, and corners in the difference of consecutive frames which arise during forgery. The research discovered a descriptor based on chrominance value of consecutive frame difference and discriminative robust LBP, which extracts the discriminant features for detecting CM forgery.

Moreover, Uliyan *et al.* [107] provided a method for detecting region duplication in the digital image. In this method, the colour based segmentation and Local Binary Pattern of colour pixels have been used to extract features from the digital image. All extracted LSBs have been used to generate the image signature. This method has not worked on detecting region duplication from other images. Ulutas *et al.* [106] provided a method for detecting frame duplication which extracts the binary features from video frames. Then the Euclidean distance between features has been used to judge the similarity between frames. After that, PSNR values has been computed between similar frames to identify the identical frames.

2.2.1.6 Color/Intensity Based Technique

Few techniques have been used color/intensity variation as a feature to detect the CM forgery in the digital videos. Anshida *et al.* [1] have provided a method based on the variation in color or intensity in digital video frames. This method has extracted several frames from the digital video and divided them into several blocks. From these blocks, the average intensities of RGB components of each pixel are calculated for decreasing the noise. Then, normalization operation is performed and feature set is created for a digital video. The feature set of each digital video are compared with that of other digital videos. After comparing, the matched feature set of digital video is given as an output and forgery is detected. This forgery detection is based on video sequence matching. Su *et al.* [89] have located and detected the forgery by computing the optical flow coefficient of the suspicious object. An approach has also been provided by Wu *et al.* [111] for detecting video inter-frame forgery based on the consistency of velocity field. Some discontinuous peaks are attained in velocity filed sequence due to frame duplication and deletion operations. These discontinuous peaks are extracted by generalized extreme studentized deviate test to detect and locate the tempered regions in forged videos. This approach has only been worked for static surveillance videos.

Moreover, it has not been computed the execution time for its efficiency. Wang *et al.* [113] presented a technique based on optical flow for detecting the inter-frame forgery in the digital videos. This technique detects the continuity points to the optical flow variation sequence which

indicates different characteristics of forgery. It has also adopted the anomaly detection scheme for distinguishing the discontinuous points in the digital videos.

Furthermore, Bidokhti *et al.* [9] described a technique for CM forgery detection in digital videos in which each video frame has been divided into suspicious and innocent parts. After this division, the optical flow coefficient has been computed from each part. Then an unusual trend has been detected in the optical flow coefficient of the suspicious object for locating the forgeries. The performance of this technique is decreased with high motion digital videos. Kingra *et al.* [45] provided a technique for detecting inter frame forgery. This technique has used prediction residual and optical flow inconsistencies as features for detecting frame addition, deletion and frame duplication. This method has not worked to detect CMFD at different locations in the digital video. Liu *et al.* [51] described a technique to detect the CKF in three ways: foreground block extraction, forged block detection, and forged block tracking. First, foreground blocks are extracted from the current frame using the multipass foreground locate method. In the second way, local features of luminance and contrast are used for computing the correlation in background and foreground. After that, altered foreground and altered frame are sought out.

At last, tampered block is tracked. This method is failed to locate the forged regions of small size. Lichao *et al.* [59] described a method for detecting video foreground forgery. It has computed the energy factor of each frame for identifying these forged frames. Then an adaptive parameter-based visual background extractor algorithm is used for detecting the suspected regions in the forged frames of digital videos. After that, the difference of energy factor (EF) between suspected regions in the forged frames and corresponding regions in the authentic frames have been discovered. At last, this method has located the tampering in digital video forged frames.

2.2.1.7 Double Quantization Based Technique

This technique has been exposed the video forgery by detecting the double quantization in digital videos. Yao *et al*. [121] have presented a double-compression detection method. The periodic features of the string of data bits and the skip macroblocks are analyzed for all I-frames and P-frames in a double-compressed H.264/AVC video. For a suspicious video, the string of data bits and the skip macroblocks are extracted for each frame. After that, both features are merged to create an enhanced feature that represents the double-compressed video's periodic artefact. At last, the periodicity of features has been detected by a time-domain analysis.

Moreover, Wang *et al.* [115] have analyzed the histogram of double quantized DCT coefficients of each macro-block. A detection function was defined in this technique using experimentally

selected threshold of 0.1. This technique has been examined on 100 digital videos by bit-rates from 4 Mbps to 8 Mbps with an average True Positive Rate of 93.4%.

2.2.2 Key Point Feature Techniques

In key point feature techniques, features are extracted and matched within the entire video frame to identify the forged part in the digital videos which are given as below:

2.2.2.1 Scale-Invariant Feature Transform Based Technique

Scale-Invariant Features Transform (SIFT) provides a way to extract distinctive invariant features from video frames which can be utilized to find the reliable matching between different views of an object.

Pandey *et al.* [76] have presented a technique based on SIFT for detecting CM forgery in the digital videos. In this technique, the SIFT features have been used to find intra-frame forgery in the digital videos. These features remain invariant if a region is manipulated using geometrical transformations or other transformations. Here, noise residue and correlation technique are used to detect inter-frame forgery. However, this technique has not detected the shuffled and disorder frames in the digital videos, decreasing its DA. Ulutas *et al.* [108] have provided a technique for detecting the frame duplication based on the Bag-of-Words model. It is a model used in textual analysis and then for image and video retrieval. It creates visual words and generates a dictionary from SIFT keypoints of video frames in the digital video. Then this method computes thresholds to improve the robustness and its performance. This method has been worked on fewer digital videos and has not also been detected the inter-frame forgery at different locations in the digital videos.

Furthermore, Yang *et al*. [123] provided a method for CM forgery detection. In this method, a modified SIFT-based detector detects key points. Strategy of key-points distribution has been established for interspersing the key-points on an image. This method has detected the similarities between the same objects within the image, but it has not detected the duplicated object from another image. Kharat *et al.* [47] provided a method for detecting frame duplication in digital video. In this method, the suspicious frames have been considered candidate frames and recognized by motion vector in the digital videos. For comparing the suspicious frames, SIFT features have been used. At last, Random Sample Consensus has been used to detect and locate duplicate frames. However, the DA of this method is quite low.

2.2.2.2 Speed Up Robust Features (SURF) Based Technique

Pandey et al. [77] have provided a technique based on SURF descriptor. This descriptor has used the integral images for reducing the computational time. SURF descriptor is consists of feature extraction and feature description. In the feature extraction, Hessian Matrix approximations have been used for the interest point detection. The Hessian matrix H(x,δ) is defined for a point X = (x, y) of an integral image I at scale δ as follows [77]:

$$H(s,\delta) = \begin{bmatrix} L_{x\,x}(X,\delta) & L_{x\,y}(X,\delta) \\ L_{x\,x}(X,\delta) & L_{y\,y}(X,\delta) \end{bmatrix} \quad (2.2.3)$$

where, $L_{x\,x}(X,\delta), L_{x\,y}(X,\delta), \text{and } L_{y\,y}(X,\delta)$ are the convolution of the Gaussian second-order derivative $\frac{\partial^2}{\partial x^2}$ with an image I at point X.

The box filters of 9 × 9 are approximations for Gaussian second-order derivatives with σ = 1.2, representing the lowest scale. In the feature description, a reproducible orientation is fixed based on the information from a circular region around the key point. Then, a square region is aligned to the selected orientation for extracting the feature descriptor. For this, a square region is centred at the interest point for calculating the descriptor and the orientation is divided into 4 × 4 square sub-regions. For each sub-region, the response of Haar wavelet in horizontal direction (dx) and vertical direction (dy) is recorded with a filter at 5×5 regularly spaced sample points. Then, the wavelet responses dx and dx are summed up for making the feature vector. Also, the absolute values of the responses |dx| and |dy| are summed up for taking the information about polarity of intensity changes. Each sub-region has a four-dimensional descriptor vector v for its underlying intensity structure as follows [77]:

$$v = \sum dx, \sum dy, \sum |dx|, \sum |dy|$$

This results in a descriptor vector for all 4×4 sub-regions of length 64. The wavelet responses are invariant to a bias in illumination (offset). Invariance to contrast (a scale factor) is achieved by turning the descriptor into a unit vector. There are few techniques based on deep learning to detect CM forgery in the digital videos.

Thakur et al. [104] designed a model that classifies the objects using learning features. This technique is also based on a convolutional neural network (CNN) to recognize inter casing replica in the digital video. Furthermore, Fadl *et al.* [26] have represented a technique based on 2D-CNN of Spatio-temporal information and fusion for deep feature extraction. This technique has been detected inter frame forgeries in the digital video. Bakas *et al.* [10] have provided a technique for detecting the frame insertion, deletion, and duplication in the digital video using

3D-CNN. In this technique, a difference layer in the CNN has been introduced to extract the temporal information from the digital videos, which provides efficient support for detecting these inter-frame forgeries in the digital videos. Long et al. [62] have presented a novel coarse-to-fine framework based on DCNN for detecting and localizing CMFD forgery automatically. Firstly, the coarse-level matches between candidate duplicated frame sequences and the corresponding selected original frame sequences have been found by an I3D network. After that, fine-level correspondences between an individual duplicated frame and the corresponding selected frame have been identified by a Siamese network based on ResNet architecture. Also, a video-level score indicating the likelihood of forgery has computed by a robust statistical approach. In this, authors have developed an inconsistency detector based on the I3D network for distinguishing the duplicated frames from the selected original frame. In [49], authors have provided a method for the exposure of inter-frame tampering in the videos DCNN. This method has been classified the forged frames on the basis of the correlation for getting irregularities using DCNN. The training swiftness has improved by decoders which are used for batch normalization of input. In [122], the authors have presented a deep learning-based approach for detecting the object-based forgery in the advanced video. The video frames have been passed through three pre-processing layers then these are fed into CNN model. In this, for achieving a similar number of positive and negative image patches before the training, an asymmetric data augmentation strategy has been used.

2.3 Edge Detector

Su *et al.* [89] have presented a technique for detecting CKF forgery based on edge features. This technique has been used object segment technique for extracting the objects. Then the edge points of each object have been located using Prewitt edge detector. This technique has shown very weak edge points of identified forged object and some edge points of background which is not desirable. Its DA is quite low and also not immune to attacks.

On the other hand, in the literature, there is a canny edge detector with a multi-stage algorithm which detects a wide range of edges in the digital images [14]. Juneja et al. [37] have presented the performance evaluation for edge detection of an image in which Sobel, Prewitt, and Roberts provide the low quality edges whereas, canny method have detected strong and weak edges of that image. Katiyar et al. [44] have described the comparative analysis of edge detection techniques. This analysis has provided that canny edge detector can be used to extract the objects with feeble edges. Sobel edge detector is efficient as canny edge detector but it also provides more false edges. On the other side, Robert and Prewitt edge detectors have failed in

the case of smaller features. Bhardwaj et al. [11] have analyzed the various edge detector techniques that result in the good performance of canny edge detector.

A grayscale frame is applied to the canny edge detector as an input which generates the edge frame as an output [43]. In a canny edge detector, a Gaussian filter is used to reduce the noise effects in a digital video frame and provides the smooth frame [21]. Then each smooth frame is applied to the 2-D first derivative operator, highlighting the regions with high first spatial derivatives [82]. A Gaussian filter kernel of size (2c+1) × (2c+1) is given by using Eq. (2.3.1) [43].

$$G_{ab} = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{\left(a-(c+1)\right)^2+\left(b-(c+1)\right)^2}{2\sigma^2}\right); \quad 1 \le a \le (2c+1) \tag{2.3.1}$$

where σ is standard deviation, $a-(c+1)$ is the distance from the origin in the horizontal axis, $b-(c+1)$ is the distance from the origin in the vertical axis, and G_{ab} is the 2D Gaussian filter.

After that, the edges are found by the edge detector where grayscale pixel values are mostly changed in the frame of digital video. These changes are discovered by calculating the gradients of each frame [69]. The gradients are determined at each pixel of frames using the edge detection operator which approximates the gradient in X-direction and Y-direction by applying the kernels as shown in Eq. (2.3.2) [12]

$$\mathrm{K_{GX}} = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \mathrm{K_{GY}} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \tag{2.3.2}$$

where $\mathrm{K_{GX}}$ is kernel for the gradient in X- direction and $\mathrm{K_{GY}}$ is kernel for the gradient in Y-direction. The magnitude of the gradient can be determined by the following Eq. (2.3.3) and (2.3.4) [110] such as

$$|\mathrm{G}| = \sqrt{\mathrm{G_X^2} + \mathrm{G_Y^2}} \quad , \tag{2.3.3}$$

$$|\mathrm{G}| = |\mathrm{G_X}| + |\mathrm{G_Y}| \tag{2.3.4}$$

where, $\mathrm{G_X}$ and $\mathrm{G_Y}$ are the gradients in X- direction and Y- direction respectively, $|\mathrm{G_X}|$ and $|\mathrm{G_Y}|$ are the magnitudes of gradients in X- direction and Y- direction respectively, $|\mathrm{G}|$is approximate gradient magnitude[110].

These gradients provide the edge strengths to each frame of a digital video. The directions of edges in each edge frame of a digital video are determined in X- direction and Y- direction by Eq. (2.3.5) [4].

$$\theta = \arctan\left(\frac{|\mathrm{G_Y}|}{|\mathrm{G_X}|}\right) \tag{2.3.5}$$

where θ is the angle of direction of the edge.

After detecting the edge direction, the non-maximum suppression is applied to trace the edge direction. It suppresses the pixel intensity value, which is not considered an edge in the Canny edge detector [4].

2.4 OTSU Method

In the literature, there are some existing techniques of CMRD and CKF forgery detection [89], [51] which have been used the fixed values of threshold for detecting these forgeries in the digital videos. However, OTSU method is a frequently used method which selects the global optimal threshold by maximizing the between-class variance. In this thesis, each edge pixel difference value is compared with threshold value T' to differentiate them into large and small edge pixel difference values. Due to large edge pixel difference values, a large threshold value is set by OTSU algorithm in the edge frame. Thus, a large number of edge pixel difference values are eliminated which are less than T', and keeps the left behind less amount of edge pixel difference values of forged foreground which are large than T'. Thus, this less amount of edge pixel difference values decreases the rate of large edge pixel difference values which identifies the forged frame. Thus, CM forgery is detected after calculation of optimal threshold.

Nobuyuki Otsu [68] has provided a automatic threshold selection method in a digital image. This method has been derived from discriminant analysis, which automatically selects threshold from a gray level histogram. Bangare *et al.* [3] have presented a review of the OTSU method in which it is observed that the OTSU method provides better results on several pixels. These pixels are very close to each other in each class. This method is the most referenced threshold method because it computes directly an optimized threshold value on the gray level histogram. Moreover, Kurita *et al*. [42] have provided performance analysis of an OTSU method. It is described that the OTSU method is the most frequently used threshold method due to its simplicity and effectiveness. The main idea of the OTSU method is to determine the optimal threshold value by maximizing the between-class variance. While the gray level distributions of foreground and background are Gaussian distributions having equal variance, then OSTU method provides effective performance on the real-world images. The OTSU method is described as below [68]:

I. Consider that pixels of a given image $g(x, y)$ are represented in K gray level, $g(x, y) \in [1, K]$. The number of pixels at level j is denoted by m_j and a total number of pixels by $M = m_1 + m_2 + m_3 + \cdots m_K$.The probability of occurrence of level j is given as, below:

$$p(j) = \frac{m_j}{M}:\ p(j) \geq 0,\ \sum_{j=1}^{K-1} p(j) = 1 \quad (2.4.1)$$

II. Now, dichotomize the pixels into two classes such as background C_0 and objects C_1 by a threshold at level T. C_0 represents the pixels with gray levels $[1, \ldots\ldots, T]$. C_1 represents those with gray levels $[T+1, \ldots\ldots, K]$. Then, the probabilities $\omega_0,\ \omega_1$ for the occurrence of each class is provided as follows:

$$\omega_0 = \sum_{j=1}^{T} p(j) \quad (2.4.2)$$

$$\omega_1 = \sum_{T+1}^{K} p(j) = 1 - \omega_0 \quad (2.4.3)$$

III. Compute the average gray level μ_0 of class C_0

$$\mu_0 = \sum_{j=1}^{T} j\frac{p(j)}{\omega_0} \quad (2.4.4)$$

IV. Compute the average gray level μ_1 of class C_1

$$\mu_1 = \sum_{j=T+1}^{K} j\frac{p(j)}{\omega_1} \quad (2.4.5)$$

V. The total average gray level μ_t of a given image

$$\mu_t = \sum_{j=1}^{K} (j(p(j))) \quad (2.4.6)$$

VI. The optimal threshold $T'$is given by

$$T' = \arg \max_{1 \leq T < K} \{\sigma^2(T)\} \quad (2.4.7)$$

where, the between-class variance $\sigma^2(T) = \omega_0(\mu_t - \mu_0)^2 + \omega_1(\mu_t - \mu_1)^2$

2.5 Histogram Equalization

Histogram Equalization (HE) is a digital image processing technique used to adjust the image's contrast using its histogram. It spreads out the most frequent pixel intensity values or stretches out the pixel intensity range to enhance the image's contrast. Xiong et al. [118] have specified that HE is generally used due to its effective performance for the image enhancement. It redistributes the pixel intensity values uniformly in a digital image for providing a higher contrast. This contrast is increased by taking transformation function as cumulative density function of that image. Kim et al. [41] have presented a technique based on HE for conserving the mean brightness of an input image. In this technique, the image histogram is divided into sub-images based on the input image's intensity mean value. After division, these sub-images are independently equalized for contrast enhancement. Dorothy et al. [71] have described a method based on HE to enhance the image's contrast. This method has been generally used to increase the global contrast of many images, while images have close contrast values. HE spreads out the most frequent pixel intensity values in this method and results in the lower

contrast area to gain a higher contrast. Therefore, this technique is utilized in the presented work of CMRD forgery detection. In the process of HE [40], probability density function (PDF) of each block is calculated firstly given as below:

$$P_L(F_f) = \frac{n_L^f}{n_L} \quad (2.5.1)$$

where f = 0,1,...,G and n_L is the total number of pixels from F_0 to F_G intensity levels. n_L^f is the total number of pixels having f gray level.

Cumulative density function (CDF) is then defined as

$$C_L(F_G) = \sum_{f=0}^{G} \left(P_L(F_f)\right) \quad (2.5.2)$$

Transform function in terms of CDF is given as below:

$$C_L(F_f) = \left(F_0 + (F_G - F_0) * C_L(F_f)\right) \quad (2.5.3)$$

Therefore, the output image Y can be obtained as follows:

$$Y = T''[g(x,y)] \ \forall (x,y) \in g \quad (2.5.4)$$

where $g(x,y)$represents every pixel in the image g, and (x, y) indicates the coordinates.

2.6 Important Definitions

The following definitions used in work carried out in this thesis are given in this section.

Coefficient of Variation (CV): CV is used in the work of detecting the CMFD and CMRD forgeries in the digital videos which is defined by [70]:

$$CV = \frac{\sigma}{\mu} \quad (2.6.1)$$

where, CV is coefficient of variation, σ is standard deviation of a frame sequence and μ is mean of a frame sequence.

Structural Similarity Index (SSIM): SSIM is used to measure the similarities between two regions that is defined as follows [29], [65]:

$$\text{SSIM (m,n)} = \frac{(2\mu_m \ \mu_n + K_1)}{(\mu_m^2 + \mu_n^2 + K_1)} \frac{(2\sigma_{mn} + K_2)}{(\sigma_m^2 + \sigma_{Yn}^2 + K_2)} \quad (2.6.2)$$

where, μ_m is the average pixel value of m region, μ_n is the average pixel value of n region, σ^2_m is the variance of m region, σ^2_n is the variance of n region, and σ_{mn} is the covariance of m and n regions.

Mean Square Error (MSE): MSE is utilised to identify an error between two blocks that is provided as below [29], [105]:

$$\mathrm{MSE}(P,Q) = \sum_{d=1}^{R} \sum_{d=1}^{R} |\ P(d,e) - Q(d,e)|^2 / R \times R \qquad (2.6.3)$$

where, MSE(P, Q) denotes MSE between two blocks P and Q and R × R is the size of block, (d, e) indicates the pixel coordinates of blocks.

Some points are observed after the study of various existing techniques of CM forgery detection in the digital videos. A summary of the prevailing literature for CMFD, CMRD and CKF forgeries detection techniques in digital videos is provided in Table 2.1.

Table 2.1: Summary of literature review for CM forgery detection techniques in digital videos

Ref. No.	Kind of Forgery	Features used	Limitations
[5]	CKF	Correlation of blurring artifact	There is a need to increase the detection accuracy.
[89]	CKF	Change of correlation between the color signals	This method does not provide the complete edge information. Therefore its detection is weak.
[118]	CKF	Quantized DCT coefficients	The detection accuracy of this approach is low. There is a need to increase its detection accuracy.
[51]	CKF	Local features of luminance and contrast	There is scope of increasing the detection accuracy.
[126]	Frame insertion and deletion	CC	Its performance decreases while the number of frames deleted is less than length of deleted frame sequence.
[28]	Frame insertion and deletion	Variation of Prediction Footprint (VPF)	This method is failure to detect the frame alteration while entire Group of Pictures (GOP) is removed or inserted by attacker
[119]	Frame deletion	Variation in prediction residual	This method failed to detect the frame deletion with slow-motion videos.
[111]	Frame deletion and CMFD	Consistency of velocity field intensity	This technique has only worked on static surveillance cameras and does not compute the execution time.

Ref. No.	Kind of Forgery	Features used	Limitations
[52]	CMFD	Spatial and temporal analysis	The computational time in frame/sec of this approach is large which decreases the efficiency of this approach.
[54]	CMFD	Tamura texture features	This technique has large computational time and has not worked with moving camera digital videos.
[91]	CMFD	Correlation between suspicious frames	This method has not detected CMFD at different locations in the digital videos and its performance is decreased with compression.
[54]	CMFD	Zernike opponent chromaticity moments (ZOCM) and Tamura coarseness feature	This method does not work to detect CNFD at different locations in the digital video.
[47]	CMFD	SIFT key-points	It does not work for detecting the shuffled frame sequence.
[76]	CMRD and CMFD	SIFT features and noise residue and correlation technique	It has not detected CMRD within small size. This technique is not capable to detect the shuffled and disorder frame sequences.
[55]	CMFD	Temporal similarity measurement strategy	It cannot detect the shuffled and disorder frame sequence.
[32]	CMRD	Temporal noise	It works only on static background videos.
[112]	CMFD and CMRD	Spatial and temporal correlation	This method failed to detect the frame duplication in videos captured by moving camera.
[120]	CMFD	Similarity measurements	It does not work to detect CMFD at different locations in the digital videos.

Ref. No.	Kind of Forgery	Features used	Limitations
[6]	CMFD	Binarized DCT features	It does not work to detect CMFD at different locations in the digital video.
[94]	CMRD	Mirror invariance	This method does not detect the region duplication from other frames, and most of the work has been done to detect large-sized regions.
[92]	CMRD	HOG	This method does not detect CMRD from other frame in the digital videos. Its performance is affected by the compression.
[7]	CMRD	Analysis of residual computed between adjacent frames	It has not detected CMRD forgery from the other frame in the digital video. The detection of this technique is decreased with the compression.
[58]	CMRD	Polar Harmonic Transform (PHT)	It cannot detect too small duplicated region.
[25]	CMFD	Temporal average and statistical textural features	It does not detect the disorder frames in the digital videos.
[129]	Frame insertion, deletion and CMFD	Similarity analysis between H-S and S-V color histograms	This method fails to detect complex inter-frame forgery with many shots in a video.
[107]	CMRD	Colour based segmentation and Least Significant Bit of colour pixels	This method does not work on the CMRD from other images.
[113]	Frame insertion and deletion	Optical flow consistency	This technique does not work on RGB frames.
[9]	CMRD	Optical flow and optical flow variation factor	The performance of this technique is decreased with high motion videos.
[106]	CMFD	Binary features	This method cannot detect shuffled and disorder frames in the digital videos.

Ref. No.	Kind of Forgery	Features used	Limitations
[45]	Frame insertion, deletion and duplication	Prediction residual and optical flow inconsistencies	This technique has not worked to detect frame duplication of different frame sequences in the digital video.
[59]	Forged foreground detection	EF and adaptive parameter-based visual background extractor algorithm	It can only locate part of the tampering traces, instead of the complete tampered regions.
[115]	CMRD	Double quantization	It does not work with videos captured by a moving camera.
[83]	CMFD	Improved levenshtein distance	It does not work for detecting the shuffled frame sequence.
[96]	CMFD	Polar cosine transform	This technique does not detect the shuffled and disorder frame sequences in the digital videos.
[39]	CMRD	Noise characteristics	It works only on Static digital videos.
[38]	CMRD	Temporal noise	This method failed to work with videos having moving scene.
[97]	Frame deletion	Motion-compensated edge artifact	This approach is not suitable for video sequences having low motion.
[15]	CMRD and CMFD	Noise residue features	There is need for evaluating more parameters.
[98]	Frame insertion and deletion	Features of power of high frequency area	This method cannot detect the breakpoint.
[99]	Frame insertion and deletion	P-frame prediction error	This method is sensitive to noise.
[16]	Frame insertion & deletion	Optical Flow Coefficient (OFC)	It is not suitable for digital videos with moving background.
[60]	CMRD	Analysis of spatial and temporal slices	This method does not work with videos captured by moving camera.

Ref. No.	Kind of Forgery	Features used	Limitations
[116]	Frame insertion, delete and CMFD	Optical flow	It failed to work with moving camera digital videos.
[100]	CMRD	K-singular value decomposition (K-SVD)	This method cannot detect the forged regions of small size.
[128]	Frame insertion and deletion	Block-wise brightness variance descriptor	The detection accuracy of this method is decreased with fewer frames insertion.
[129]	CMFD and CMRD	Motion vector pyramid and its variation factor	This technique cannot detect forgery in digital videos having moving backgrounds.
[17]	CMRD	Motion residuals	This method does not detect the CMRD from another frame in the digital video.
[81]	CMRD	Curvelet transform	This technique has detected duplicated region in the digital images.
[31]	CMFD	DCT coefficients	This method has detected frame duplication in the digital videos.
[61]	Frame insertion and deletion	Consistency of quotient of mean structural similarity	This method fails to detect complex inter-frame forgery with many shots in a video.
[123]	CMRD	Modified SIFT based detector	This method has detected forged region in the digital videos.
[13]	Frame insertion, deletion and CMFD	Haralick coded frame correlation	This approach has not detected the shuffled and disordered frame sequences.
[114]	Frame insertion, deletion and CMFD	Multi-scale normalized mutual information descriptors	This method does not work for CMFD at long continuous location of frame sequence in the digital video.

Most of techniques have been detected CMFD forgery with small frame length. However, these techniques have not detected the CMFD forgery at different locations. They cannot detect the shuffled and disorder frame sequences in the digital videos. The performance of some techniques has decreased if the number of duplicated frames are less than considered frame sequence. On the other hand, the existing techniques have not detected CMRD forgery from another digital video frame. These techniques are also disabled to detect CMRD forgery within different shapes and size in the digital videos. Similarly, there are very few techniques for detecting CKF forgery. The detection of these techniques is quite low and is also not immune against the attacks.

2.7 Performance Metrics

It is observed that the performance of each existing technique has been evaluated qualitatively and quantitatively in the literature. The qualitative analysis involves the experimental detection results in the visual form whereas, the quantitative analysis compares existing techniques in the form of performance metrics. Therefore, the performance metrics are used to show the effectiveness of the presented work in which the following parameters are used for CM forgery detection.

Precision Rate: Precision Rate (PR) indicates the rate of detected authentic digital videos by the proposed approach which is given as follows [18], [84] and [114]:

$$\mathrm{PR} = \frac{\mathrm{TP}}{\mathrm{TP+FP}} \tag{2.7.1}$$

TP means that authentic digital video is detected as authentic and FP means that authentic digital video is detected as forged digital video [23], [34].

Recall Rate: Recall Rate (RR) shows the rate of detected forged digital videos by the proposed approach which is given as [17], [18], and [84]:

$$RR = \frac{\mathrm{TP}}{\mathrm{TP+FN}} \tag{2.7.2}$$

where, TP means that authentic digital video is detected as authentic and FN means that forged digital video is detected as authentic digital video [23], [34].

Detection Accuracy: Detection Accuracy (DA) represents the percentage of correct detection in the presented work which is provided by [114], [120]:

$$DA = \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}} \tag{2.7.3}$$

TP + TN means the total number of detected digital videos by the proposed approach and TP + TN + FP + FN means the total number of digital videos in the experiments [23], [34].

F measure: F measure is a measurement of search effectiveness which considers both PR and RR to compute F1 (β=1) and F2 (β=2) score, given as below [2], [17], [18], and [124]:

$$F_{\beta} = (1 + \beta^2) \frac{PR \,.RR}{(\beta^2 \,.PR)+RR} \tag{2.7.4}$$

where, PR indicates the Precision Rate and RR represents Recall Rate.

False Positive Rate: False Positive Rate (FPR) represents the percentage of digital videos, which are incorrectly identified as forged digital videos and calculated by [19]:

$$FPR = \frac{FP}{FP+TN} \tag{2.7.5}$$

False Negative Rate: False Negative Rate (FNR) represents the percentage of digital videos, which are incorrectly identified as authentic digital videos, and computed by [19]:

$$FNR = \frac{FN}{FN+TP} \tag{2.7.6}$$

Sensitivity: Sensitivity measures the actual positives which are correctly identified by the proposed approach and it is also called True Positive Rate (TPR) given as [75]:

$$Sensitivity = \frac{TP}{TP+FN} \tag{2.7.7}$$

Specificity: Specificity is the measurement of correct identification of actual negatives by the proposed approach and it is also called True Negative Rate (TNR) which is provided by [75]:

$$Specificity = \frac{TN}{TN+FP} \tag{2.7.8}$$

Execution Time: Execution time is a parameter which measures the time of execution of a technique in sec/frame.

2.8 Digital Video Dataset for CM Forgery Detection

SULFA dataset [22] is mostly used to detect CM forgery in the digital videos. In this dataset, 102 digital videos have taken with different three digital cameras such as CANON SX200, FUJIFILM 2800 and NIKON S3000. There are different kinds of digital videos in this dataset like static camera digital videos with stationary and moving objects, moving camera digital videos with stationary and moving objects, surveillance digital videos, digital videos with camera zoom in-out function, digital videos with different environmental conditions as fast raining, strong wind, cloudy and light effected digital videos. Each digital video in SULFA dataset is 10 seconds long, with a frame rate of 30 fps and has a resolution of 320 × 240. The

digital videos downloaded from the internet [72] are also used in performance evaluation. A generated dataset consists of digital videos taken from the SULFA dataset and the internet in the dataset and setting. Some digital videos constitute the training dataset for training purposes, and the remaining digital videos of a generated dataset have been used as a testing dataset for testing purposes. The testing dataset is further divided with 50:50 ratio into authentic digital videos and forged digital videos for evaluation. There are different digital videos with different lengths in the dataset. Each digital video has different bitrate. It has been noted that the bitrate of an authentic digital video is same after the manipulation in that digital video.

2.9 Research Gaps

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

- Most existing CM video forensic techniques do not detect the frame duplication of different frame sequences in the digital video.
- The existing CMRD detection techniques do not detect the region duplication from another digital video frame.
- There is a scope to improve DA of video forensic techniques against the CKF forgery.
- The previous techniques failed to detect the frame duplication if a copied set of frames are shuffled or reversed before moving them on different positions in the video.
- The performance of some of previous techniques decreases with fewer frames insertion. In some techniques, their performance decreases if the number of deleted frames is less than the length of deleted frame sequence.
- Some techniques have not been worked with the videos captured by moving cameras.
- The performance of some previous techniques is decreased with compression.
- Some existing techniques failed to detect the small size regions in the video.

2.10 Research Objectives

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

1) To study and analyze the existing Copy-Move video forensics techniques.
2) To propose a forensics technique for Copy-Move frame duplication within video frame sequences.
3) To propose a forensics approach for Copy-Move region duplication from another frame of the digital video.

4) To propose a video forensics scheme to improve the detection against chroma key forgery with various attacks.

2.11 Research Methodology

The presented research work has mainly focused on improving detection of CMFD, CMRD and CKF in the digital videos to identify their authenticity. Therefore, the existing CMFD, CMRD and CKF techniques are analyzed to find their limitations. Based on these limitations, the research is initially targeted to develop a technique for CMFD forgery detection. In this approach, CMFD forgery has been detected at long continuous locations and many different locations with different frame sequences in size. This approach also detected CMFD forgery from other digital videos. This work has been extended for detecting the multiple CMFD forgeries in the digital videos.

The research work is also devoted to designing a technique for detecting CMRD forgery in the digital videos. In this technique, CMRD forgery has been detected in regular and irregular forms within the same frame and from another frame. This research work has also extended for detecting the multiple CMRD forgery within different region size in the digital videos. These approaches for CMFD and CMRD analyzed the variations in the pixel intensity values of each frame of the digital video. This analysis provides the information about the variation artifacts between different frame sequences and within video frame regions. These artifacts indicate many disturbances within the pixel intensity values of video frames and its regions. After that, statistical methods are implemented in these approaches.

Moreover, a CKF forgery detection approach is designed based on FEI. This approach improves the detection and provides the robustness against various attacks. The performance of proposed approaches is evaluated on the digital videos taken from the SULFA dataset and downloaded from the internet. Then the evaluation parameters of proposed approaches are compared with those of existing techniques. All the simulations are performed using MATLAB R2017b software on a system with 2.40 GHz CPU and 4 GB RAM. The flow of research work carried out in this thesis is provided in Figure 2.1.

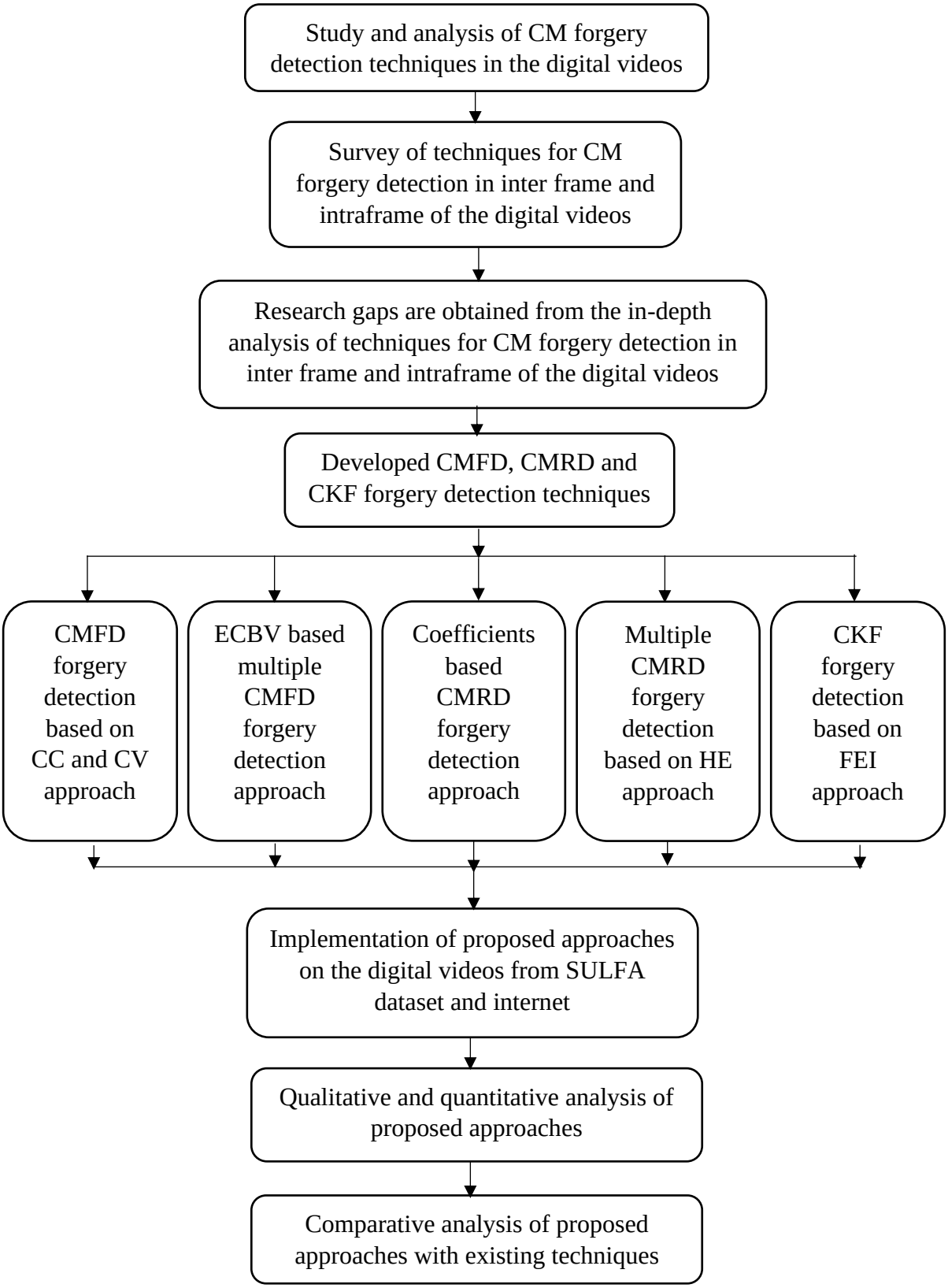


Figure 2.1: Flow diagram of work done

CHAPTER 3

CMFD FORGERY DETECTION IN DIGITAL VIDEO

The comprehensive analysis of the literature related to CMFD forgery detection creates the necessity to further explore this forgery detection in digital videos. In this chapter, a proposed approach is presented which detects CMFD forgery in three different forms such as (i) a long duplicated consecutive frame sequence at its continuous location, (ii) the number of duplicated frame sequences with their different lengths and locations, and (iii) a lot of duplicated frame sequence from other digital video having different or same resolutions. The performance of the proposed approach has been evaluated on the digital videos taken from the SULFA dataset and internet. The comparison of the proposed approach with other existing techniques demonstrates that the proposed approach provides better results on the accurate detection of CMFD forgery than the existing techniques in the digital videos.

3.1 CMFD Forgery Detection Based on CC and CV Approach

The practice of detecting duplicated frame sequences having small lengths has been provided in the previous techniques for many years. However, the long duplicated consecutive frame sequence at its continuous location is difficult to detect due to low pixel intensity variation between frames in the digital video. Several activities in a digital video may be lost at different time intervals by duplicating several frame sequences with different lengths and locations. It can be represented that nothing has happened at those time intervals in front of the court as evidence.

Moreover, the frame duplication from other digital videos having the same or different resolutions can also change the complete meaning of the digital video. Therefore, CMFD forgery detection based on the CC and CV approach has detected the frame sequences duplicated in different forms within the digital videos. Figure 3.1 shows the flow diagram of CMFD forgery detection based on the CC and CV approach. Firstly, a digital video has been taken as an input from which the number of RGB frames are extracted with the proposed approach. These RGB frames are a collection of digital images with the same resolutions as Figure 3.2. Now, each extracted RGB frame is transformed into a grayscale frame. The pixel values of each grayscale frame are intensities of respective pixels of each RGB frame which are attained by Eq. (3.1) [63]**.**

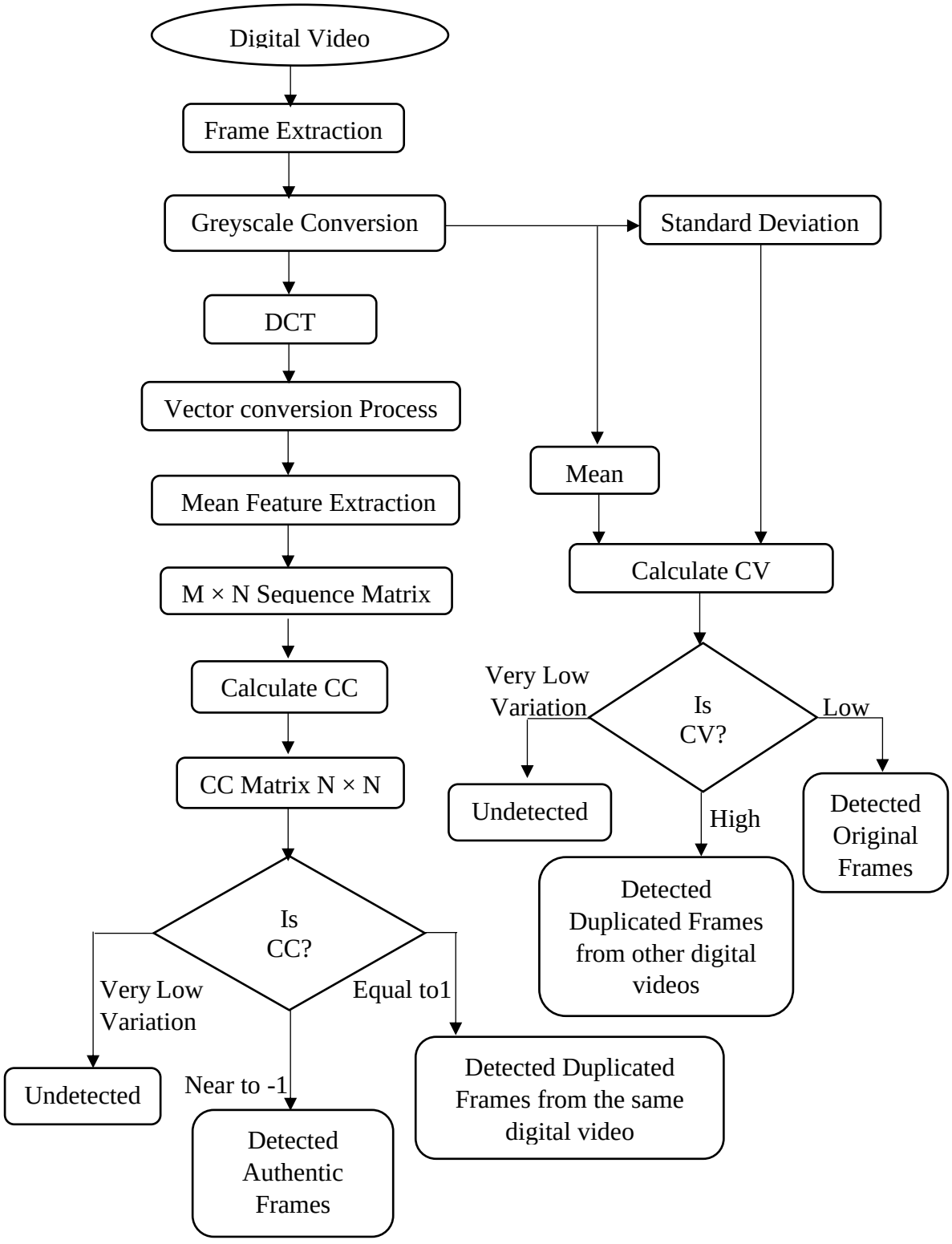


Figure 3.1: Flow diagram of CMFD forgery detection based on CC and CV approach

Figure 3.2: Frame extraction from the input digital video

$$\mathrm{I} = 0.299R + 0.587G + 0.114B \tag{3.1}$$

Where *R*, *G* and *B* are red, green, and blue channels of the input RGB frame, I represents the luminance component. This conversion reduces the color complexity and noise in the frames of digital video. Also, in the grayscale frame, only 8 bit is need to store a single pixel of that frame. Thus, less memory is required to store the grayscale frame than RGB frame. Due to one channel in grayscale frame, the range of a pixel value varies from 0 to 255. Pixel value 0 denotes the black color and the pixel value 255 represents the white color. On other side, the RGB frame has three color channels. Therefore, a RGB pixel value has three numbers from 0 to 255 which increases the complexity in the work.

DCT can be utilized on the 2D array. These grayscale frames are 2D arrays, whereas the RGB frames are a 3D array [46]. So, DCT is implemented on grayscale frames because its direct implementation on the RGB frame will generate an error. Thus, the complexity in the calculation of RGB frame becomes easy with grayscale conversion. These all grayscale frames are transformed into their DCT matrices. DCT transformations of grayscale frames are shown in the form of DCT matrices of M × N in Figure 3.3, where M indicates several rows and N shows several columns.

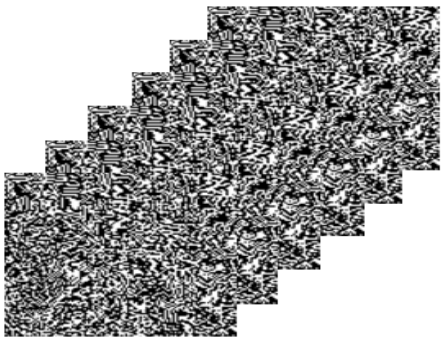


Figure 3.3: DCT transformation of grayscale frames of a digital video

It has been observed that while camera is stationary then all pixel values of adjacent frames are very near to close. It may provide the correlation between frames near to 1 i.e., frames are duplicated which is wrong detection. Therefore, DCT is applied to change all pixel values of each frame in the digital video. So that correct duplication forgery could be detected. After this transformation, one-dimensional vectors are made from corresponding DCT matrices. This process converts a DCT matrix into one dimensional vector whose elements are represented by $A_i = \{A_1, A_2, A_{3.....}A_m\}$ as shown in Figure 3.4 where, A_i is a vector feature of the DCT matrix of frame F_i, k is a total number of pixel intensity values, and 'i' is number of vectors.

$\mathbf{A_1}$
$\mathbf{A_2}$
$\mathbf{A_3}$
…
…
…
$\mathbf{A_M}$

Figure 3.4: Converting DCT matrix into a vector

Now, the mean features of each frame have been found by computing the mean of each vector in the digital video using Eq. (3.2) [109].

$$\mu_{A_k} = [\frac{1}{M} \sum_{x=1}^{M} A_{(x,1)}] \quad 3.2$$

where, $A_{(x,1)}$ is a pixel intensity value of a vector A_k, M is a total number of pixel intensity values, $\sum_{x=1}^{M} A_{(x,1)}$ is the sum of all pixel intensity values and μ_{A_k} is the mean of a vector of k^{th} frame in the digital video. A_k represents one dimensional vector of k^{th} frame in the digital video Thus, mean of each frame has been calculated. After getting mean features of each frame, the entire digital video is settled into several frame sequences. These frame sequences are organized by arranging the mean feature of each frame in the form of an array. Each frame sequence contains an array with equal finite length of *n. 'n'* is the number of mean features. The second frame sequence has begun from the second element of the first frame sequence to $(n + 1)^{th}$e element. The third frame sequence has started from the third element of the first frame sequence to $(n + 2)^{th}$ element, as shown in Figure 3.5. Thus, while each mean feature of the first frame sequence is used to construct other frame sequences, the next frame sequence will begin from $(n+1)^{th}$ to 2*n* and so on

					N+1 ↓	
First Element →	**1**	**2**	**3**	**... ... ...**	**9**	**.**
Second Element →	**2**	**3**	**4**	**... ... ...**	**10**	**.**
Third Element →	**3**	**4**	**5**	**... ... ...**	**11**	**.**
.	**4**	**5**	**6**	**... ... ...**	**12**	**.**
.	**5**	**6**	**7**	**... ... ...**	**13**	**.**
.	**6**	**7**	**8**	**... ... ...**	**14**	**.**
.	**7**	**8**	**9**	**... ... ...**	**15**	**.**
.	**8**	**9**	**10**	**... ... ...**	**16**	**.**
.	↑	↑	↑		↑	**.**
Last Element →	***n***	***(n+1)th***	***(n+2)th***		***2n***	

Figure 3.5: Matrix of mean features for a digital video

. This arrangement provides a frame sequence matrix of $n \times m$ after arranging all mean features in the different frame sequences. Here m is total number of frame sequences in a digital video calculated by Eq. (3.3) [120].

$$m = l - n + 1 \tag{3.3}$$

where, l is length of a digital video i.e. total number of frames, and n is length of a frame sequence.

Now CC of each frame sequence are found with remaining other frame sequences of a digital video to make CC matrix of m × m. These CC are used to detect the similar frame sequences in the digital video. If CC between two frame sequences is equal to 1, then it means these both frame sequences are similar, i.e. all frames of one frame sequence are matched with frames of other frame sequence. Out of these two similar frame sequences, one frame sequence is authentic and the other is duplication of one. On the other hand, if the value of CC is near to -1, it means no frame duplication exists between frame sequences. These sequences are authentic frame sequences.

After detecting any two similar frame sequences, CC between first frames of both similar and previous frames is computed to differentiate the duplicated frame sequence from them. If CC is close to 1, then that sequence is authentic frame sequence otherwise it is duplicated frame sequence. Thus, a long consecutive frame sequence running at continuous location has been detected in the digital video. Similarly, CC between all frame sequences of a digital video are calculated to detect the similar frame sequences having different lengths and placed at different locations in the digital video.

The frame sequences that are copied from other digital video having the same or different resolutions have also been detected by the proposed approach using CV. The mean and standard deviation have been calculated in each grayscale frame of the digital video. Then the CV of each frame has been computed using Eq. (2.6.1) in the digital video. It is observed that the CV of duplicated frame sequences having higher resolution is reduced more than that of lower resolution due to the larger value of mean. In contrast, the CV of all frames of authentic frame sequence are almost constant.

3.2 Performance Analysis of CMFD Forgery Detection Based on CC and CV Approach

In this section, the proficiency of proposed CMFD forgery detection based on the CC and CV approach is confirmed qualitatively and quantitatively by taking a generated dataset in which digital videos have been taken from the SULFA dataset and the internet. Moreover, the proposed approach is compared against the existing techniques of CMFD forgery detection.

3.2.1 Dataset and Setting

To evaluate the proposed approach for detecting CMFD forgery in digital videos, a dataset has been generated with 340 digital videos. In this dataset, out of 340 digital videos, 40 digital videos have been selected for training purposes. Whereas remaining 300 digital videos have been selected for testing purposes in which 150 digital videos are authentic and 150 videos are forged digital videos. These selected digital videos for the training set and testing set are non-overlapping.

3.2.2 Simulation Results for Test Digital Videos of Dataset

Qualitative and quantitative analysis is conducted on the test digital videos to confirm the capability of the presented CMFD forgery detection based on the CC and CV approach.

3.2.2.1 Qualitative Performance Analysis

In qualitative performance analysis of the proposed approach, the extracted mean features of four test digital videos have been shown in Figure 3.6 (a), (b), (c) and (d) respectively in which mean of each frame of test digital videos are demonstrated. Also, CC of one frame sequence with all other frame sequences have been shown in Figure 3.7 (a), (b), (c) and (d) for test digital videos respectively which indicate if CC of any two frame sequences is equal to 1 then these two frame sequences are similar to each other. On the other hand, if CC is less than 1, then the frame sequences are authentic frame sequences of the digital videos.

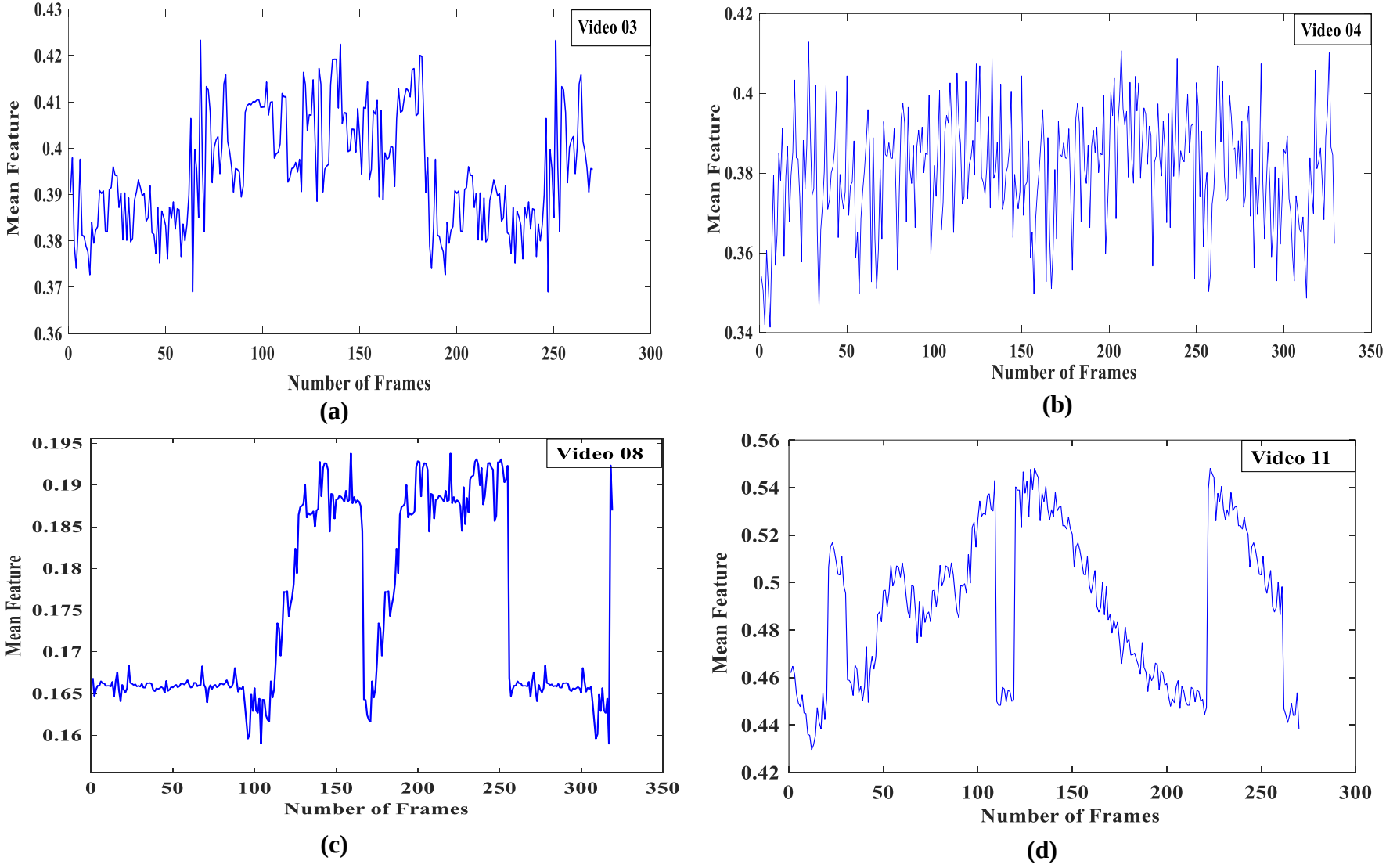


Figure 3.6: (a), (b), (c) and (d) Mean feature of test digital videos

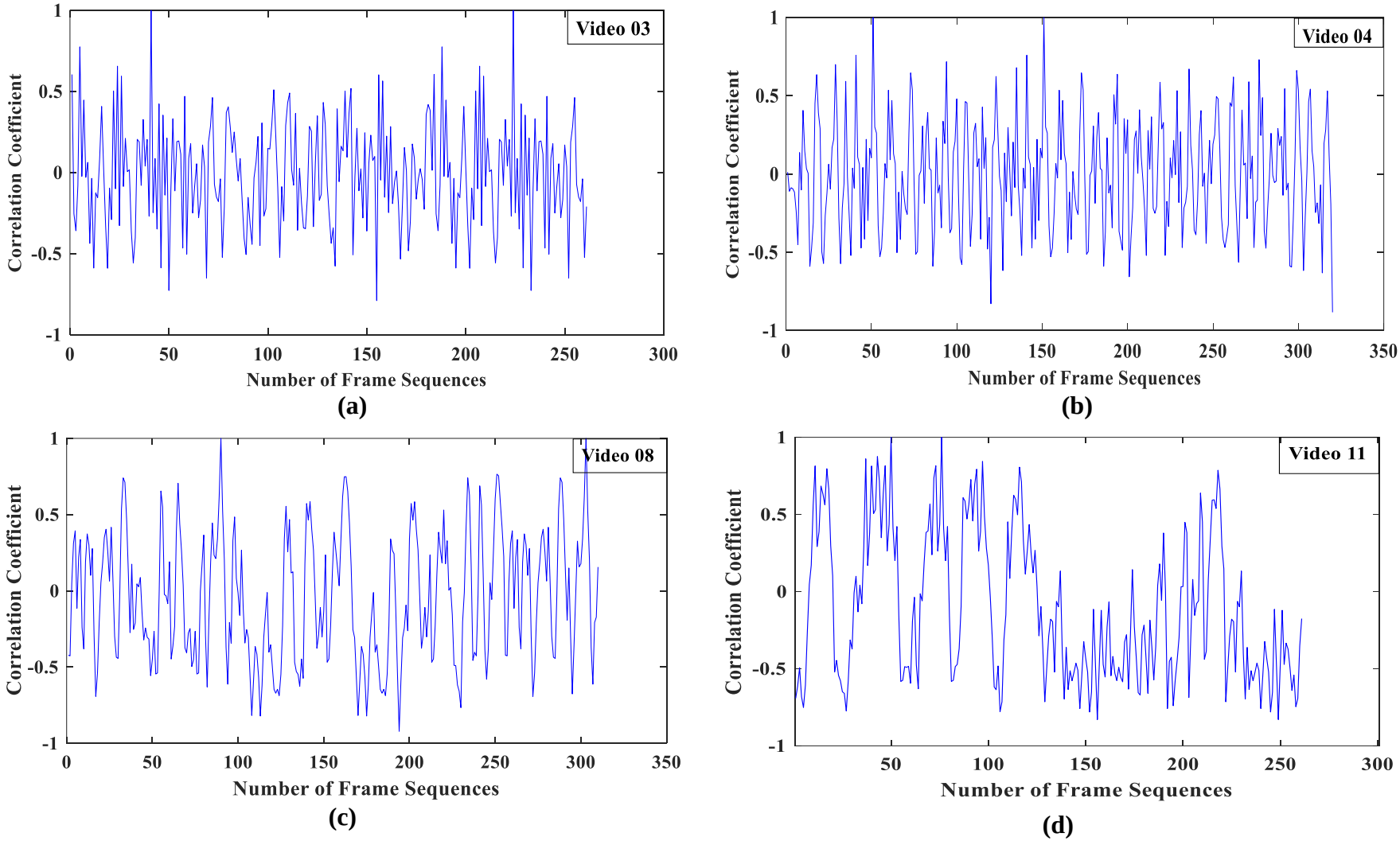
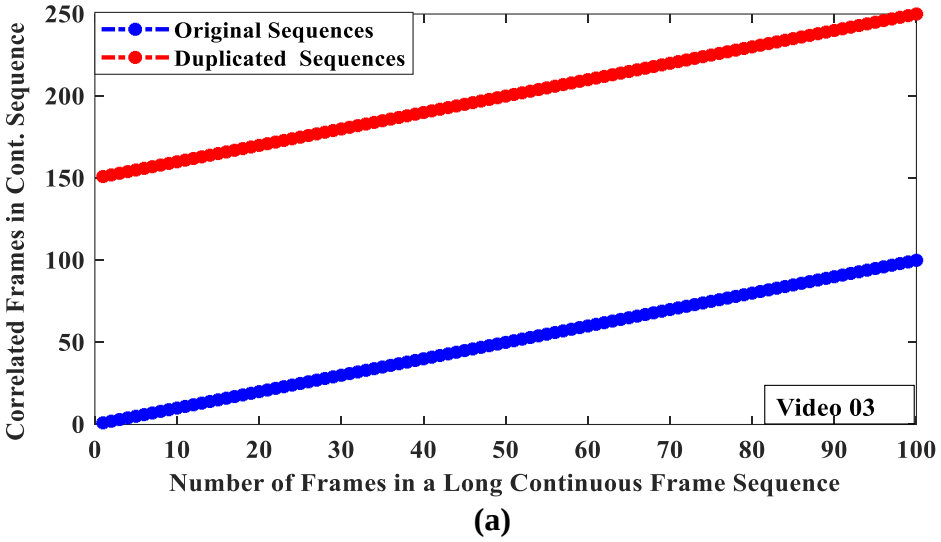
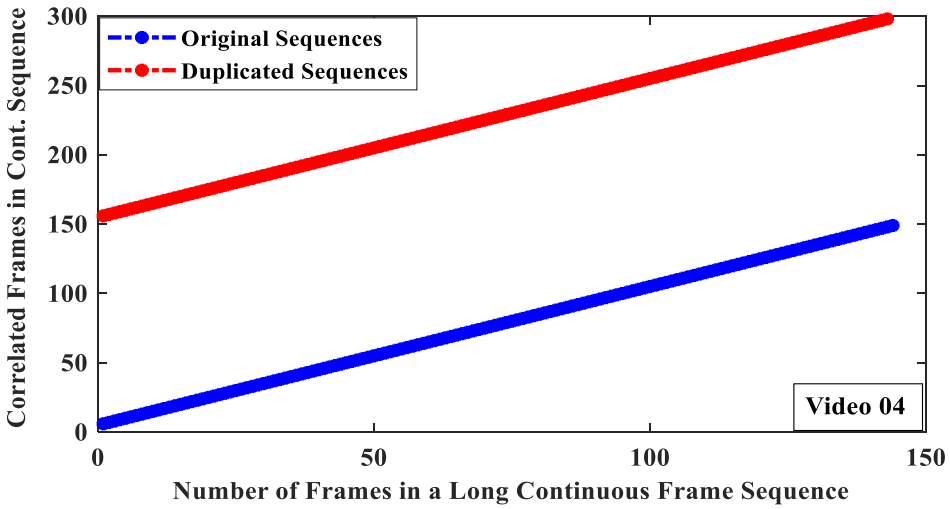


Figure 3.7: (a), (b), (c) and (d) CC of a frame sequence with all other frame sequences of test digital videos

After carrying out the intensive simulations, the duplicated long consecutive frame sequences running at continuous locations have been detected by proposed CMFD forgery detection based on the CC and CV approach in the digital videos shown in Figure 3.8. The blue lines in Figure 3.8 show the authentic frame sequence in the digital videos whereas red lines show the duplicated frame sequence in that digital videos. Here, x-axis of Figure 3.8 show a number of frames in which the total number of duplicated frames have been shown by the x-axis and the correlated frame sequences have been shown by the y-axis.

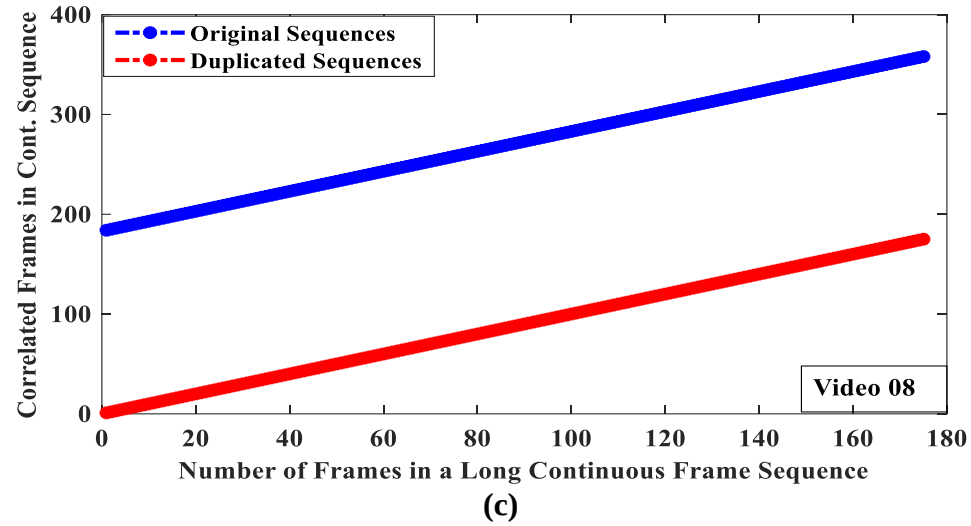


(a)

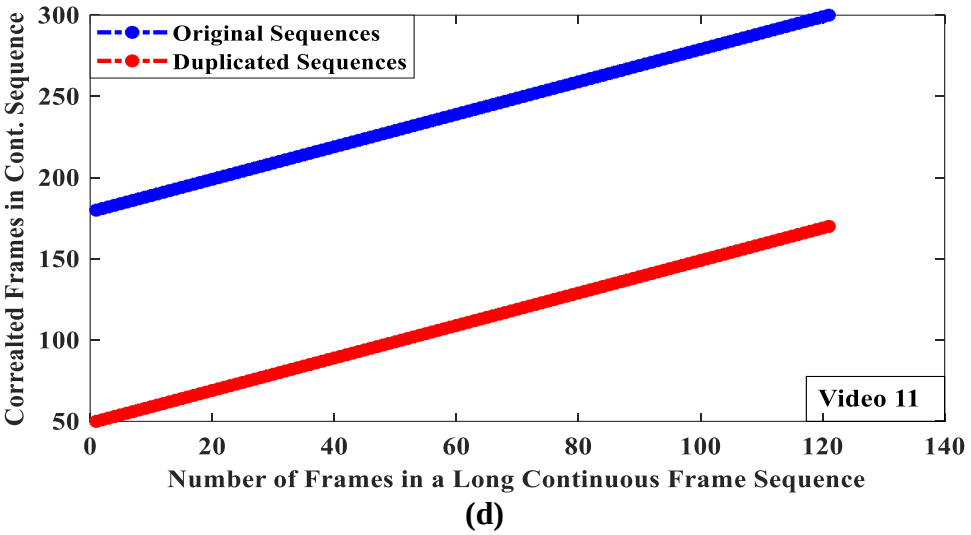


(b)

Figure 3.8: (a) and (b) CMFD forgery detection in a long consecutive frame sequence at continuous location in test digital video



(c)



(d)

Figure 3.8: (c) and (d) CMFD forgery detection in a long frame sequence at continuous location in test digital video

Also, several duplicated frame sequences having different lengths at different locations have been detected by the proposed approach in the digital videos shown in Figure 3.9. Similarly, the blue lines in Figure 3.9 show the authentic frame sequence in the digital videos whereas red lines show the duplicated frame sequence in that digital videos. Here, the total number of duplicated frames have been shown by the x-axis. Whereas, the y-axis has shown the correlated frame sequences.

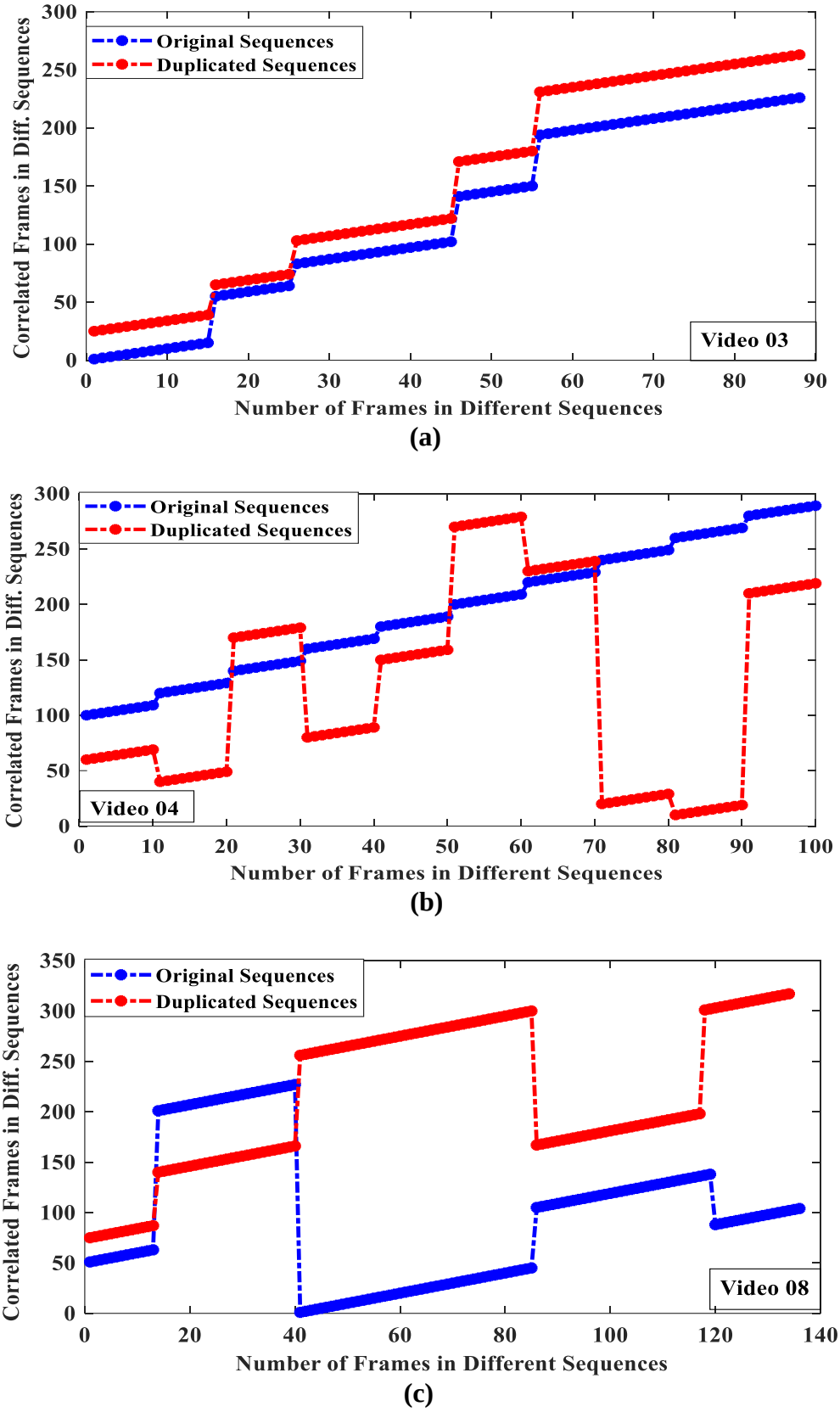
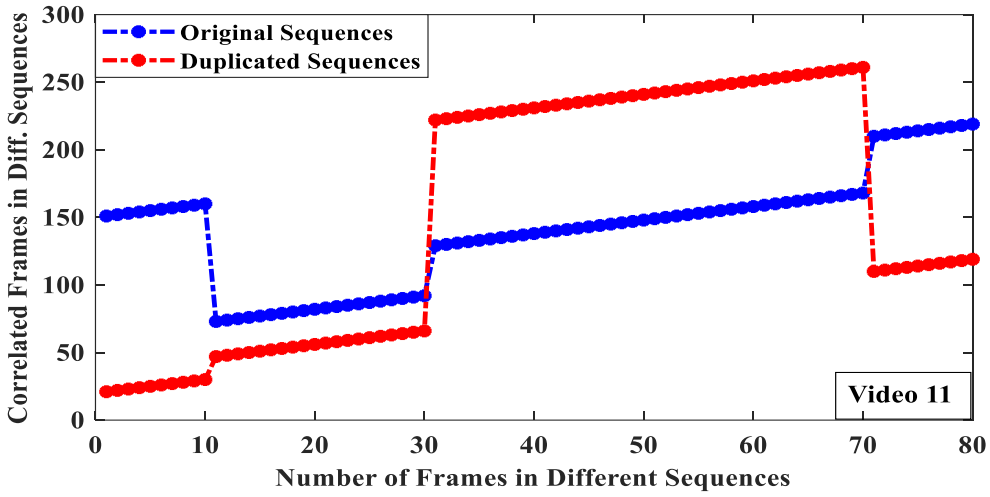


Figure 3.9: (a), (b) and (c) CMFD forgery detection in the number of frame sequences having different lengths at different locations in test digital videos



(d)

Figure 3.9: (d) CMFD forgery detection in the number of frame sequences having different lengths at different locations in test digital videos

Figure 3.10 shows very low CV for second duplicated frame sequence having higher resolution than CV for first duplicated frame sequence having low resolution and CV of authentic frame sequence is almost constant.

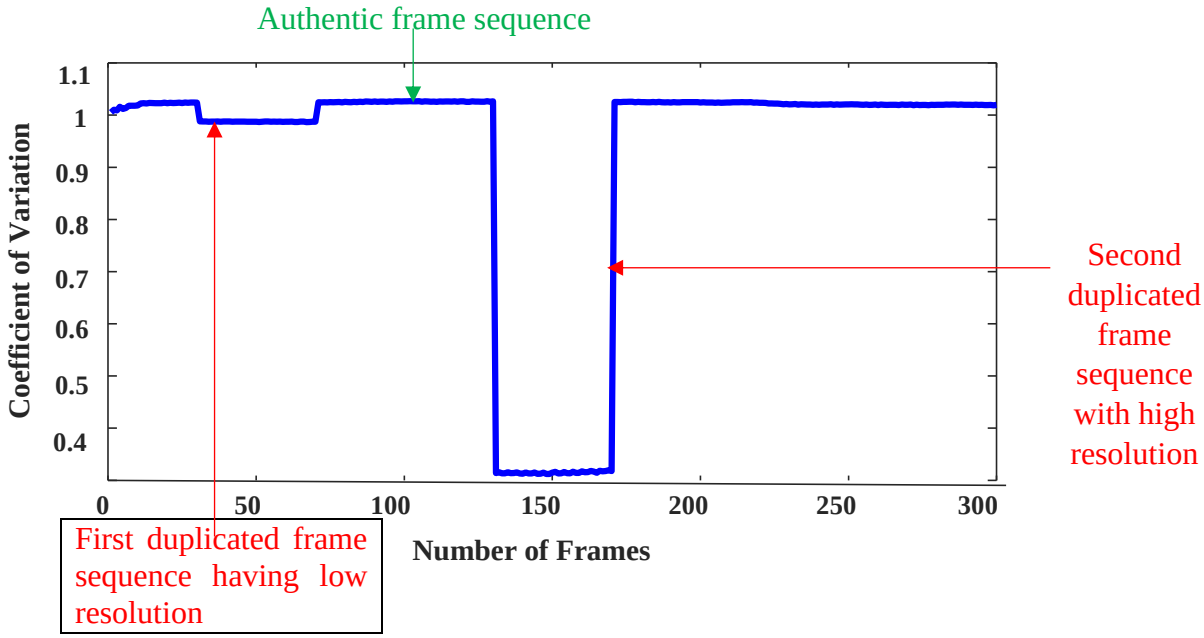


Figure 3.10: CMFD forgery detection from other digital videos having different resolution

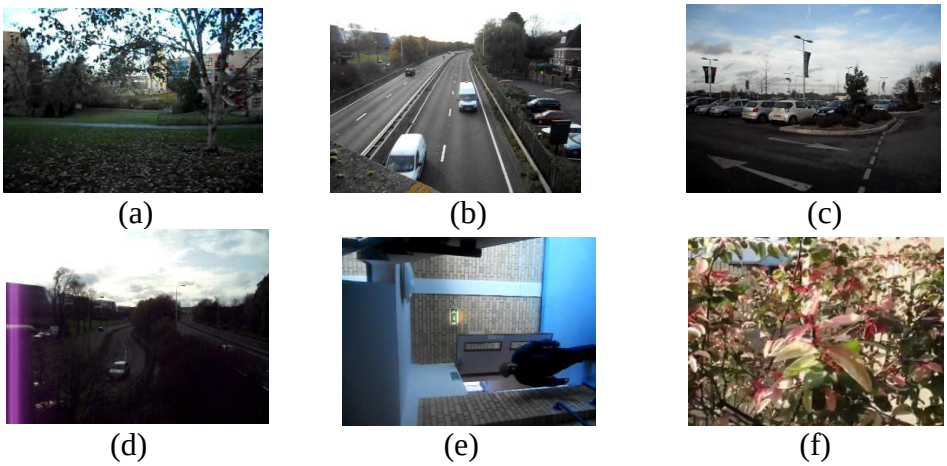
The detail of some digital videos is given with CMFD forgery at continuous and different locations in Table 3.1. In the experimental work, it has been observed that some test digital videos have effected by camera and object positions. In these digital videos, the camera is static with stationary and moving objects, whereas in other few digital videos, the camera is moving at 180 degree with stationary and moving objects.

Table 3.1 Detail of some testing digital videos with CMFD at continuous locations and different locations (Sample 25 videos out of 300 testing digital video

Video Name	Video Length	Resolution	Video Format	Camera Model	CMFD at Continuous Location	CMFD with Different Lengths at Different Locations
Video_01	354	320×240	.mov	Canon SX200	01-45 copied to 256-300	12-31 to 74-93,105-138 to 36-68, 201-250 to 151-200,277- 300 to 253-276, 141-150 to171-180, 194 - 226 to 231-263
Video_02	270	320×240	.avi	Canon SX200	36-107 copied to 122-193	83-102 to 103-122, 151-160 to 21-30, 201-212 to 213-224
Video_03	300	320×240	.avi	Canon SX200	01-100 copied to 151-250	1-15 to25-39, 55-64 to 65-74, 83-102 to 103-122, 141-150 to171-180, 194 -226 to 231-263
Video_04	360	320×240	.mov	Canon SX200	06-149 copied to 156-298	100-109 to 60-69, 120-129 to 40-49, 140-149 to 170-179,160 to 169 to 80-89, 180-189 to 150-159,200-20to 270-279,220-229 to 230-239, 240-249 to 20-29, 260-269 to 10-19, 280-289 to 210-219
Video_05	329	320×240	.avi	Canon SX200	38-100 copied to 138-200	1-30 to 111-140, 161-189 to 301-329, 41-75 to 211-245, 31-40 to 262-271, 85-94 to 281-290
Video_06	210	320×240	.avi	Canon SX200	143-192 copied to 27-76	1-25 to 176-200, 71-90 to 100-119, 143-172 to 35-64
Video_07	312	320×240	.avi	Canon SX200	268-300 copied to 26-58	61-100 to 231-270, 101-140 to 1-40, 151-163 to 188-200, 45-54 to 300-309,272-292 to 205-225
Video_08	319	320×240	.avi	Canon SX200	160-300 copied to 01-140	51-63 to 75-87, 201-227 to 140-166, 1-45 to 256-300, 105-138 to 167-198, 88-104 to 301-317
Video_09	262	320×240	.avi	Canon SX200	011-50 copied to 161-200	1-20 to 61-80, 101-110 to 91-100, 171-180 to 35-45
Video_10	330	320×240	.avi	Canon SX200	41-77 copied to 1-37	23-40 to 51-68, 82-103 to 117-138, 105-114 to 191-200
Video_11	300	320×240	.avi	Fujifilm 2800	180-300 copied to 50-170	151-160 to 21-30, 73-92 to 47-66,129-168 to 222-261, 210-219 to 110-119

Video Name	Video Length	Resolution	Video Format	Camera Model	CMFD at Continuous Locations	CMFD with Different Lengths at Different Locations
Video_12	240	320×240	.avi	Fujifilm 2800	26-64 copied to 137-175	1-15 to 25-39, 73-92 to 47-60
Video_13	554	320×240	.avi	Fujifilm 2800	278-527 copied to 17-266	251-260 to 381-390, 261-270 to 391-400, 271-280 to 351-360, 281-290 to 361-370, 291-300 to 371-380
Video_14	360	320×240	.avi	Fujifilm 2800	37-41 copied to 111-115	101-105 to 171-175, 111-116 to 191-196, 121-124 to 181-184, 131-137 to 151-157
Video_15	420	320×240	.avi	Nikon S3000	128-158 copied to 251-301	1-10 to 261-270, 11-20 to 71-80, 21-30 to 181-190, 31-40 to 91-100, 41-50 to 151-160
Video_16	304	320×240	.avi	Nikon S3000	82-121 copied to 23-62	201-210 to 251-260, 211-220 to 291-300, 221-230 to 281-290, 231-240 to 261-270, 241-250 to 271-280
Video_17	188	320×240	.avi	Nikon S3000	101-147 copied to 51-97	17-30 to 43-56, 62-84 to 131-153
Video_18	299	384×288	.mp4	From Internet	18-30 copied to 32-45	51-91 to 215-255, 145-159 to 196-212, 256-276 to 95-115
Video_19	299	384×288	.mp4	From Internet	18-30 copied to 32-45	51-91 to 215-255, 145-159 to 196-212, 256-276 to 95-115
Video_20	2011	1024×768	.mp4	From Internet	1500-1600 cpied to 1438-1538	1951-1982 to 1700-1730, 1626-1660 to 1865-1899
Video_21	337	1280 × 720	.mp4	From Internet	271-310 copied to 231-270	305-330 to 245-270, 220-251 to 69-100, 21-40 to1-20
Video_22	1587	720 × 576	.mp4	From Internet	1100-1219 copied to 977-1096	1415-1450 to 1500-1535, 1235-1260 to 1365-1390
Video_23	299	384×288	.mp4	From Internet	18-30 copied to 32-45	51-91 to 215-255, 145-159 to 196-212, 256-276 to 95-115
Video_24	1052	240×160	.mp4	From Internet	600-750 copied to 801-951	807-850 to 1000-1043, 941-960 to 725-745, 673-698 to 525- 550
Video_25	588	640 ×480	.avi	From Internet	428-462 cpoied to 501-535	436-455 to 553-573, 428-462 to 501-535 ,291-320 to 91-120

Under these situations, the proposed CMFD forgery detection approach detects accurately different forms of CMFD forgery in the digital videos. The proposed approach detected this forgery in the test digital videos taken from internet which are already compressed and decompressed many times. It has also been observed that some test digital videos are affected by camera Zoom in-out function and some are affected by climate conditions such as running strong wind, strong raining and sharp sunlight as shown in Figure 3.11. The proposed approach has also detected CMFD forgery in these digital videos effectively.



(a) (b) (c)

(d) (e) (f)

Figure 3.11: Test digital videos (a) and (b) effected by camera zoom in-out function, (c) and (d) effected by climate condetions (d) suvillance video (f) effected with sharp sun-light

3.2.2.2 Quantitative Performance Analysis

Besides the simulation results, the proposed CMFD forgery detection based on CC and CV approach is also assessed quantitatively by considering various performance metrics. The proposed approach is evaluated based on performance parameters in test digital videos such as PR, RR, DA, F1, F2 score and execution time [2], [17], [18], [23], [34], [84], [113], and [124]. The generated dataset has been classified for detecting CMFD forgery in test digital videos which is based on coefficient values between frame sequences. CMFD forgery has been identified by calculating the CC and CV between frame sequences in each test digital video. The selected digital videos for the training set and testing set are non-overlapping. There is a threshold value 0.90 to establish the forgery level between two sequences. If CC between first frame and its previous frame is less than threshold value than the sequence is forged, otherwise the sequence is authentic. The outcomes are labelled as authentic digital video and forged digital video. The performance evaluation of the proposed approach has been shown in Table 3.2, whereas different parameters evaluation for the proposed approach has been provided in Table 3.3.

Table 3.2: Performance evaluation of CMFD forgery detection based on CC and CV approach for a testing set of digital videos

	Positive	**Negative**
True	1	0.99
False	0	0.01

Table 3.3: Evaluation of different parameters for CMFD forgery detection based on CC and CV approach

PR	**RR**	**DA**	**F1**	**F2**
1.000	0.990	0.995	0.994	0.991

Table 3.2 shows that CMFD forgery detection based on the CC and CV approach has effectively been performed to detect authentic and forged digital videos. On the other side, Table 3.3 indicates the results of the proposed approach in the form of different parameters PR, RR, DA, F1, and F2 of proposed approach such as 1.000, 0.990, 0.995, 0.994 0.991 respectively. These results show the effective capability of the proposed approach for detecting CMFD forgery in the digital videos.

3.3 Comparative Analysis

CMFD forgery detection based on CC and CV approach has been compared with existing techniques for detecting CMFD forgery in the digital videos in terms of PR, RR, DA, F1, and F2 as shown in Table 3.4. The existing techniques are represented such as Lin *et al.* [52], Wang *et al.* [112], Yang *et al.* [120], Ulutas *et al.* [106] and Bozkurt *et al.* [6] in Table 3.4.

Table 3.4: Comparison of CMFD forgery detection approach with existing techniques

	PR	**RR**	**DA**	**F1**	**F2**
Wang *et al.* [112]	0.385	0.817	0.658	0.523	0.667
Lin *et al.* [52]	0.879	**1.000**	0.940	0.935	0.973
Yang *et al.* [120]	0.982	**1.000**	0.991	0.990	0.996
Ulutas *et al.* [106]	0.99	0.99	0.99	0.99	0.99
Bozkurt *et al.* [6]	**1.000**	0.996	**1.000**	**0.997**	**0.996**
Proposed	**1.000**	0.990	0.995	0.994	0.991

Bold indicates higher values of parameters.

It indicates the higher value of PR of the proposed approach than existing techniques, whereas its RR is slightly low. However, DA of the proposed approach is higher than Wang *et al.*, Lin *et al.*, Yang *et al.*, and Ulutas *et al.* but little bit lower than Bozkurt *et al*. The F1 score of proposed approach is higher than Wang *et al.*, Lin *et al.*, Yang *et al.* and Ulutas *et al.* but less than Bozkurt *et al.* On the other hand, the F2 score of the proposed approach is low compared to Yang *et al.* and Bozkurt *et al.* while it is higher than Wang *et al.*, Lin *et al.* and Ulutas *et al.* These existing techniques have been detected small duplicated frame sequence at a location in the digital videos. However,the results of CMFD forgery detection based on the CC and CV approach indicate that the proposed approach provides effective performance for detecting CMFD forgery with different forms in the digital videos.

3.4 Computational Cost

The execution time of CMFD forgery detection based on the CC and CV approach has been shown in Table 3.5. In contrast, the comparison in execution time of the proposed approach and the existing techniques has been demonstrated in Table 3.6.

Table 3.5: Execution time of CMFD forgery detection based on CC and CV approach

Resolutions	720 × 576	640 × 480	320 × 240	240 × 160	384 × 288	1024 × 768	1280 × 720
Execution Time in f/s	0.149	0.118	0.024	0.121	0.084	1.59	0.983

Table 3.6: Comparison for execution time of CMFD forgery detection based on CC and CV approach with that of the existing techniques

Resolution	Ulutas *et al.* [106]	Bozkurt *et al.* [6]	Yang *et al.* [120]	**Proposed**
720 × 576	-	-	0.346	**0.149**
320 × 240	**0.01**	0.07	0.090	0.024
640 × 480	-	-	0.358	**0.118**

-means data has not been calculated in the existing techniques and bold indicates higher values of parameters.

Table 3.5 indicates the execution time of proposed approach on test digital videos having different resolutions such as 720 × 576, 640 × 480, 320 × 240, 240 × 160, 384 × 288, 1024 × 768, 1280 × 720. The execution times on resolutions of 720 × 576, 320 × 240 and 640 × 480 have also been compared with existing techniques, as shown in Table 3.6. It demonstrates the

better performance of the proposed approach in execution time than the existing techniques. The reason is that the mean features are used to detect the CMFD forgery which reduces the execution time of the proposed approach to a large amount. Therefore, the proposed approach provides effective efficiency for detecting CMFD forgery in the digital videos.

3.5 Summary

In this chapter, CMFD forgery detection based on CC and CV approach detects the similarities between frame sequences in the digital video. The proposed approach has detected CMFD forgery with long consecutive frame sequences at continuous locations, the number of frame sequences having different lengths at many different locations in the digital videos, and duplicated frame sequences from the other digital videos using CC and CV. This approach has provided effective results on the digital videos taken from SULFA dataset and internet. The proposed approach has also provided better execution time on digital videos with different resolutions. Therefore, it is apparent that CMFD forgery detection based on CC and CV approach has outperformed the existing techniques. It has further encouraged detecting the multiple CMFD forgeries in the digital videos. Hence, the next chapter deals with developing a novel approach for detecting multiple CMFD forgeries in the digital videos.

CHAPTER 4

MULTIPLE CMFD FORGERY DETECTION BASED ON ECBV

Multiple CMFD forgery have been detected in the digital videos in this chapter. The detection of multiple CMFD forgery is based on the identification of ECBV between digital video frames. The performance of the proposed approach has been examined on the digital videos having different resolutions taken from the SULFA dataset and internet. The proposed approach has been compared with other existing techniques. The proposed approach provides better results on accurately detecting multiple CMFD forgery in digital videos.

4.1 ECBV Based Multiple CMFD Forgery Detection Approach

ECBV based multiple CMFD forgery detection approach has been detected the following multiple CMFD forgery in the digital videos such as

(i) The proposed approach removes the limitation of the least number of detected frames in the existing techniques by detecting the single frame duplication (SFD). A frame is copied and moved anywhere within the same digital video in this duplication.

(ii) This approach detects the repetition of a frame (RF) for removing the forged gaps between different events of the digital video. A copied frame is repeated for making forged frame sequences in the digital video.

(iii) This approach detects the shuffled frame sequences (SFS) interchanged with other frame sequences of the digital video.

(iv) It also detects the disorder frame sequences (DFS). Any frame sequence is copied from the digital video and moved in disorder form at any other location of the digital video.

These SFD and DFS are more difficult to detect because there is no replicated frame or sequence. All shuffled, and disorder frames in the sequence are authentic digital video frames, but their locations have been changed. The flow diagram of ECBV based multiple CMFD forgery detection approach has been shown in Figure 4.1.

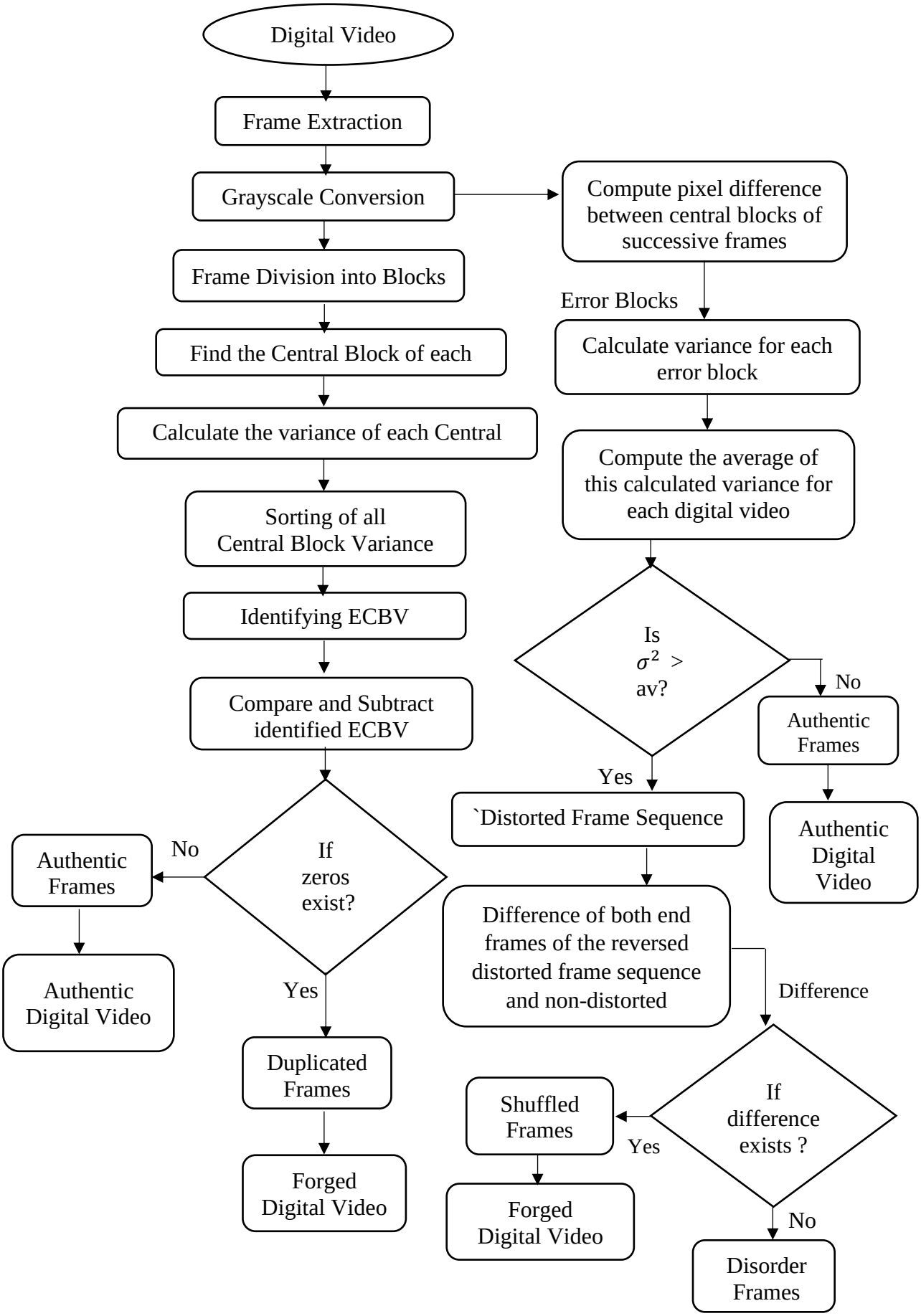


Figure 4.1: Flow diagram of ECBV based multiple CMFD forgery detection approach

Initially, ECBV based multiple CMFD forgery detection approach is extracted the number of frames from input digital video. These extracted RGB frames are converted into grayscale frames. Each grayscale frame is divided into several blocks made by sliding a square-shaped block over the grayscale frame from top-left pixel to bottom-right pixel. In CMFD forgery, the entire frame has been duplicated from one location to another location in the digital video. Thus, the complete information of a frame has been copied i.e., no any part of frame has altered. Therefore, all pixel values of a duplicated fame will be same as its authentic frame. Similarly, all pixel values in each block of duplicated frame will be same as that in each block of its authentic frame which results in equal variance for corresponding blocks.

After that, the central block of each grayscale frame is selected so that the proposed approach can focus on the central block of each frame rather than on the entire frame of digital video. If the proposed approach works on all blocks of each frame to detect the multiple CMFD forgery, it will consume more execution time for its processing, which is not desirable. Therefore, the proposed approach works on the central block of each frame for detecting the multiple CMFD forgery in the digital videos, as shown in Figure 4.2.

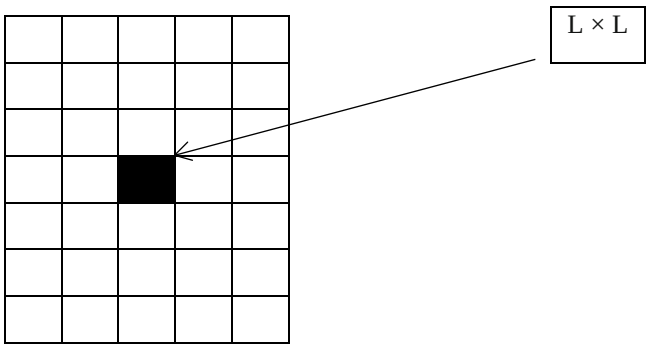


Figure 4.2: Representation of blocks of a grayscale frame with the selected central block

These selected central blocks are converted into vectors for computing their variances using Eq. (4.1) [73]. These variances are sorted to identify ECBV in the entire digital video. These ECBV are compared and subtracted from each to discover the equal variance.

$$\sigma^2 = \frac{\sum_{i=1}^{M}(A_i-\mu)^2}{M} \quad (4.1)$$

where σ^2 is variance, M is the total number of pixel intensity values in a vector, A_i is an element in a vector, and μ is the mean of a vector. When all variances are compared and subtracted, the equal variances become zero and unequal variances become non-zero. In this calculation, if there is only one equal variance, there is only one zero, i.e. there is a single duplicated frame in the entire digital video. This single duplicated frame is detected as a forged frame, and the digital video is identified as forged digital video, as shown in Figure 4.3. Figure 4.3(a) shows

the current frame of input digital video. Figure 4.3(b) indicates the pixel intensity values of a central block, whereas, the variance of each central block of the entire digital video is demonstrated in Figure 4.3(c). The detection of single duplicated frame with red circle mark in the entire digital video has been shown in Figure 4.3(d).

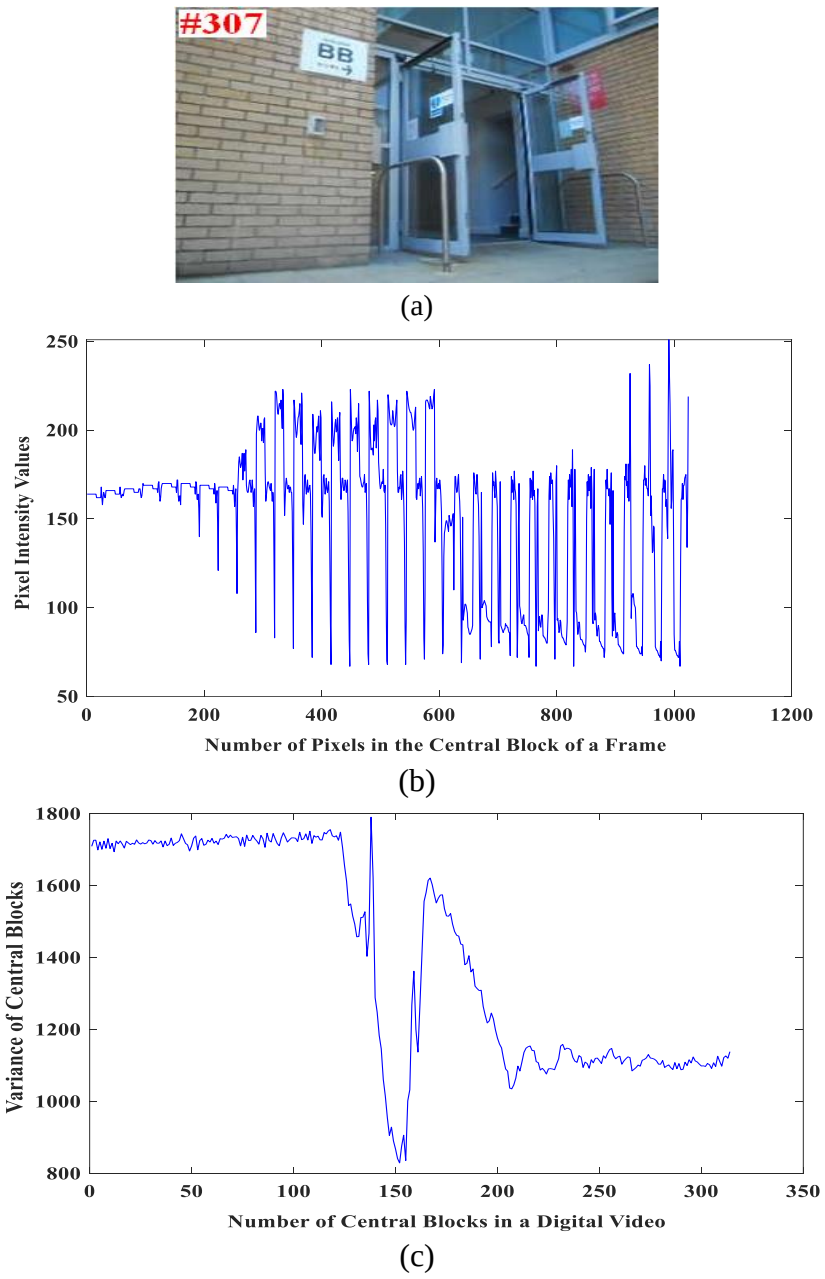
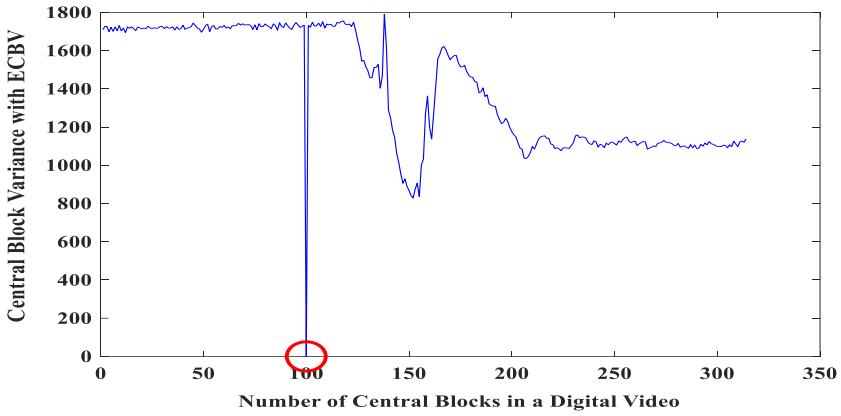


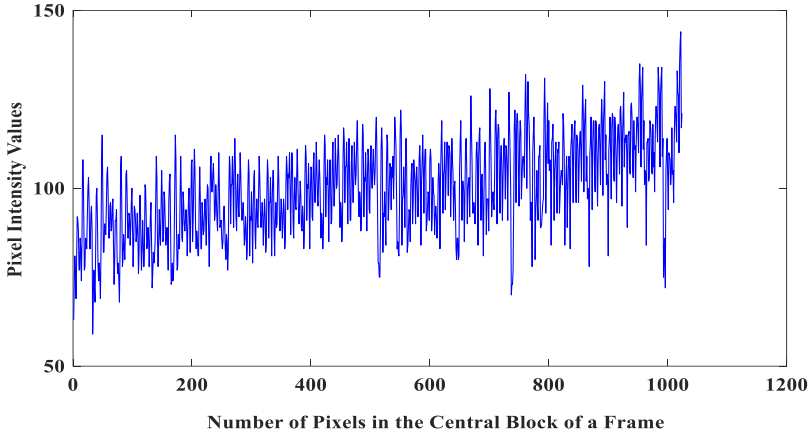
Figure 4.3: (a) Digital video frame (b) Pixel intensity values of a central block (c) Variance of each central block of the entire digital video



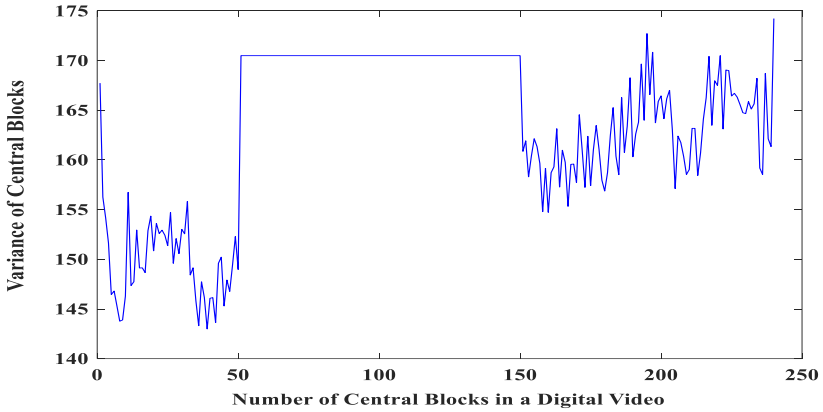
(d)

Figure 4.3: (d) Detection of SFD

If the number of zeros is generated in frame sequences of digital video, these generated zeros detect the RF in the digital video as shown in Figure 4.4. Figure 4.4 (a) shows the pixel intensity values of a central block of the current frame. Figure 4.4 (b) shows the variance of each central block of all frames in the digital video.

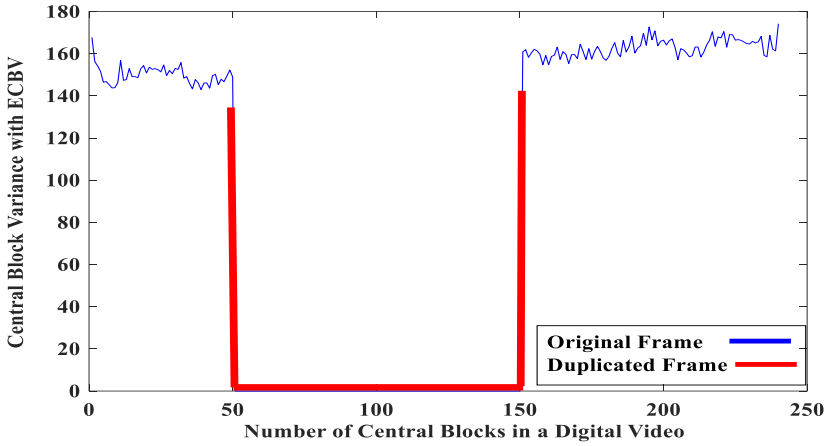


(a)



(b)

Figure 4.4: (a) Pixel intensity values of a central block of a frame (b) Variance of each central block of the entire digital video



(c)

Figure 4.4: (c) Detection of RF in a consecutive sequence in the digital videos.

Here, the frame variances from frame 50th to frame 150th become equal and constant due to RF. Figure 4.4 (c) shows the detection of RF in a consecutive sequence with a red mark.

On the other side, when a frame's central block variance becomes non-zero, that frame is identified as an authentic frame in the digital video. Similarly, if all frames' central block variances become non-zero, all frames are identified as authentic frames, and the digital video is identified as authentic digital video.

Now, the central blocks of all consecutive frames of the digital video have been subtracted from each other to generate the number of error blocks. These error blocks with pixel intensity difference values detect the SFS and DFS in the digital videos. The variance of each error block has been calculated using Eq. (4.1) in the digital video. After calculating the variance of each error block, compute the average of these calculated variances for the entire digital video using Eq. (4.2) [74].

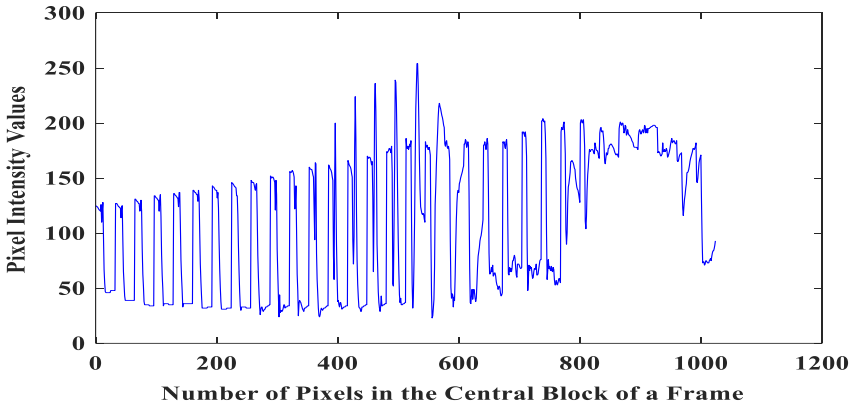
$$av = \frac{1}{\mathrm{M}} \sum_{i=1}^{\mathrm{M}} \mathrm{A}_i \tag{4.2}$$

where *av* is the average of calculated variances, M is a total number of pixel intensity values in a vector, and A_i is an element in a vector.

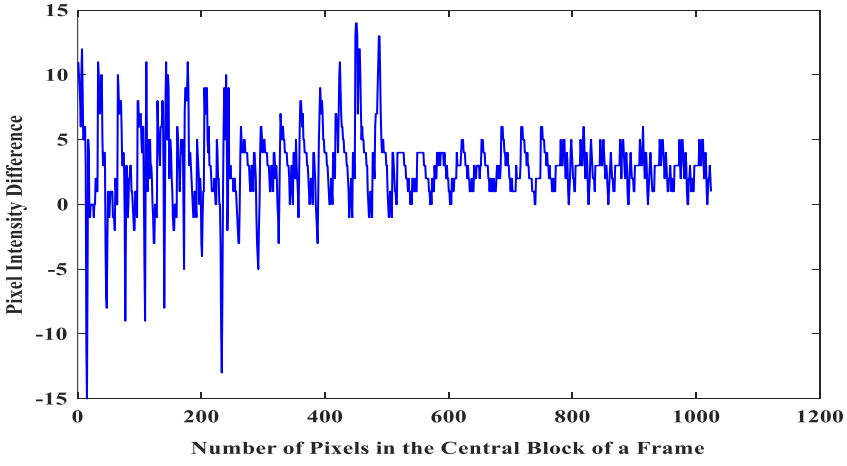
In the forged digital video, two high peaks of variance are generated at each end of a duplicated frame sequence due to high pixel intensity difference between two frames. Thus, if there are two duplicated frame sequences in a forged digital video then four high peaks will be generated. Due to these high peaks of variance, the average variance becomes more higher in the forged digital video than that of authentic digital video. However, there are authentic low and high variance due to authentic frame distance between two high peaks. Therefore, a digital video has been identified by computing the average variance and high variance between two highest peaks of pixel intensity differences in the central blocks. If average variance is less than the

high variance then digital video is authentic. On other side, if average variance is more than the high variance then those frames are detected as distorted frames. The sequence of these distorted frames is identified as a distorted frame sequence.

Now, this distorted frame sequence is reversed to calculate the difference between both end frames of the reversed distorted frame sequence and their neighbour frames. If a high pixel intensity difference occurs between them, the distorted frame sequence is identified as shuffled. Figure 4.5 (a) indicates the variation in the pixel intensity values of a central block for the shuffled frame sequence. Figure 4.5 (b) shows the pixel intensity difference between consecutive frame central blocks. Figure 4.5 (c) indicates SFS detection in which two high peaks show much higher pixel intensity differences on both ends of two SFS. However, low variance will exist between these two high peaks due to authentic frames in the frame sequence of digital video.

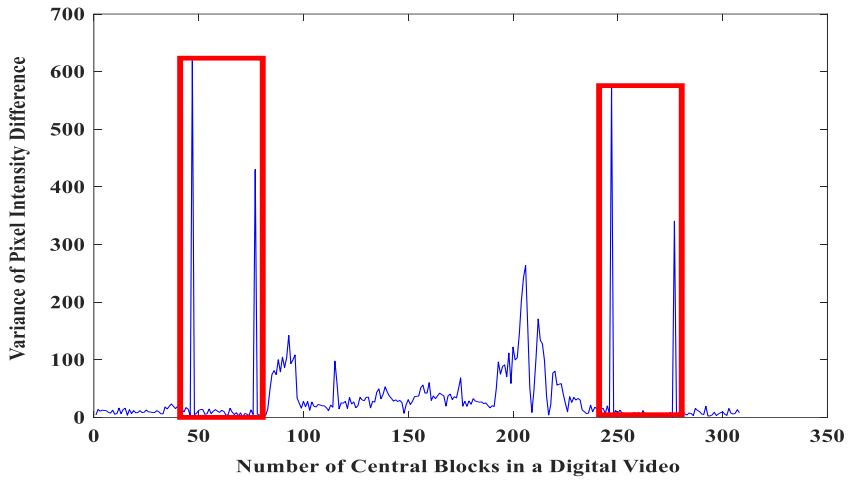


(a)



(b)

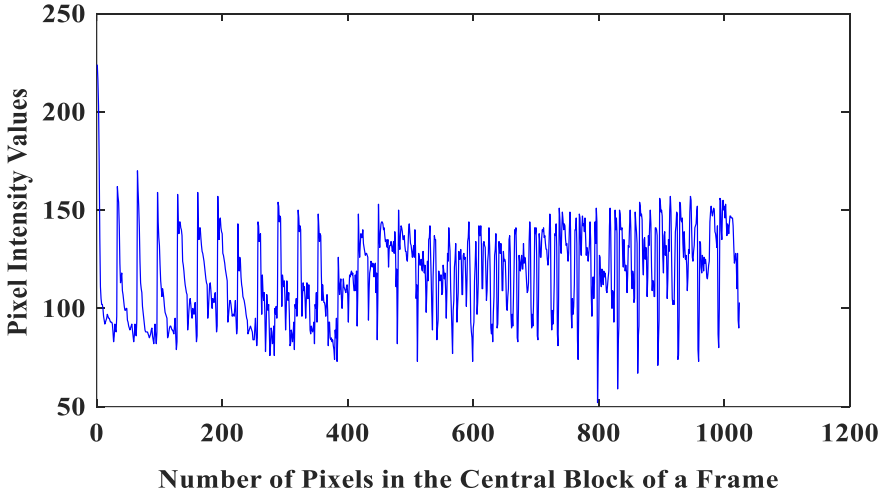
Figure 4.5: (a) Pixel intensity values of a central frame block (b) Variance of each central frame block of the entire digital video



(c)

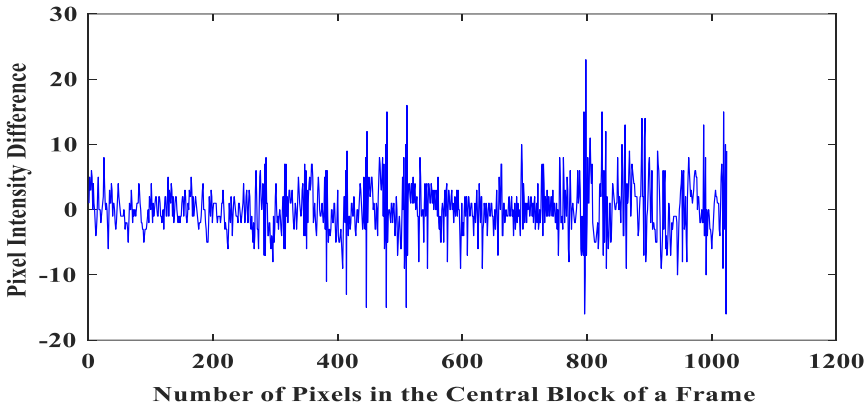
Figure 4.5: (c) Detection of SFS.

If the difference between both end frames of the reversed distorted frame sequence with their neighbour frames is very low, then the distorted frame sequence is identified as a disorder frame sequence as shown in Figure 4.6. Figure 4.6 (a) indicates the variation in the pixel intensity values for a central block of the disorder video frame. Figure 4.6 (b) shows a pixel difference between consecutive central blocks. Figure 4.6 (c) indicates the detection of a disorder frame sequence in which two high peaks show high pixel intensity variation on both ends of a disorder frame sequence. In contrast, low variance between these two high peaks will exist due to authentic frames in the frame sequence of digital video.

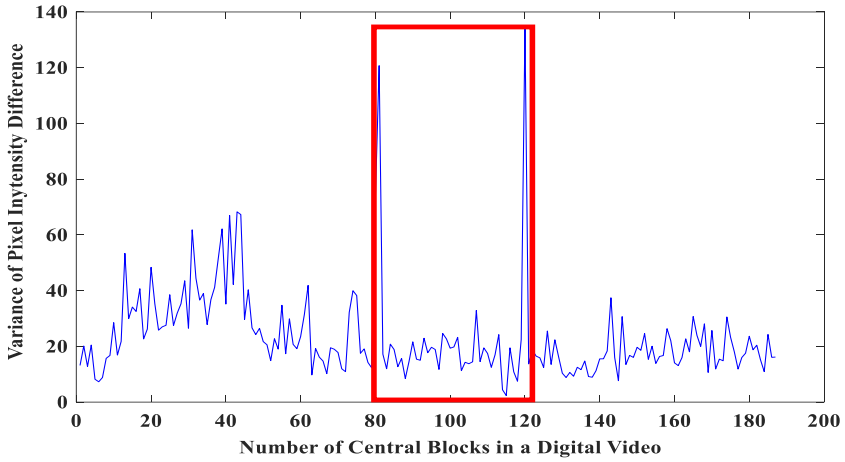


(a)

Figure 4.6: (a) Pixel Intensity values of a Frame Central Block



(b)



(c)

Figure 4.6: (b) Variance of each Frame Central Blocks of the entire video (c) Detection of DFS

4.2 Performance Analysis of ECBV Based Multiple CMFD Forgery Detection Approach

In this section, the ability of the proposed ECBV based multiple CMFD forgery detection approach is established both qualitatively and quantitatively by taking a generated dataset in which digital videos have been taken from the SULFA dataset and internet. Moreover, the proposed approach is compared against the existing techniques.

4.2.1 Dataset and Setting

For evaluating the proposed ECBV based multiple CMFD forgery detection approach, a dataset has been generated with 350 digital videos. Out of 350 digital videos, 50 digital videos have been selected for training purpose. Whereas remaining 300 digital videos have been selected for testing purposes in which 150 videos are authentic digital videos, and 150 video are forged digital videos. These selected digital videos for the training set and testing set are non-

overlapping. These digital videos have been arranged in dataset in form of different cases such as

Case I: Static camera digital videos with stationary and moving objects (SC)

Case II: Moving digital camera videos with stationary and moving objects (MC)

Case III: Digital videos with camera zoom in-out function (CZIOF)

Case IV: Surveillance digital videos (SvC)

Case V: Environment conditional digital videos (EC) and

Case VI: Internet downloaded digital videos (IDV).

4.2.2 Simulation Results for Test Digital Videos of Dataset

The analysis of ECBV based multiple CMFD forgery detection approach is conducted qualitatively and quantitatively on the test digital videos from the generated dataset to confirm the proposed approach's capability.

4.2.2.1 Qualitative Performance Analysis

The proposed approach has been performed on the digital videos having different cases for detecting multiple CMFD forgery. These different cases are based on the variation of pixel intensity values in the digital videos, out of which some digital videos with different cases have been detailed in Table 4.1. The detection results of multiple CMFD forgery detection approach have been shown in each case of the digital videos from Figures 4.7 to 4.10.

Table 4.1: Detail of some digital test videos with multiple CMFD forgery (Sample of 25 digital videos out of 350)

Video Name	Video Form -at	Different Cases	Video Type	SFD sequence	RF sequence	SFS	DFS
Video1	.mov	SC	Forged	10-176	10 => 176-275	01-50 =>125-175	135-200 =>200-135
Video2	.avi	SC	Forged	150 -125	150 => 01-125	123-168 =>35-80	201-250 =>250-201
Video_3	.avi	SC	Forged	186 -210	125 => 151-170, 186-210	57 =>147	263-313 =>313-263
Video_4	.mov	SC	Forged	37 - 100	174 => 175-200, 149-173	165-195 =>220-250	181-185 =>185-181
Video_5	.avi	MC	Authentic	Authentic	Authentic	Authentic	Authentic
Video_6	.mov	MC	Forged	174 - 175	25 =>182-250	17-35 => 89-107	17-35 =>35-17
Video_7	.avi	MC	Forged	227 - 58	227 => 58-125	53-93 => 128-168	53-93 =>128-168
Video_8	.avi	MC	Forged	145 - 153	145 => 155-200, 211-235	105 => 201	214-259 =>259-214
Video_9	.avi	CZIOF	Forged	195 - 33	105 => 106-140, 104-56	263-313 =>2801-2850	23-95 =>95-23
Video_10	.avi	CZIOF	Authentic	Authentic	Authentic	Authentic	Authentic
Video_11	.mov	CZIOF	Forged	159 - 227	159 => 187-227	11-35 => 111-135	01-05 =>05-01
Video_12	.avi	CZIOF	Forged	01 - 02	69 => 70-140, 68-05	181-185 => 207-211	45-100 => 100-45
Video_13	.avi	SvC	Forged	13 - 49	13 => 49-98, 111-156	71 => 49	21-30 => 30-21
Video_14	.avi	SvC	Forged	289 - 257	289 => 259-214, 210-170	222-257 => 258-293	75-98 => 98-75
Video_15	.avi	SvC	Authentic	Authentic	Authentic	Authentic	Authentic
Video_16	.mov	SvC	Forged	191 - 300	191 => 235-300	135-200 =>235-300	149-199 => 199-149
Video_17	.avi	EC	Forged	121 - 23-95	121 => 23-95	155-185 =>243-278	215-245 => 245-215

Video Name	Video Form -at	Different Cases	Video Type	SFD sequence	RF sequence	SFS	DFS
Video_18	.avi	EC	Forged	41 - 43	300 => 301-364,299-225	68 =>10	68-75 =>75-68
Video_19	.avi	EC	Forged	73 - 132	73 => 132-184, 205-2682	37-87 =>149-199	164-188 => 188-164
-Video_20	.avi	EC	Authentic	Authentic	Authentic	Authentic	Authentic
Video_21	.mp4	IDV	Forged	115 - 145	115 => 145-210	201-264 => 24-88	24-88 =>88-24
Video_22	.mp4	IDV	Forged	180 -100	47 => 63-89, 102-133, 163-198	153-197 => 96-140	158-178 =>178-158
Video_23	.mp4	IDV	Authentic	Authentic	Authentic	Authentic	Authentic
Video_24	.mp4	IDV	Forged	173 - 01	173 => 150-100, 50-99,01-40	164-188 => 266-290	11-16 disorder as 16-11
Video_25	.mp4	IDV	Forged	450 - 600	450 => 451-600, 449-200	325 =>575	400-550 =>550-400

The detection results of SFD in each case of the digital video have been shown in Figure 4.7, in which Figure 4.7 (a) shows the current frame of each case and Figure 4.7 (b) indicates the pixel intensity variation of the central block of the frame. Figure 4.7 (c) shows the variance of each central block of all frames and Figure 4.7 (d) shows the detection of SFD with generated single zero in the variance. The red circle on the detection waveform represents the single duplicated frame in the digital video.

The detection results for the RF in each case of digital video have been shown in Figure 4.8, in which Figure 4.8 (a) show the current frame of each case in digital video, whereas Figure 4.8 (b) indicate the pixel intensity variation of a central block of frame. Figure 4.8 (c) indicate the variance of each central block of all frames and Figure 4.8 (d) shows the detection for the RF in which all constant or equal variances become zero. The blue colour waveforms show the authentic frame sequence whereas the RF is shown by red coloured waveform.

Similarly, the detection results of shuffled frame sequence forgery and disorder frame sequence forgery in each case of digital video have been shown in Figures 4.9 and 4.10, respectively. High peaks of pixel intensity difference are enclosed with red colour lines.

Figure 4.9 (a) shows the current frame of each case and Figure 4.9 (b) indicates the pixel intensity variation of the central frame block. Figure 4.9 (c) shows the variance of each central block of all frames and Figure 4.9 (d) shows the detection of shuffled frame sequence forgery in the digital videos.

The detection results for the disorder frame sequence forgery in each case of digital video have been shown in Figure 4.10 in which Figure 4.10 (a) show the current frame of each case in digital video, whereas Figure 4.10 (b) indicate the pixel intensity variation of a central block of frame. Figure 4.10 (c) indicate the variance of each central block of all frames and Figure 4.10 (d) shows the detection disorder frame sequence forgery in the digital videos.

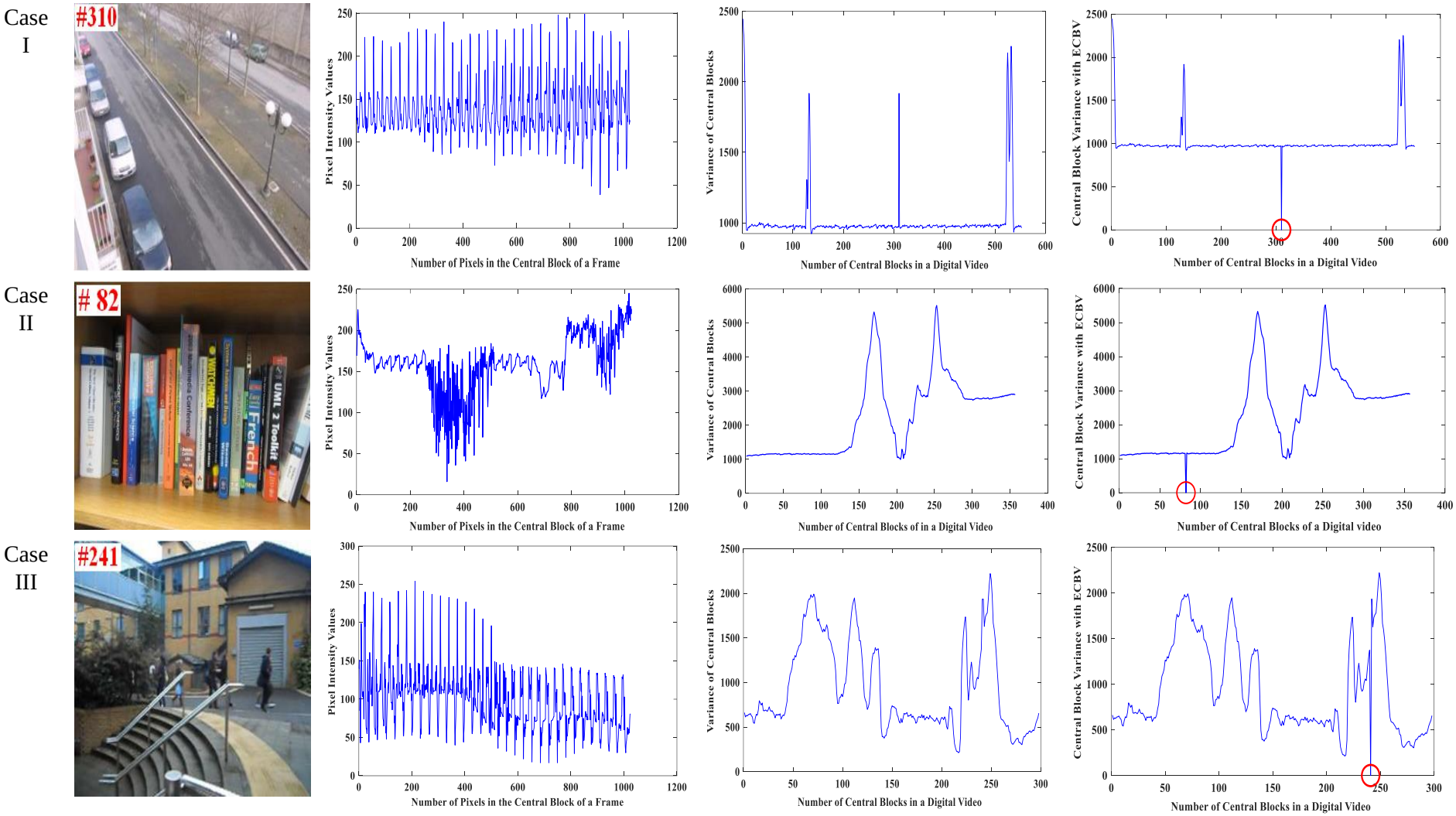


Figure 4.7: (a) Frames of digital videos with different cases (b) Pixel intensity values of a central block of frame (c) Variance of each central block of the entire digital video (d) Detection of SFD in test digital videos

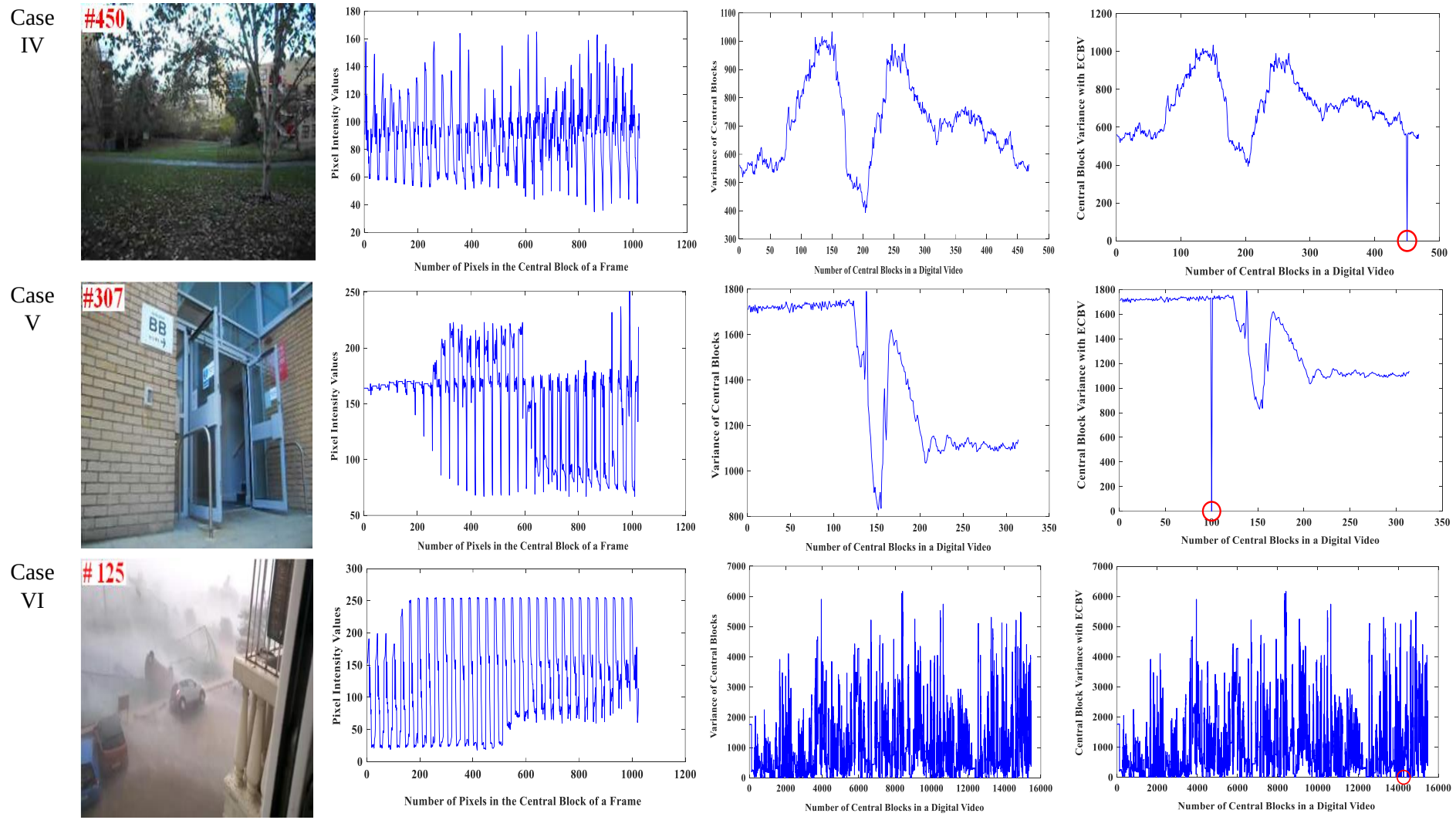


Figure 4.7: (a) Frames of digital videos with different cases (b) Pixel intensity values of a central block of frame (c) Variance of each central block of the entire digital video (d) Detection of SFD in test digital videos

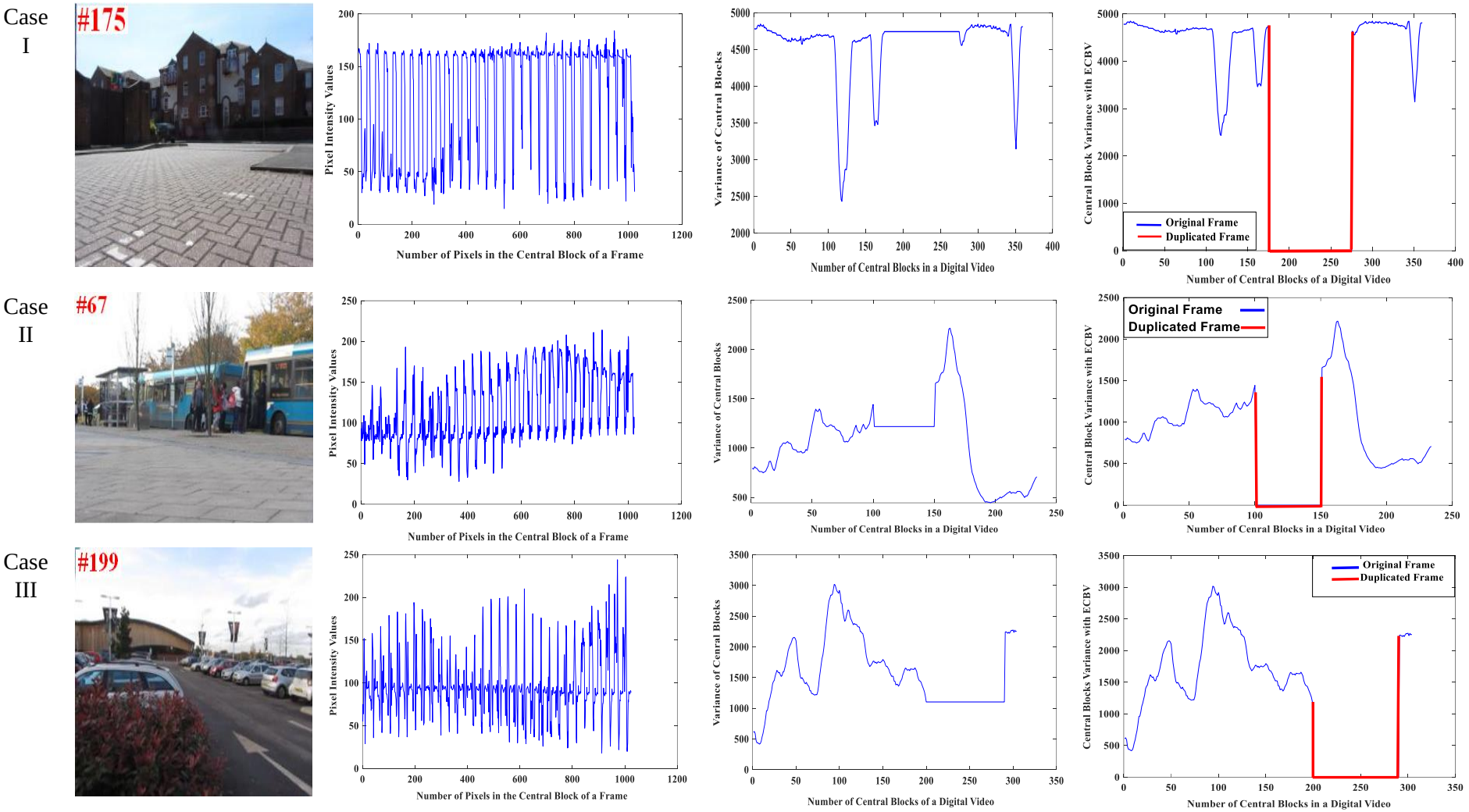


Figure 4.8: (a) Frames of digital videos with different cases (b) Pixel intensity values of a central block of frame (c) Variance of each central block of the entire digital video (d) Detection for the RF in test digital videos

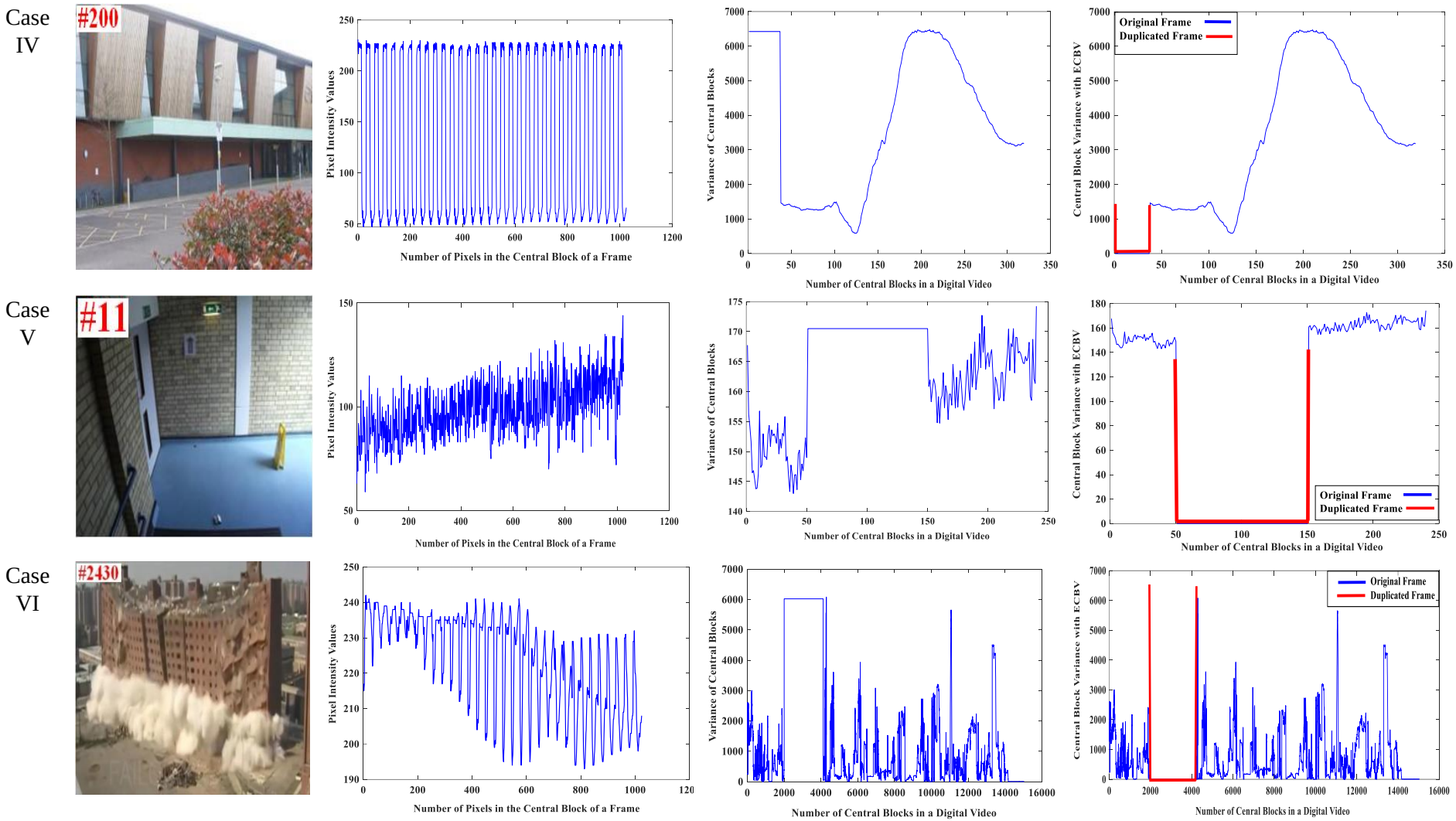


Figure 4.8: (a) Frames of digital videos with different cases (b) Pixel intensity values of a central block of frame (c) Variance of each central block of the entire digital video (d) Detection for the RF in test digital videos

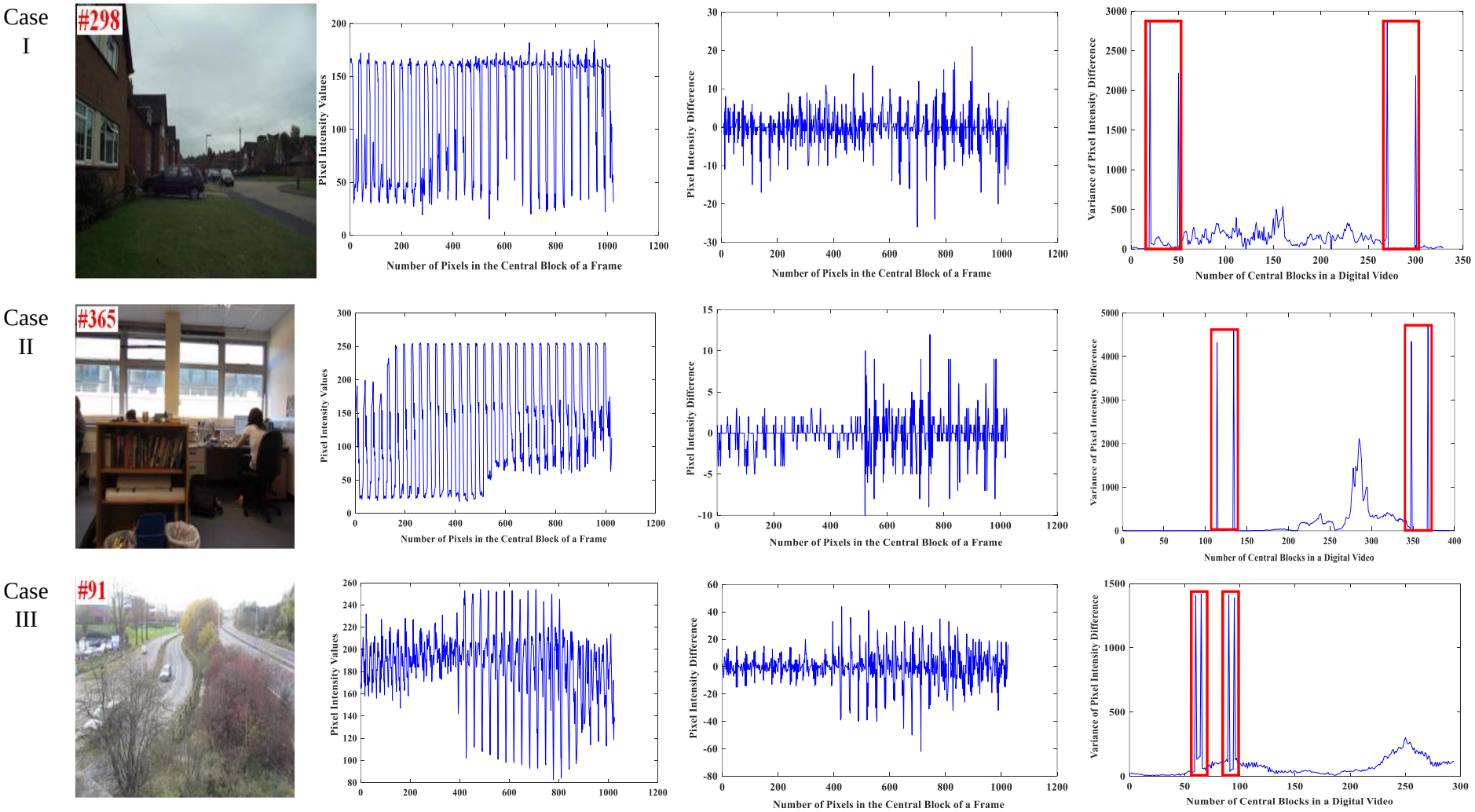


Figure 4.9: (a) Frames of digital videos with different cases (b) Pixel intensity values of a central block of frame (c) Variance of each central block of the entire digital video (d) Detection of SFS in test digital videos

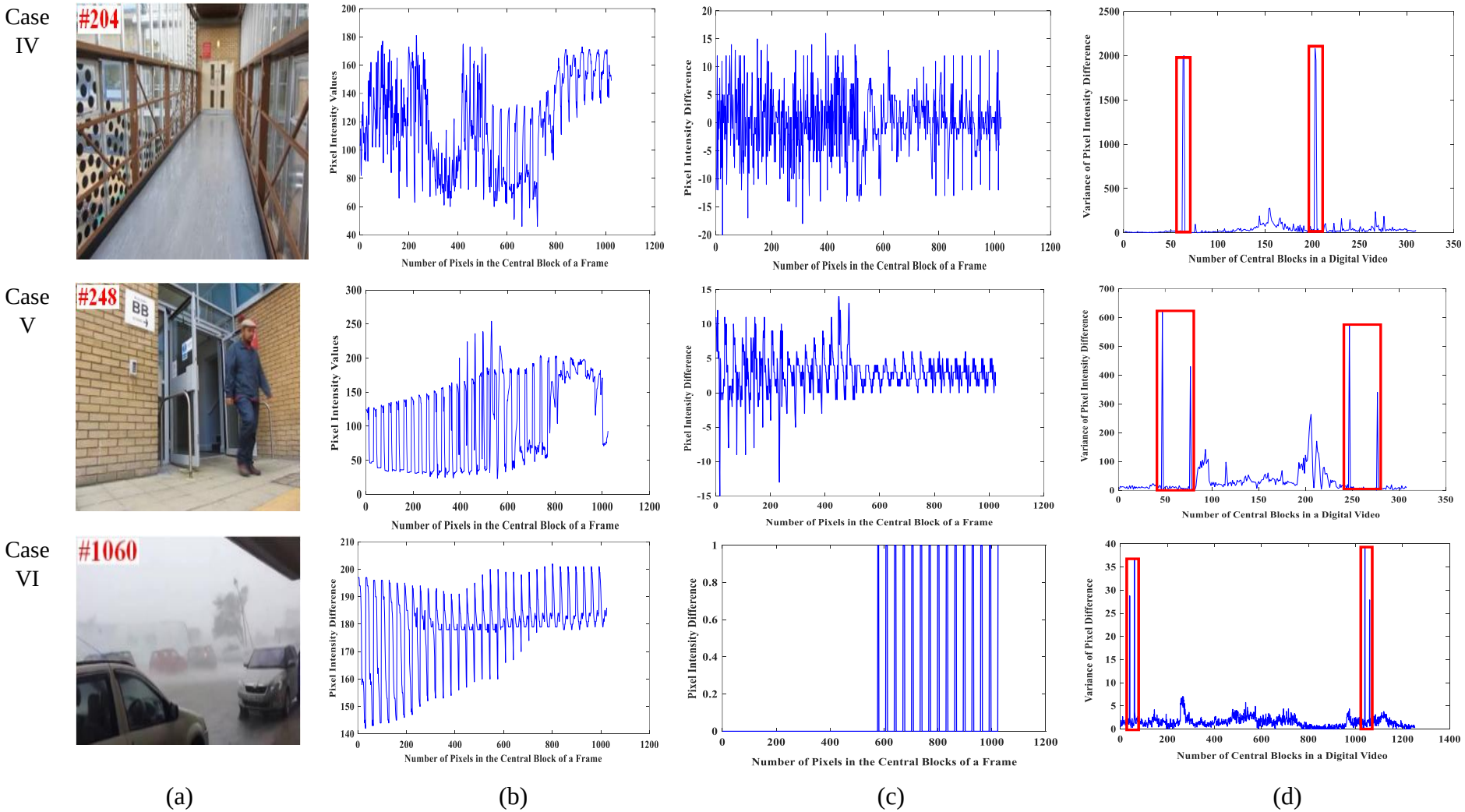


Figure 4.9: (a) Frames of digital videos with different cases (b) Pixel intensity values of a central block of frame (c) Variance of each central block of the entire digital video (d) Detection of SFS in test digital videos

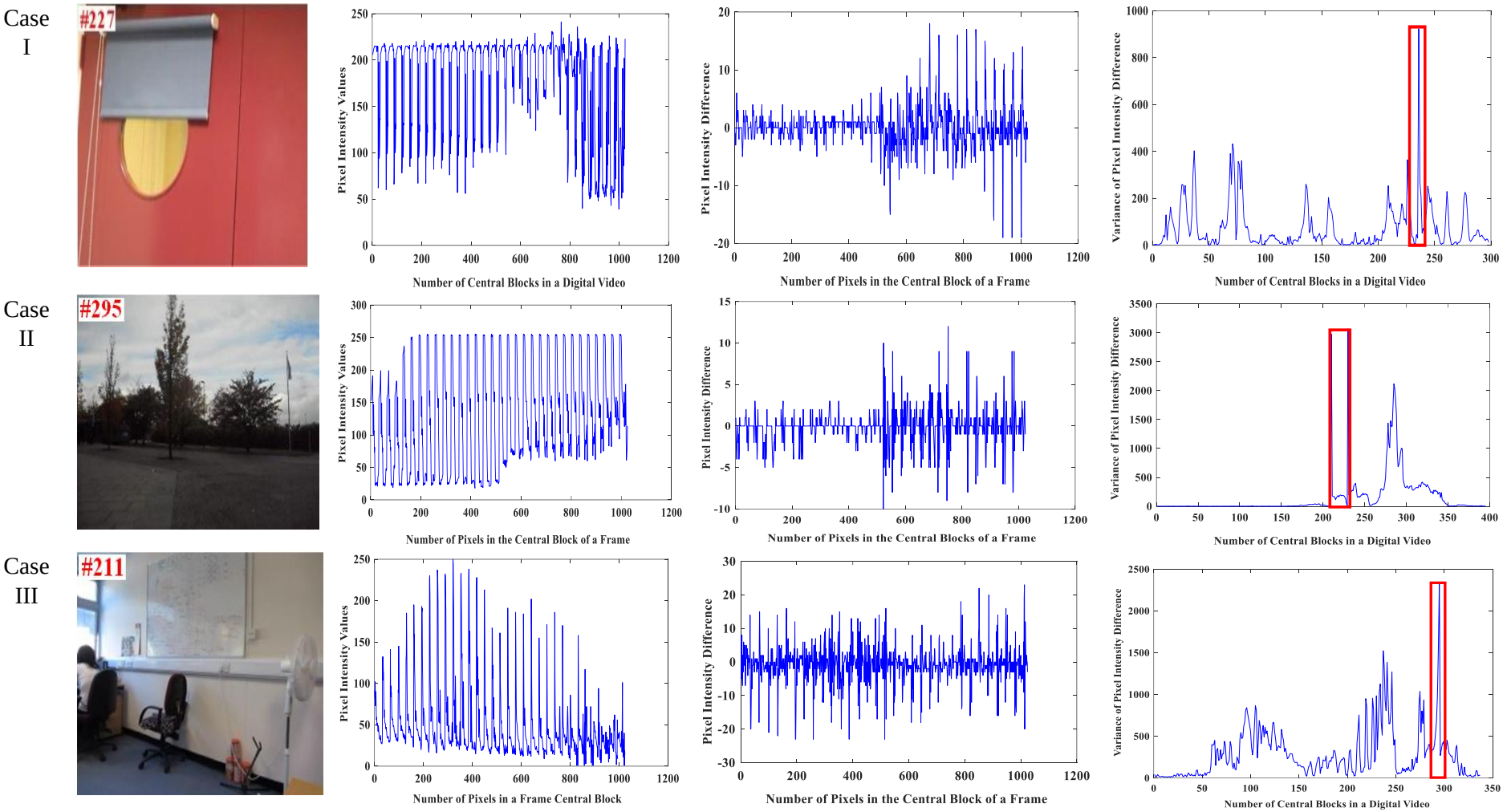


Figure 4.10: (a) Frames of different case digital videos (b) Pixel Intensity values of a Frame Central Block (c) Variance of each Central Blocks of the entire video (d) Detection of DFS in test digital videos

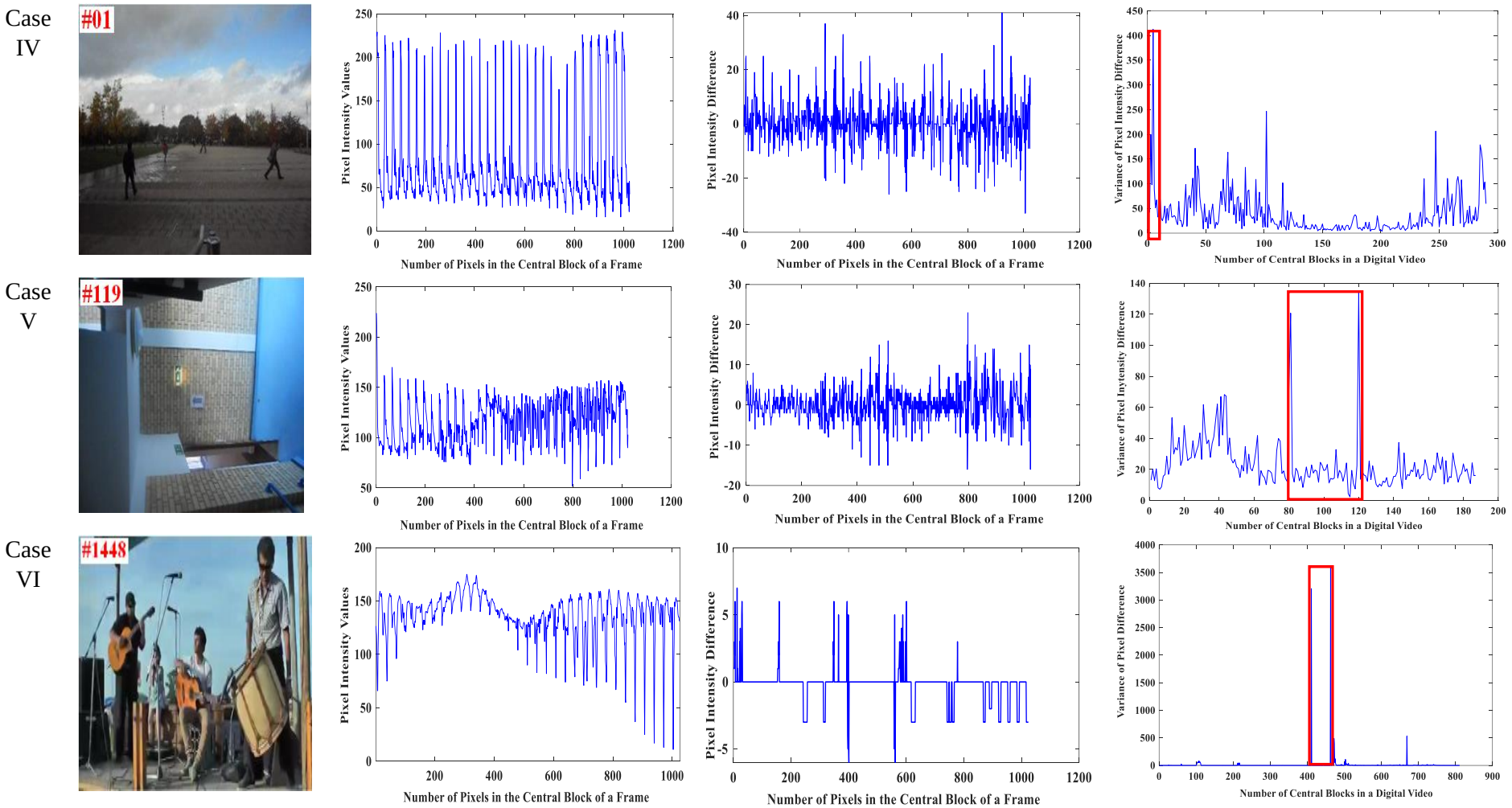


Figure 4.10: (a) Frames of digital videos with different cases (b) Pixel Intensity values of a Frame Central Block (c) Variance of each Central Blocks of the entire video (d) Detection of DFS in test digital videos

4.2.2.2 Quantitative Performance Analysis

The generated dataset has been classified for detecting multiple CMFD forgery in the digital videos based on variances of the central blocks. The selected digital videos for the training set and testing set are non-overlapping. To detect multiple CMFD forgery, each test digital video has been identified by computing the average variance and high variance between two highest peaks of pixel intensity differences in the central blocks. If average variance is less than the high variance then digital video is authentic. On other side, if average variance is more than the high variance then digital video is forged. The outcomes are labelled as authentic digital video and forged digital video. The performance of ECBV based multiple CMFD forgery detection approach has been evaluated quantitatively on different cases of the digital videos by calculating the parameters such as PR, RR, DA, F1, F2, FPR, FNR, sensitivity, specificity and execution time.

The experimental results demonstrate the effective performance of the proposed approach for detecting multiple CMFD forgery in the digital videos. The ROC curve of the testing set for the proposed approach is shown in Figure 4.11. Table 4.2 shows the performance evaluation of the proposed approach, whereas Table 4.3 provides its parameter evaluation. The proposed approach has also evaluated for detecting each CMFD forgery separately in the digital videos as shown in Table 4.4.

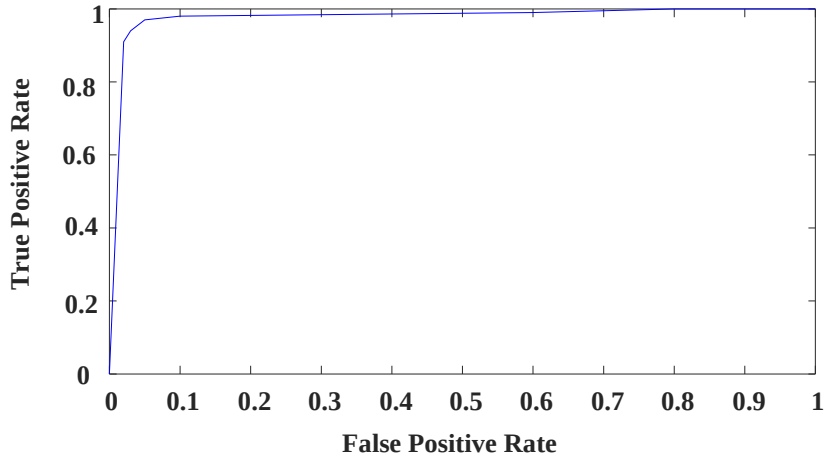


Figure 4.11: ROC curve for testing set of multiple CMFD forgery approach

Table 4.2: Performance evaluation of ECBV based multiple CMFD forgery detection approach for testing set of digital videos

	Positive	**Negative**
True	0.999	0.998
False	0.001	0.002

Table 4.3: Evaluation of different parameters of ECBV based multiple CMFD forgery detection approach

PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Selectivity**
1.000	0.9980	0.9985	0.9994	0.9991	0.0010	0.0019	0.9980	0.9989

Table 4.4: Evaluation of parameters of ECBV based multiple CMFD forgery detection approach separately

Multiple CMFD Forgeries	**PR**	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Specificity**
SDF detection	1.000	0.9990	0.9995	0.9994	0.9991	0.000	0.0009	0.999	1.000
RF detection	0.999	0.9980	0.9985	0.998	0.9981	0.001	0.002	0.998	0.9989
SFS detection	0.999	0.999	0.999	0.9994	0.999	0.001	0.001	0.999	0.999
DFS detection	0.997	0.9979	0.9975	0.9974	0.9977	0.002	0.002	0.9979	0.997

Table 4.2 indicates the values of true positives and true negatives, which shows that ECBV based multiple CMFD forgery detection approach is more effective for detecting the authentic and forged digital videos having multiple CMFD forgery. On other side, Table 4.3 shows the values of different parameters such as PR, RR, DA, F1, F2, FPR, FNR, Sensitivity and Specificity for ECBV based multiple CMFD forgery detection approach in which the proposed approach achieved the detection accuracy of 99.7% at a false negative rate of 0.05 %. Table 4.4 shows the results of the proposed approach in the form of different parameters for each multiple CMFD forgery separately.

4.3 Comparative Analysis

ECBV based multiple CMFD forgery detection approach has been compared with existing techniques such as such as Lin *et al.* [52], Kharat *et al.* [47], Wang *et al.* [112], Yang *et al.* [120], Ulutas *et al.* [106], Ulutas *et al.* [108], Ren *et al.* [83], and Singh *et al.* [101] as shown in Table 4.5.

Table 4.5: Comparison between ECBV based multiple CMFD forgery detection approach and existing techniques

	PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Specificity**
Wang *et al.* [112]	0.385	0.817	0.658	0.523	0.667	-	-	-	-
Lin *et al.* [52]	0.879	**1.000**	0.940	0.935	0.973	-	-	-	-
Ulutas *et al.*[108]	0.983	0.983	0.975	0.983	0.982	-	-	-	-
Ulutas *et al.* [106]	0.99	0.99	0.99	0.99	0.99	-	-	-	-
Yang *et al.* [120]	0.982	**1.000**	0.991	0.990	0.996	0.016	0.000	**1.000**	0.983
Singh *et al.* [101]	1.000	0.990	0.995	0.994	0.991	**0.000**	0.009	0.990	**1.000**
Kharat *et al.* [47]	0.999	0.997	0.998	0.997	0.997	-	-	-	-
Ren *et al.* [83]	0.995	1.000	-	0.997	0.995	-	-	-	-
Proposed	**1.000**	0.9980	**0.9985**	**0.9994**	**0.9991**	0.0010	0.0019	0.9980	**0.9989**

- means data has not been calculated in the existing techniques and bold indicates higher values of parameters.

The comparative analysis of the proposed approach and existing techniques has shown in Table 4.5 in terms of PR, RR, DA, F1, F2, FPR, FNR, sensitivity and specificity for detecting multiple CMFD forgery in the digital videos. It indicates that DA of the proposed approach is higher than the existing techniques. It also shows the improved parameters such as F1 score, sensitivity and specificity of the proposed approach. Therefore, these experimental results show the better performance of the proposed approach for detecting multiple CMFD forgery in the digital videos with different cases.

4.4 Computational Cost

The average run time of ECBV based multiple CMFD forgery detection approach is 0.018 s per frame and 0.092 s per frame for 320× 240 resolution videos and 720 × 576 resolution digital videos respectively as shown in Table 4.6. The execution time of the proposed approach is also compared with that of existing techniques which indicate the minimum execution time of the proposed approach. The fact is that in this approach, the central block of each frame has been used for detecting the multiple CMFD forgery rather than the entire frames of the digital video. It reduces the more execution time for the processing of proposed approach. Therefore, the ECBV based multiple CMFD forgery detection approach provides minimum execution time.

Table 4.6: Comparison of the execution time of the proposed approach with existing techniques

Video Resolution	**Video Type**	**Execution Time (sec/frame)**				
		Ulutas *et al.*[106]	Ulutas *et al.* [108]	Yang *et al.*[120]	Singh *et al.* [101]	**Proposed**
320 × 240	Forged	0.1	0.07	0.090	0.024	**0.018**
720 × 576	Forged	-	-	0.346	0.149	**0.092**
640×480	Forged	-	-	0.358	0.118	**0.065**
384×288	Forged	-	-	-	0.084	**0.039**
240×160	Forged	-	-	-	0.121	**0.043**
1024×768	Forged	-	-	-	1.59	**0.327**
1280 × 720	Forged	-	-	-	0.983	**0.574**

- means data has not been calculated in the existing techniques and bold indicates higher values of parameters.

4.5 Summary

In this chapter, ECBV based multiple CMFD forgery detection approach has detected multiple CMFD forgery such as (i) single duplicated frame in the entire digital video, (ii) repetition of a frame in the form of a frame sequence, (iii) shuffled frame sequence and (iv) disorder frame sequence in the digital videos. The digital videos are taken from the SULFA dataset and the internet to evaluate the proposed approach's performance. This approach has provided better results on accurately detecting multiple CMFD forgery. It has also provided minimum execution time on digital videos having different resolutions. Therefore, ECBV based multiple

CMFD forgery detection approach outperforms the existing approaches as evident from the simulation results. After that, the next chapter will deal with the development of an innovative approach for detecting CMRD forgeries within the same frame and from other frames of the digital videos.

CHAPTER 5

REGULAR AND IRREGULAR CMRD FORGERY DETECTION

This chapter is focused on the improvement of CMRD forgery detection in the digital videos. The proposed approach has been found CMRD forgery in two forms in this chapter such as (i) regular region duplication and (ii) irregular region duplication in the digital videos. In the detection of regular region duplication, the rectangular and square shape duplicated regions have been detected by the proposed approach in the digital videos. On other side, in irregular region duplication detection, the duplicated regions with many irregularities have been detected in the digital videos. The performance of proposed approach has been evaluated on the digital videos which are taken from SULFA dataset and the internet with different resolutions. The proposed approach has also been compared with the existing techniques which provides better results on the detection of CMRD forgery in the digital videos.

5.1 Coefficients Based CMRD Forgery Detection Approach

Coefficients based CMRD forgery detection approach detects the regular and irregular duplicated regions within same or from another frame of digital video. In region duplication within the same frame, the regular or irregular region is copied from one location of a frame and moved it to other location within the same frame. These region duplications have been processed in the frame sequence of digital video. On the other hand, in region duplication from another frame, the regular or irregular region is copied from one location of a frame and moved to another frames of the digital video at same locations. It is observed that the pixel intensity values of a copied region are slightly changed from its authentic region. Therefore, both regions indicate as distinct from each other in the frame of a digital video. Figure 5.1 shows the flow diagram of coefficients based CMRD forgery detection approach for detecting both forms of CMRD forgery in the digital videos. Firstly, the number of frames are extracted by coefficients based CMRD forgery detection approach from input digital video. Each extracted RGB frame of digital video is converted into the grayscale frame as shown in Figure 5.2. The matrices of these grayscale frames are converted into vectors so that each vector is subtracted from its previous/next vector. This subtraction results into a vector difference for each frame of a digital video as shown in Figure 5.3 (a). Therefore, a grayscale

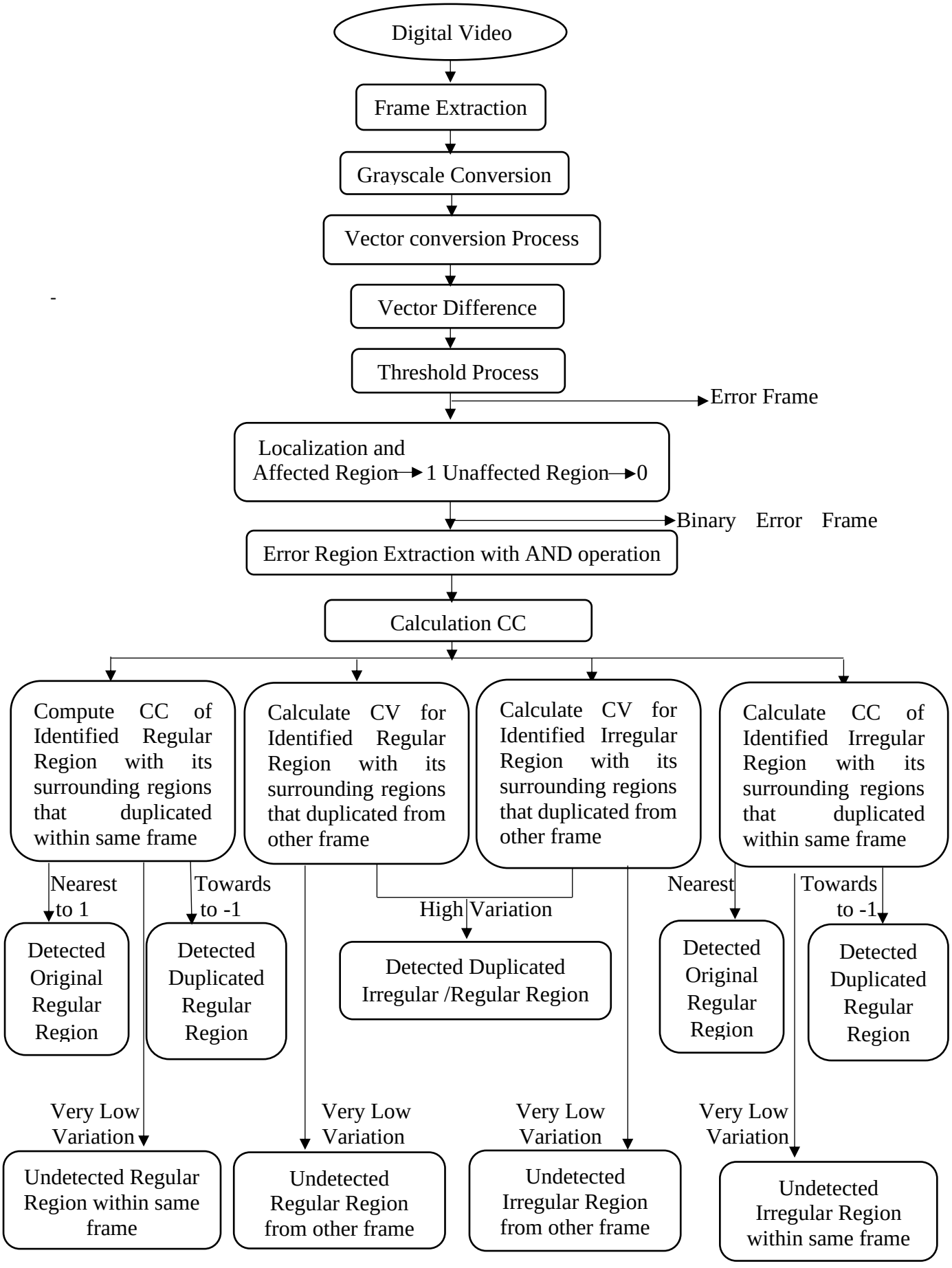


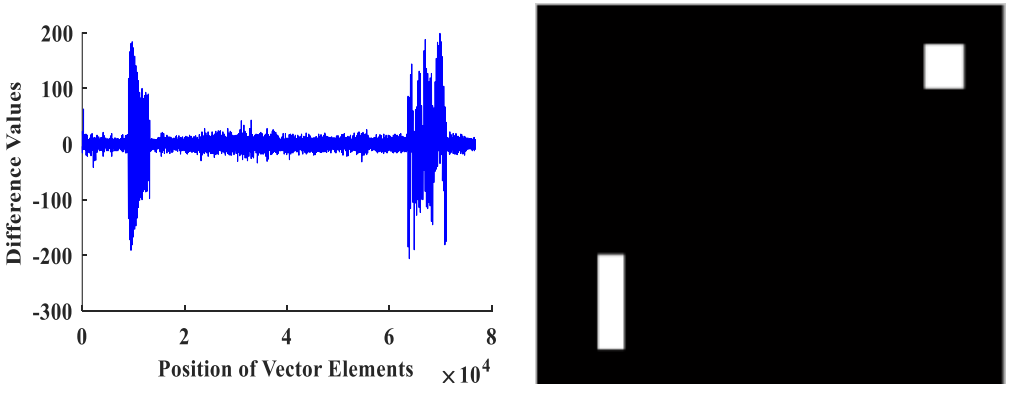
Figure 5.1: Flow diagram of coefficients based CMRD forgery detection approach

(a) (b)

Figure 5.2: (a) RGB frame (b) Gray scale frame

matrix is converted into the vector in order to plot a vector difference which shows the pixel intensity variations. This vector difference is retransformed into matrix to obtain a binary error frame which has been made by assigning the value '1' to identified duplicated region and '0' to the remaining authentic portion of frame as shown in Figure 5.3 (b). Thus, the pixel intensity values of an identified region and its surrounding regions are extracted by performing AND operation between each grayscale frame and its corresponding binary error frame.

When a region is copied and moved it very near to its authentic region, then the variation in the pixel intensity of copied region is very low. Figure 5.1 shows that region having very low variation are undetected.



(a) (b)

Figure 5.3: (a) Pixel difference values with error (b) Binary error frame

The duplicated region has been detected by calculating CC of identified duplicated region of the current frame with its surrounding regions and the regions which are placed at same locations in its previous or next frame as shown in Figure 5.4 and Figure 5.5. Figure 5.4 indicates CC of duplicated regular region with its surrounding regions of current frame and that of its previous frame within the same frame. Figure 5.5 shows CC of duplicated irregular region with its surrounding regions of current frame and that of its previous frame within the same frame.

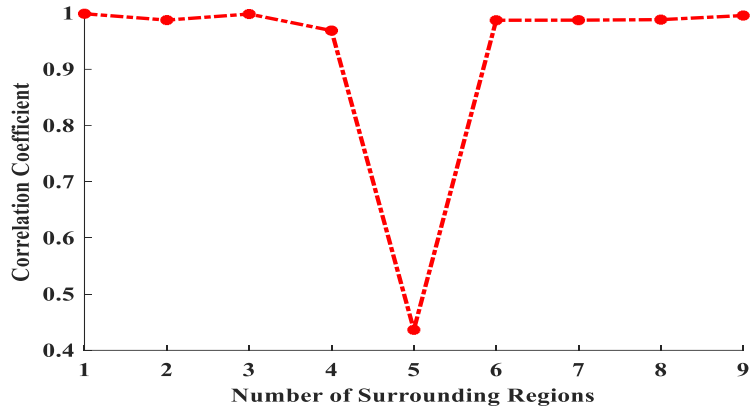


Figure 5.4: CC of identified duplicated regular region with surrounding regions in current frame and previous frame within the same frame

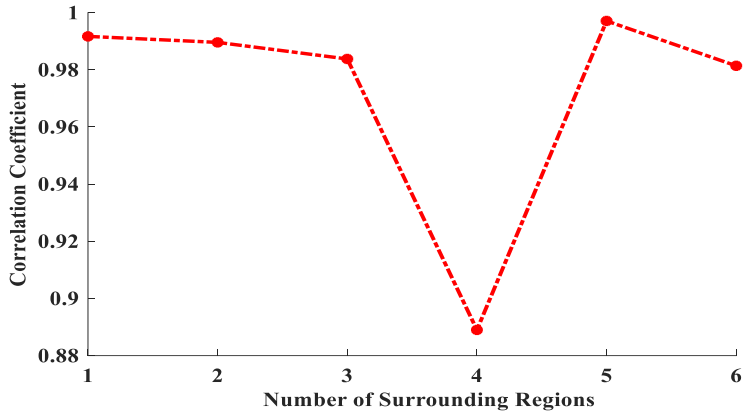


Figure 5.5: CC of identified duplicated irregular region with surrounding regions in current frame and previous frame within the same frame

During CC calculations, it has been observed that CC of identified region and authentic region are near to 1 within the same frame but not exactly 1. This is due to slight change in pixel intensity values of identified region. If these CC at same locations are near to 1 then the region of current frame is authentic. But if CC goes towards to -1, then the region is duplicated. On the other hand, when a regular or irregular region is copied from another frame and moved to consecutive frame sequence of the digital video, then the detection of this region duplication becomes more difficult because the identified regular or irregular region of current frame and previous frame provides CC near to 1 at the same locations with their surrounding regions as shown in Figure 5.6 and Figure 5.7 respectively.

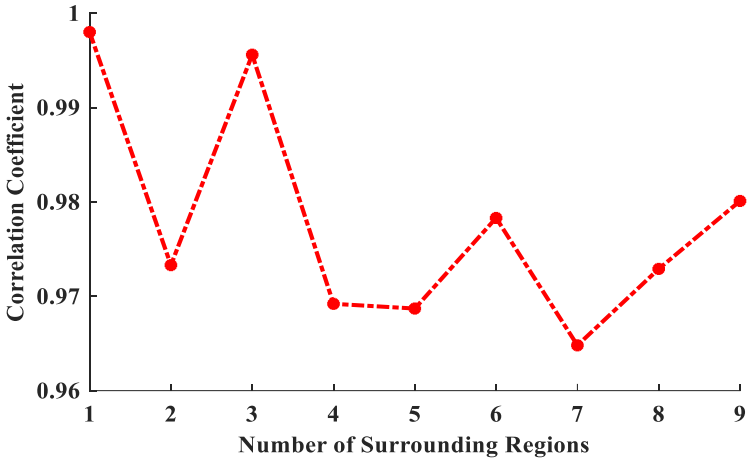


Figure 5.6: CC of non-detectable duplicated regular regions of current frame and previous frame with their surrounding regions presented at same locations

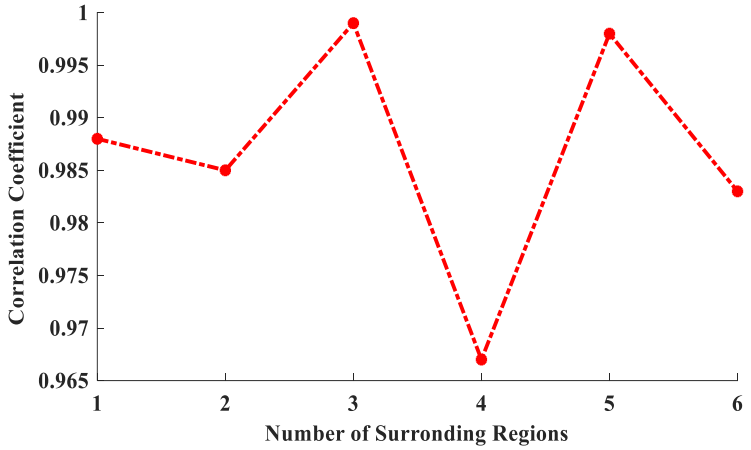


Figure 5.7: CC of non-detectable duplicated irregular regions of current frame and previous frame with their surrounding regions presented at same locations

Thus, it does not show these copied regular and irregular regions as duplicated regions in the digital video. The proposed approach has identified and detected this challenge of CMRD forgery within the digital video effectively. Therefore, for detecting the duplicated regular or irregular region from another frame, the proposed approach has calculated CV using Eq. (2.6.1) for the identified duplicated region with its surrounding regions in current frame of the digital video as shown in Figure 5.8 and Figure 5.9.

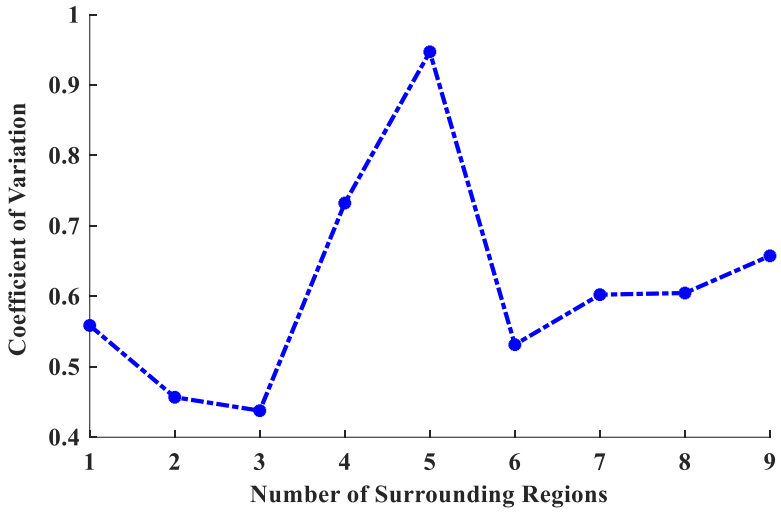


Figure 5.8: CV of the current frame for detecting the regular region duplication from another frame with its surrounding regions

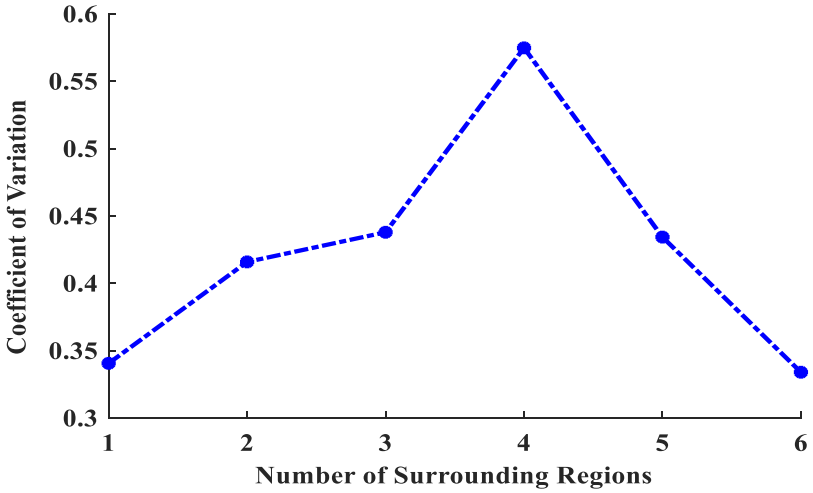


Figure 5.9: CV of the current frame for detecting the irregular region duplication from other frame with its surrounding regions

The CV calculation provides the pixel intensity variation in the regions of current frame. It provides high similarity in low variation between all authentic regions of the frame whereas, the variation within duplicated region has become higher than the authentic regions which detects the duplicated regular and irregular regions from another frame of the digital video as shown in Figure 5.8 and Figure 5.9 respectively.

5.2 Performance Analysis of Coefficients Based CMRD Forgery Detection Approach

In this section, a generated dataset has used to measure qualitatively and quantitatively the ability of coefficients based CMRD forgery detection approach. The digital videos have been taken from SULFA dataset and the internet for the generated dataset. Furthermore, the proposed approach is compared against the existing techniques of CMRD forgery detection.

5.2.1 Dataset and Setting

In order to evaluate the proposed approach for detecting CMRD forgery in digital videos, a dataset has been generated with 340 digital videos. In this dataset, out of 340 digital videos, 40 digital videos have selected for training purpose. The remaining 300 digital videos have selected for testing purpose in which 150 digital videos are authentic and 150 video are forged digital videos. These selected digital videos for training set and testing set are non-overlapping.

5.2.2 Simulation Results for Test Digital Videos of Dataset

For confirming the capability of coefficients based CMRD forgery detection approach, this approach is conducted qualitatively and quantitatively on the test digital videos from the generated dataset.

5.2.2.1 Qualitative Performance Analysis

In the qualitative performance analysis, the proposed approach has provided the experimental results for the detection of regular and irregular region duplication within the same frame and from another frame of the digital videos respectively.

5.2.2.1.1 Regular Region Duplication Detection within the Same Frame

The experimental results show the detection of duplicated rectangular and square shape regular regions in the frame sequence of digital video in this section. Figure 5.9 demostrates the detection of regular region duplication within the same frame in which a sequence of authentic frames from #242 to #246 has been shown in Figure 5.9 (a) whereas, its forged frame sequence has been shown in Figure 5.9 (b). This forged frame sequence is affected by rectangular and square shape regular region duplication within the same frame.

(a)

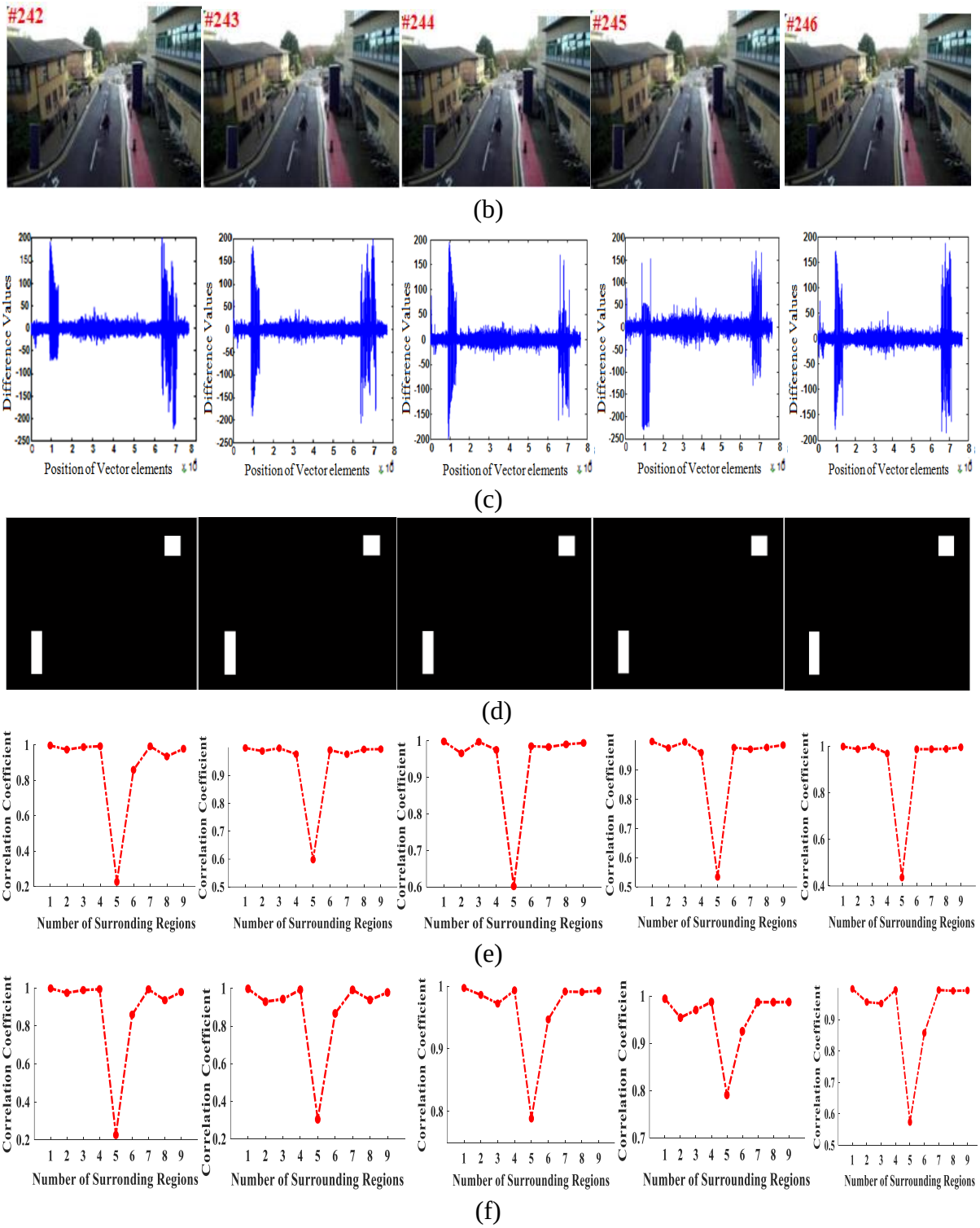


Figure 5.10: (a) Authentic frame sequence from #242 to #246 of digital video (b) Forged frame sequence from #242 to #246 of digital video (c) Difference in pixel intensity values with errors in each vector of consecutive frames from #242 to #246 (d) Identification and localization of duplicated rectangular and square shape regular region within the same frame (e) CC of identified rectangular regular region with its surrounding regions in current frame and its

previous frame (f) CC of identified square regular region with its surrounding regions in current frame and its previous frame

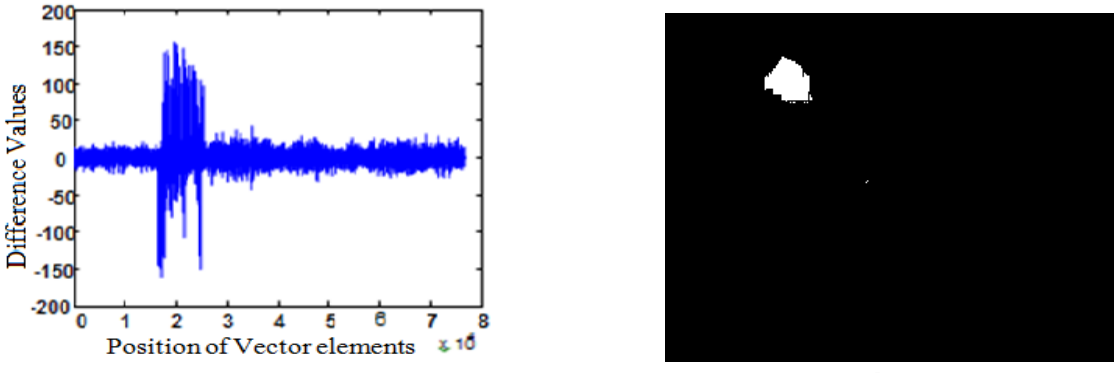
The difference in pixel intensity values of each vector has been shown two errors in each frame as shown in Figure 5.10 (c). From these errros, the duplicated rectangular and square shape regular regions have been identified and localized in the each binary frame as shown in Figure 5.10 (d). The CC of identified duplicated rectangular and seqaue shape regular regions with their surrounding regions of current frame and those of the previous frame have been shown in Figures 5.10 (e) and 5.10 (f) respectively which detects the duplicated rectangular and square shape regular regions within the same frames of the digital video. Figure 5.10 (e) and Figure 5.10 (f) also indicate that the CC of authentic regions are very close to each other, whereas the CC of duplicated regions are far away from those of authentic regions.

5.2.2.1.2 Irregular Region Duplication Detection within Same Frame

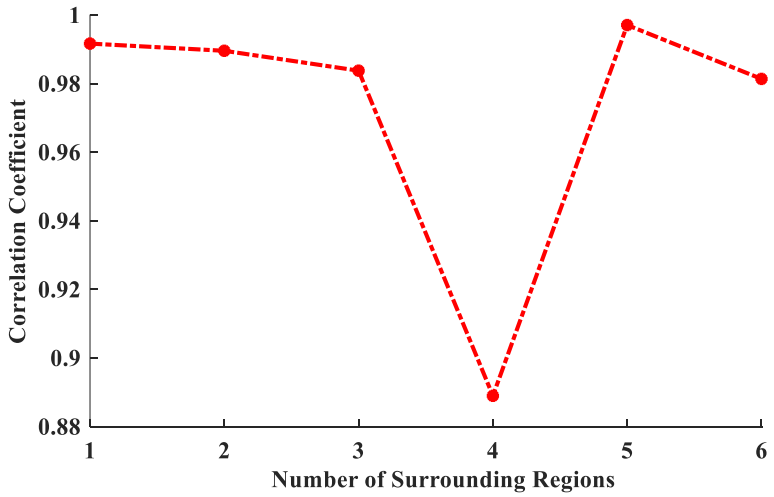
The coefficients based CMRD forgery detection approach has detected effectively irregular region duplication within the same frame as shown in Figure 5.11. Figure 5.11 (a) and Figure 5.11 (b) show the consecutive frames in frame sequence of the digital video. The difference between pixel intensity values of vectors provides an error within the same frame as shown in Figure 5.11 (c). The duplicated irregular region has been identified and localized within binary frame as shown in Figure 5.11 (d).

(a) (b)

Figure 5.11: (a) and (b) consecutive frames with duplicated irregular region in the same frame



(c) (d)



(e)

Figure 5.11: (c) Difference in pixel intensity values with error (d) Binary Frame (e) CC of identified irregular region with its surrounding regions in current frame and previous frame

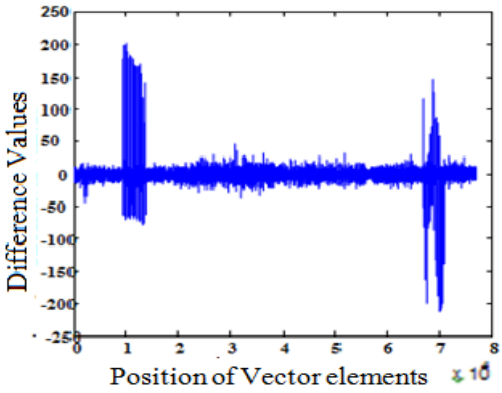
The CC of identified region with its surrounding regions of current frame and previous frame have been shown in Figure 5.11 (e) which detects the irregular region dulication within same frame of the digital video. It also shows that the CC of authentic regions are very close to each other whereas, the CC of duplicated region is far away from that of authentic regions.

5.2.2.1.3 Regular Region Duplication Detection from Another Frame

The proposed approach has well performed for detecting the regular region duplication from another frame of the digital video. Figure 5.12 (a) and Figure 5.12 (b) show the consecutive frames with duplicated regular regions from another frame in the frame sequence of digital video. The difference in pixel intensity values between vectors has been attained by the proposed approach which indicates two errors in the frame as shown in Figure 5.12 (c). The rectangular and square shape regular regions, which are duplicated from another frame, have been identified and localized in the binary frame as shown in Figure 5.12 (d).

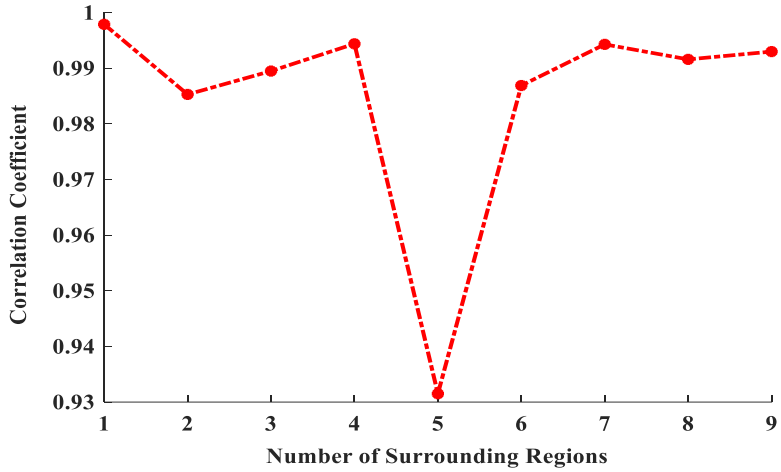
(a) (b)

Figure 5.12: (a) and (b) consecutive frames with duplicated irregular region in the same frame

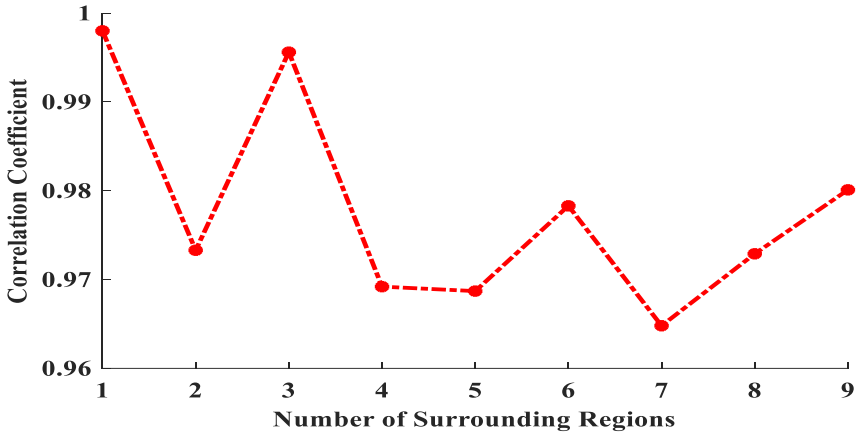


(c)

(d)

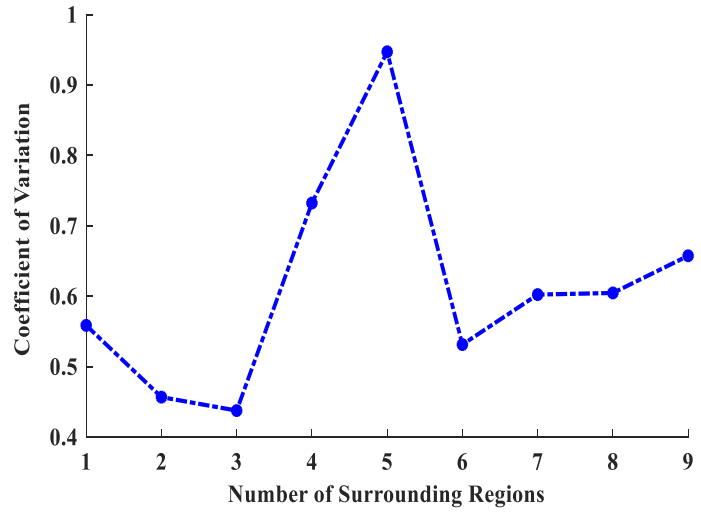


(e)

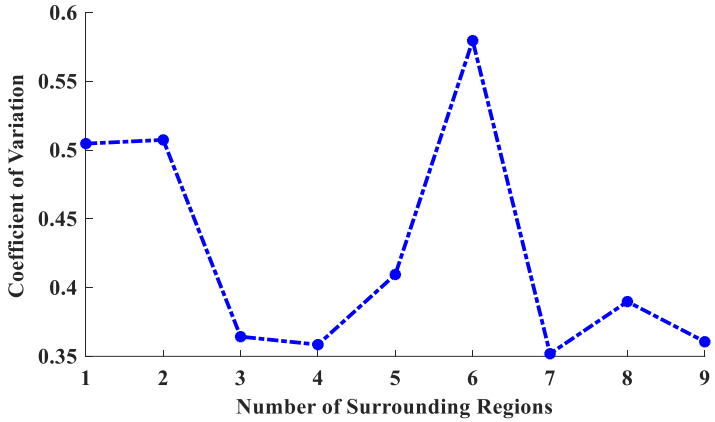


(f)

Figure 5.12: (c) Difference in pixel intensity values with error (d) Binary Frame (e) CC of non-detectable duplicated rectangular regular region with its surrounding regions in current frame and previous frame (f) CC of non-detectable duplicated square regular region with its surrounding regions in current frame and previous frame



(g)



(h)

Figure 5.12: (g) CV of duplicated rectangular regular region with its surrounding regions within the current frame (h) CV of duplicated square regular region with its surrounding regions within the current frame

It has been observed that the CC of non-detectable duplicated rectangular regular region and its surrounding regions in current frame and previous frame are very near to 1 as shown in Figure 5.12 (e). Similarly, the CC of non-detectable duplicated square regular region and its surrounding regions in current frame and previous frame are also very close to 1 as shown in Figure 5.12 (f). Figures 5.12 (e) and (f) do not show the rectangular and square shape regular regions as duplicated regions which are copied from another frame in the digital video. Therefore, the above identified rectangular and square shape regular regions have been detected by computing the CV in identified region with its surrounding region of current frame. The CV in each surrounding region is correlated to each other because these regions are authentic in the frame of digital video whereas, the CV in duplicated region is completely different from that of its surrounding regions as shown in Figure 5.12 (g) and (h). Figure 5.12 (g) and (h)

indicate the detection of duplicated rectangular and square shape regular regions from another frame using CV in duplicated regions and their surrounding regions.

5.2.2.1.4 Irregular Region Dulication Detection from Another Frame

The proposed approach has also detected the irregular region duplication from another frame effectively as shown in Figure 5.13. Figure 5.13 (a) and Figure 5.13 (b) show the consecutive frames with duplicated irregular region from another frame. The difference between pixel intensity values of vectors has been shown an error to recognize the duplicated irregular region in the frame as shown in Figure 5.13 (c). The duplicated irregular region has been identified and localized within the binary frame as shown in Figure 5.13 (d).

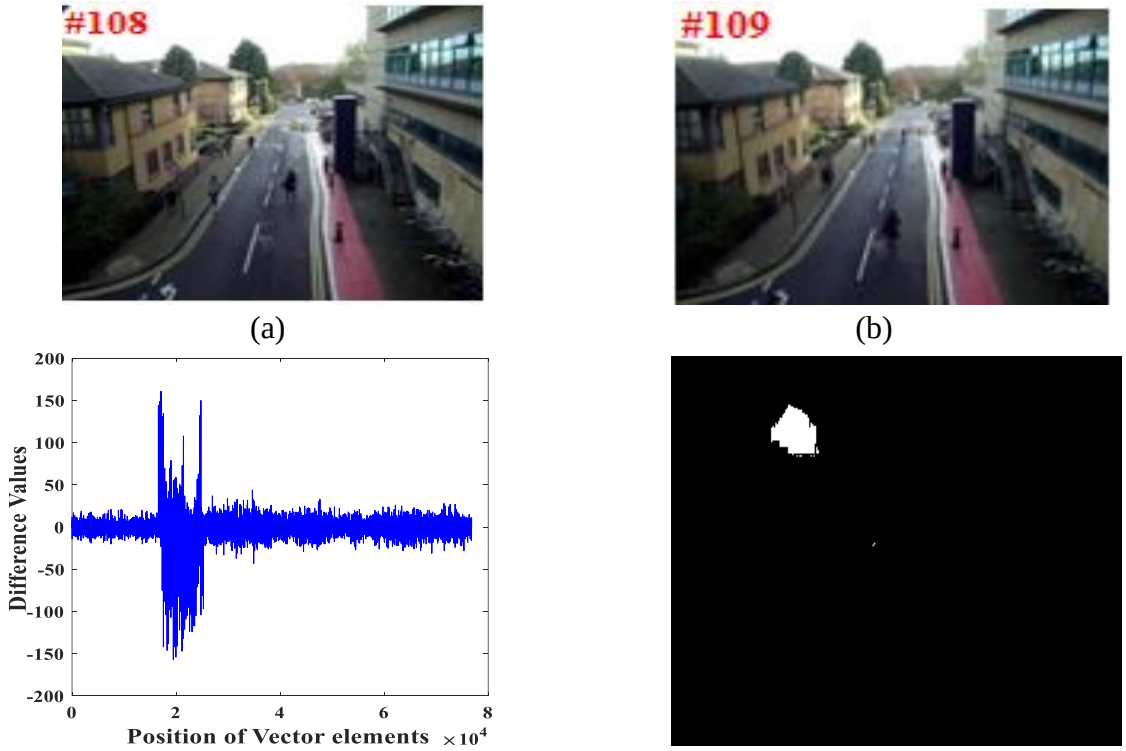
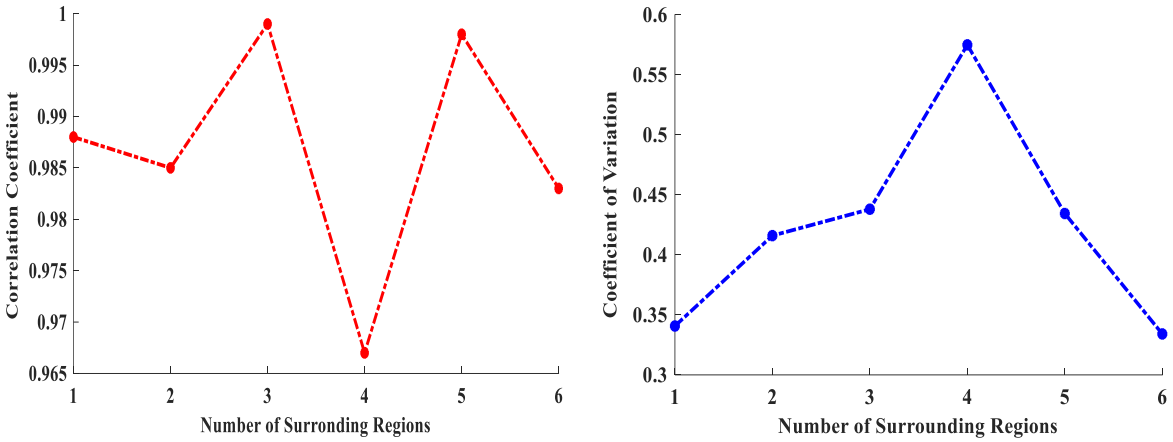


Figure 5.13: (a) and (b) Consecutive frames with duplicated irregular region from another frame (c) Difference in pixel intensity values with error (d) Binary Frame



(e) (f)

Figure 5.13: (e) CC of non-detectable duplicated irregular region with its surrounding regions in current frame and previous frame (f) CV of duplicated irregular region with its surrounding regions in the current frame

In this case, it has also been observed that the CC of non-detectable duplicated irregular region and its surrounding regions of current and previous frame are near to 1 as authentic regions of the frame which is shown in Figure 5.13 (e). This irregular region has been detected by computing the CV in identified region with its surrounding region of the current frame. The CV in each surrounding region is correlated to each other because these regions are authentic in the frame of digital video whereas, the CV in duplicated region is completely different from that of its surrounding regions as shown in Figure 5.13 (f). Figure 5.13 (f) indicates the detection of duplicated irregular region from other frame using CV in the duplicated region and its surrounding regions of the current frame.

5.2.2.2 Quantitative Performance Analysis

Besides the simmulation results, the parameters such as PR, RR, DA, F1, F2 and execution time [59], [108], [115], [121], and [123] have been calculated for evaluating the performance of coefficients based CMRD forgery detection approach in the digital videos.

The generated dataset has been classified for the detection of CMRD forgery in the digital videos which is based on coefficient values of the identified region and its surrounding regions. For the detection of both forms of CMRD forgery, each test digital video has been identified by calculating CC and CV of the identified region and its surrounding regions in each frame of the digital video. If CC < 0.90 or CV >0.5 then the outcomes are labelled as forged digital video. Otherwise, the outcomes are labelled as authentic digital video. The performance evaluation of coefficients based CMRD forgery detection approach has been shown in Table

5.1 whereas, Table 5.2 indicates the evaluation of different parameters for the proposed approach.

Table 5.1: Performance evaluation of coefficients based CMRD forgery detection approach for testing set of digital videos

	Positive	**Negative**
True	1	0.933
False	0	0.067

Table 5.2: Perameters evaluation of coefficients based CMRD forgery detection approach

PR	**RR**	**DA**	**F1**	**F2**
1.000	0.933	0.966	0.965	0.945

Table 5.1 shows the effective performance of coefficients based CMRD forgery detection approach for detecting the authentic and forged digital videos. Table 5.2 provides the values of different parameters PR, RR, DA, F1, and F2 of proposed approach such as 1, 0.933, 0.966, 0.965 and 0.945 respectively which gives better results. These results show the efficient capability of proposed approach for detecting CMRD forgery in the digital videos.

5.3 Comparative Analysis

The coefficients based CMRD forgery detection approach has been compared with existing techniques for the detection of CMRD forgery in the digital videos in terms of PR, RR, DA, F1, and F2 as shown in Table 5.3. The existing techniques are represented in Table 5.3 such as Wang *et al.* [112] used own dataset, Su *et al.* [94] used own dataset, Subramanyam *et al.* [92] used SULFA dataset, Bestagini *et al.* [7] used SULFA dataset, and Pun *et al.* [79] used own dataset. Table 5.3 indicates the higher detection accuracy of coefficients based CMRD forgery detection approach than the existing techniques. The proposed approach also provides the values of parameters PR, RR, F1 and F2 such as 1.000, 0.933, 0.965 and 0.945 respectively. This shows the effective performance of the proposed approach for detecting CMRD forgery in the digital videos.

Table 5.3: Comparison between coefficients based CMRD forgery detection approach and existing techniques

	DA
Wang *et al.* [112]	0.700
Subramanyam *et al.* [92]	0.897
Pun *et al.* [79]	0.908
Bestagini *et al.* [7]	0.91
Su *et al.* [94]	0.926
Proposed	**0.966**

Bold indicates higher values of parameters.

Furthermore, the values of parameters PR and RR show the better ability to detect the authentic and forged digital videos. Besides, F1 and F2 scores demonstrates the effectiveness of proposed approach.

5.4 Computational Cost

The execution time of the proposed approach has been calculated for detecting CMRD forgery in the digital videos having different resolution such as 720 × 576, 640 × 480, 320 × 240, 240 × 160, 384 × 288, 1024 × 768, 1280 × 720 as shown in Table 5.4.

Table 5.4: Execution time of coefficients based CMRD forgery detection approach

Resolutions	720 × 576	640× 480	320× 240	240× 160	384× 288	1024× 768	1280× 720
Execution Time in f/s	0.65	0.62	0.46	0.46	0.59	0.70	1.50

These execution times have also been compared with that of existing techniques as shown Table 5.5. Table 5.5 demonstrates the better performance in execution time because there is no need of frame segmentation in the proposed approach. Therefore, the proposed approach provides higher efficiency for detecting CMRD forgery in the digital videos than existing techniques.

Table 5.5: Comparison of execution time for the proposed approach with existing techniques

Resolution	Su *et al.* [94]	Wang *et al.* [112]	Pun *et al.* [79]	Subramanyam *et al.* [92]	**Proposed**
1280 × 720	**1.47**	3.40	> 6.66	> 6.66	1.50
720 × 576	-	-	-	-	**0.65**
1024 × 768	1.03	2.28	9.78	>10	**0.70**
240 × 160	-	-	-	-	**0.46**
640 × 480	0.65	1.37	7.52	>10	**0.62**
320 × 240	**0.36**	0.70	3.13	6.97	0.46
384 × 288	-	-	-	-	**0.59**

- means data has not been calculated in the existing techniques and bold indicates higher values of parameters.

5.5 Summary

In this chapter, CMRD forgery detection approach is based on coefficients. It has been detected rectangular and square shape regular duplicated regions as well as irregular region within the same frame and from another frame using CC and CV respectively. The performance of proposed approach has been evaluated on the digital videos which are taken from SULFA dataset and the internet with different resolutions. This approach has provided better results for detecting the regular and irregular duplications in CMRD forgery. The proposed approach has also provided better execution time on digital videos of different resolutions. Therefore, it is apparent that coefficients based on CMRD forgery detection approach has outperformed the existing techniques. It further encouraged for detecting the CMRD forgery with different region size in the digital videos. Hence, the next chapter deals with the implementation of a new approach for detecting single and multiple CMRD forgery having different region size in the digital videos.

CHAPTER 6

MULTIPLE CMRD FORGERY DETECTION WITH DIFFERENT REGION SIZE

The research work of last chapter has been enhanced towards the detection of CMRD forgery with different region size in the digital video. The proposed approach detects the single and multiple CMRD forgeries of different region sizes such as 3× 3, 4× 4, 8×8, 16×16, 24× 24, and 32× 32 in digital videos. The performance of proposed approach has been examined with digital videos having different resolutions taken from SULFA dataset and the internet. The proposed approach has been compared with existing techniques in which it provides better results for the detection of single and multiple CMRD forgeries in the digital videos than others.

6.1 Multiple CMRD Forgery Detection Approach

Multiple CMRD forgery detection approach is based on HE which detects the single and multiple CMRD forgeries of different region sizes. HE distributes the pixel intensity values uniformly over a large intensity range in the blocks of each frame which enable to detect a small duplicated region of frame in the digital video. The flow diagram of multiple CMRD forgery detection approach is shown in Figure 6.1.

The proposed approach extracts the number of RGB frames from input digital video. These extracted RGB frames are converted into grayscale frames. Each grayscale frame is divided into the number of blocks which are made by sliding a square-shaped block over the grayscale frame from the top-left pixel to the bottom-right pixel. After dividing the frames into blocks, HE is applied to each block of frame. It improves the contrast of each block which may be either blurred or have a bright or dark background and foreground. The low contrast frames usually have histograms within a narrow range of values due to which a small duplicated region of frame is difficult to detect. Therefore, HE is applied to each block of all frames. It distributes the pixel intensity values uniformly over a large intensity range. Therefore, the bins of histogram of a block will be perfectly flat as bar chart which is easy to understand as shown in Figure 6.2. The frequency in this histogram tells how many times each pixel occurs in a block. Now, histograms with equal number of frequencies are identified in order to reduce the number of blocks in each frame. It decreases the execution time of the proposed approach.

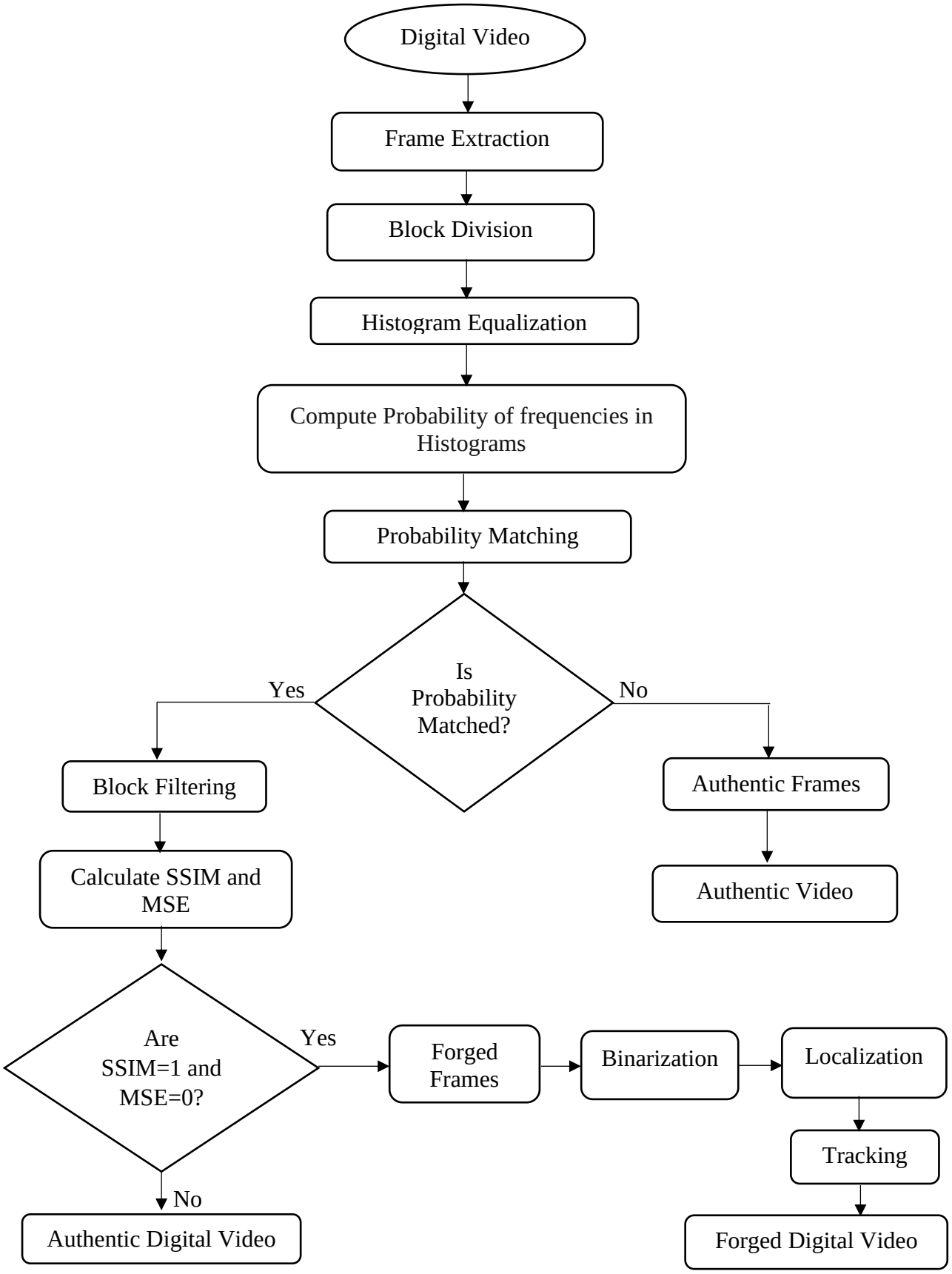


Figure 6.1: Flow diagram of multiple CMRD forgery detection approach time of the proposed approach for detecting the duplicated region in digital video.

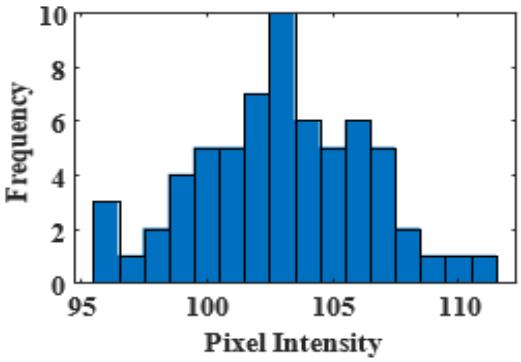


Figure 6.2: HE of a block

Figure 6.3 shows the number of histograms with equal frequency count in the entire digital video. Each frequency will be integer. Therefore, the probabilities (p) of these frequencies have been calculated using Eq. (6.1) [102] to eliminate a number of false negatives.

$$p = \frac{\text{Number of pixels of intensity level i}}{\text{Total number of pixels in a block}} \tag{6.1}$$

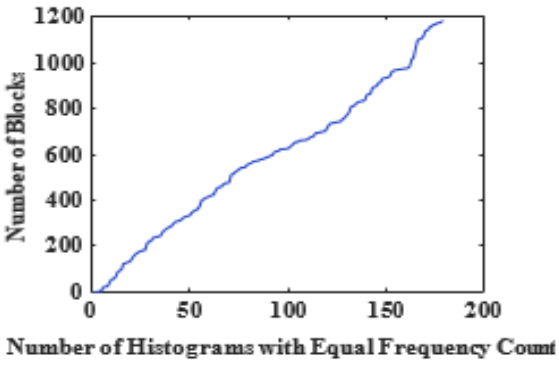


Figure 6.3: Detection of histograms with equal number of frequencies

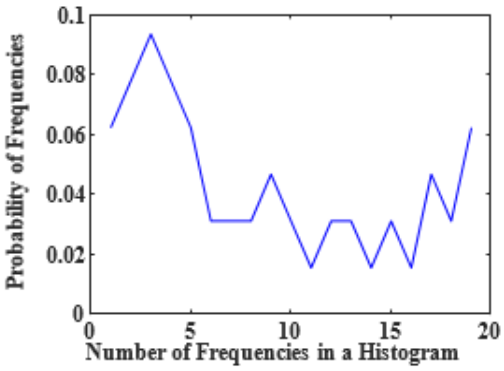


Figure 6.4: Probabilities (p) of each frequency in a histogram

These probabilities of a histogram are compared with those of other histograms to identify the similar block in each frame. This reduces the number of false positives and false negatives in the detection process. When the probabilities of a histogram are not matched with those of other histogram then its corresponding block is identified as authentic block. If the probabilities of histograms are matched then their corresponding blocks are collected to verify their authenticity. For verifying these blocks, the block filtering is used to remove the false positives and negatives. In block filtering, SSIM and MSE are calculated between blocks having matched probabilities. If SSIM and MSE between these blocks are unity and zero respectively then blocks are similar and replicated to each other. After identifying the similar and replicated blocks, the duplicated region has been differentiated from its authentic region by calculating SSIM and MSE between similar blocks and their neighbour blocks. If SSIM and MSE between them are near to 1 and 0 respectively then the blocks are authentic blocks and video is authentic

digital video. On other side, if SSIM and MSE are near to -1 and 1 respectively, then the blocks are forged blocks and video is forged digital video.

(a) (b) (c)

Figure 6.5: (a) Binarization of the forged frame with duplicated region (b) Localization of duplicated region in grayscale frame (c) Tracking of duplicated region in RGB frame

The forged frame is converted into binary frame in which all pixel values of detected duplicated region become '1' and remaining part of frame becomes '0' as shown in Figure 6.5 (a). For finding the location of duplicated region in the frame of digital video, the localization process has been done as shown in Figure 6.5 (b). Then, this duplicated region has been tracked in RGB frame of the digital video as shown in Figure 6.5 (c).

6.2 Performance Analysis of Multiple CMRD Forgery Detection Approach

The capability of multiple CMRD forgery detection approach is confirmed both qualitatively and quantitatively by taking a generated dataset in which digital videos have been taken from SULFA dataset and the internet. Moreover, the proposed approach is compared against the existing approaches.

6.2.1 Dataset and Setting

In order to evaluate the proposed multiple CMRD forgery detection approach in the digital videos, a dataset has been generated with 350 digital videos. In this dataset, out of 350 digital videos, 50 digital videos have been selected for training purpose whereas, remaining 300 digital videos have been selected for testing purpose in which 150 videos are authentic digital videos and 150 video are forged digital videos. These selected videos for training set and testing set are non-overlapping.

6.2.2 Simulation Results for Test Digital Videos of Dataset

The qualitative and quantitative analysis is conducted on the test digital videos from the dataset for confirming the capability of multiple CMRD forgery detection approach. The detail of some digital videos have been provided for the detection of multiple CMRD forgery within different region size in Table 6.1. Table 6.1 shows the video names like Video_1, Video_2 etc., different

video resolutions, video formats used in dataset as .mov, .avi and .mp4. It also indicates the types of digital video such as forged and authentic videos.

Table 6.1: Detail of some test digital videos used for multiple CMRD forgery detection

Video Name	Video Resolution	Video Format	Video Type
Video_1	320 × 240	.mov	Forged
Video_2	320 × 240	.avi	Forged
Video_3	320 × 240	.avi	Forged
Video_4	320 × 240	.mov	Forged
Video_5	1024×768	.avi	Authentic
Video_6	1024×768	.mov	Forged
Video_7	1024×768	.avi	Forged
Video_8	1024×768	.avi	Forged
Video_9	720 × 576	.avi	Forged
Video_10	720 × 576	.avi	Authentic
Video_11	720 × 576	.mov	Forged
Video_12	720 × 576	.avi	Forged
Video_13	720 × 576	.avi	Forged
Video_14	720 × 576	-.avi	Forged
Video_15	640 × 480	.avi	Authentic
Video_16	640 × 480	.mov	Forged
Video_17	640 × 480	.avi	Forged
Video_18	240×160	.avi	Forged
Video_19	240×160	.avi	Forged
Video_20	384 × 288	.avi	Authentic
Video_21	320 × 240	.mp4	Forged
Video_22	320 × 240	.mp4	Forged
Video_23	320 × 240	.mp4	Authentic
Video_24	320 × 240	.mp4	Forged
Video_25	320 × 240	.mp4	Forged

6.2.2.1 Qualitative Performance Analysis

In the qualitative performance analysis, the proposed approach has provided the experimental results for the detection of multiple CMRD forgery in digital videos. HE of a block of different digital video frames have been shown in Figure 6.6 (a). It shows frequencies of each pixel intensity in the histograms of different size blocks. Whereas, the detection of histograms with equal frequency count have been shown in Figure 6.6 (b). The probabilities of frequencies in histograms have been shown in Figure 6.6 (c). It provides the probability of each frequency in a histogram of different size blocks. In the Figure 6.6, the number of Histograms and blocks represent the quantities of Histograms and blocks which are showing as increasing due to different resolutions. This Figure shows that the x^{th} histogram having equal count on X axis is related to y^{th} block on Y axis.

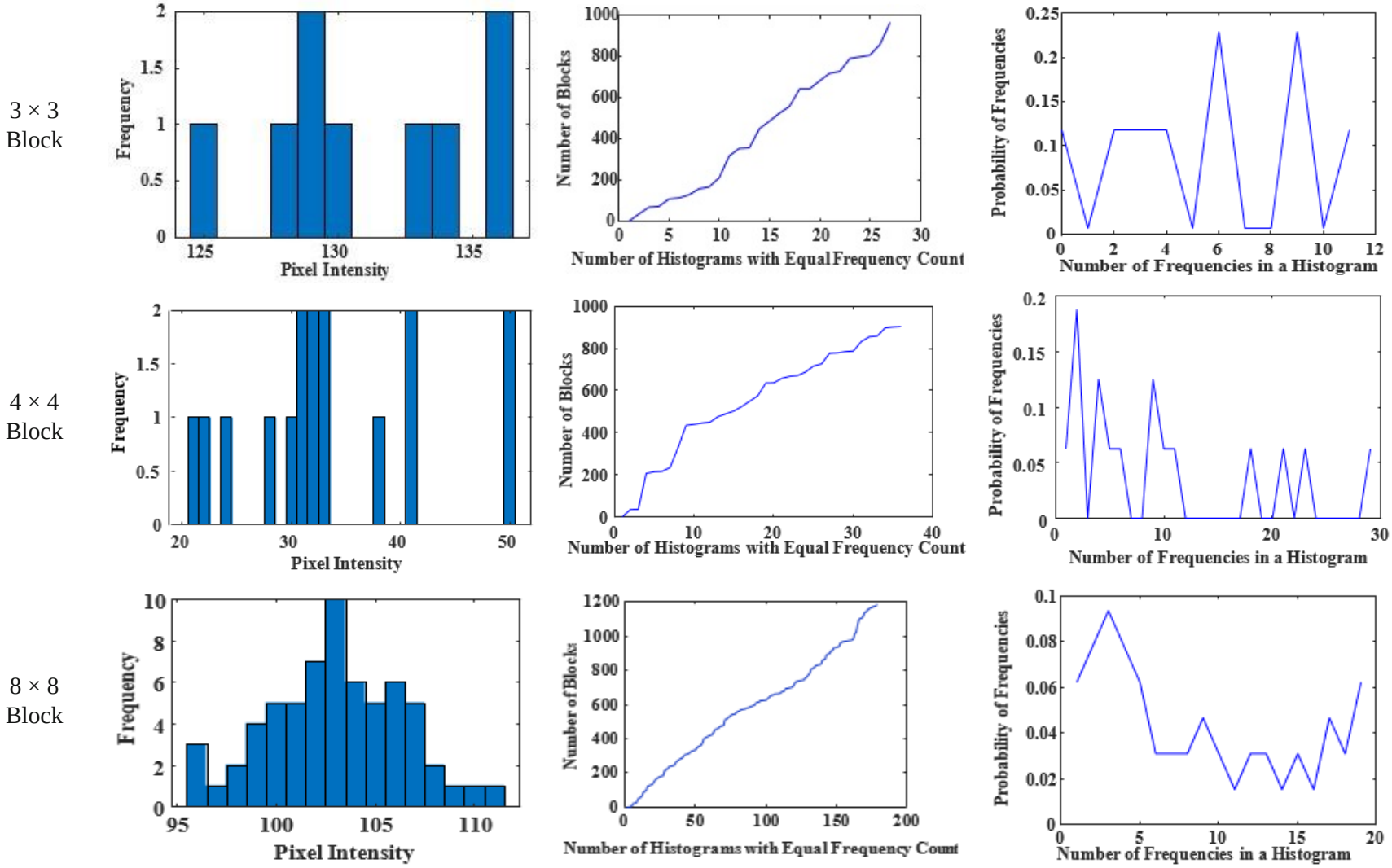


Figure 6.6: (a) HE of different sized blocks (b) Detection of histograms with equal number of frequencies (c) Probability of frequencies in histograms

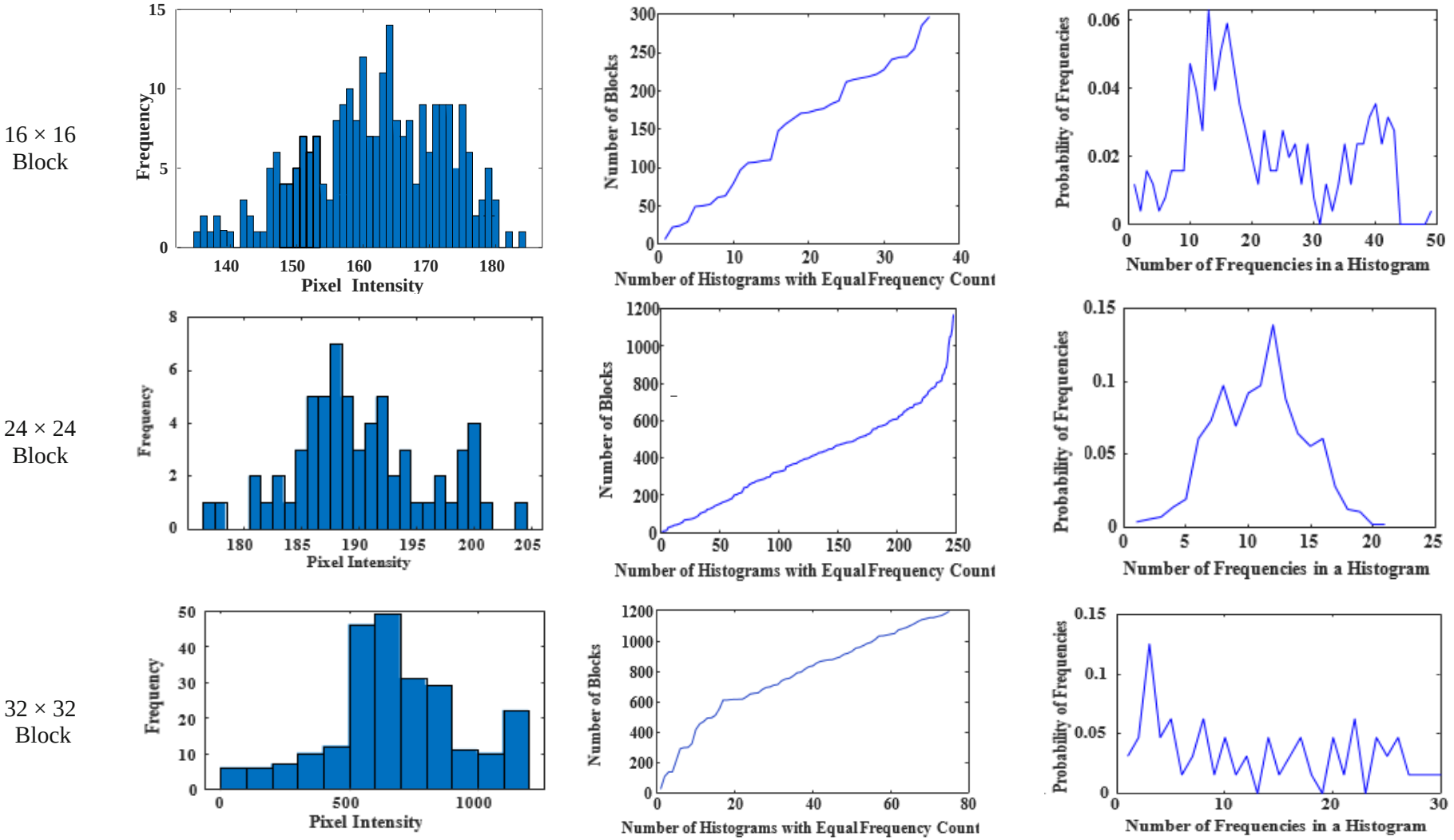


Figure 6.6: (a) HE of different sized blocks (b) Detection of histograms with equal number of frequencies (c) Probability of frequencies in Histograms

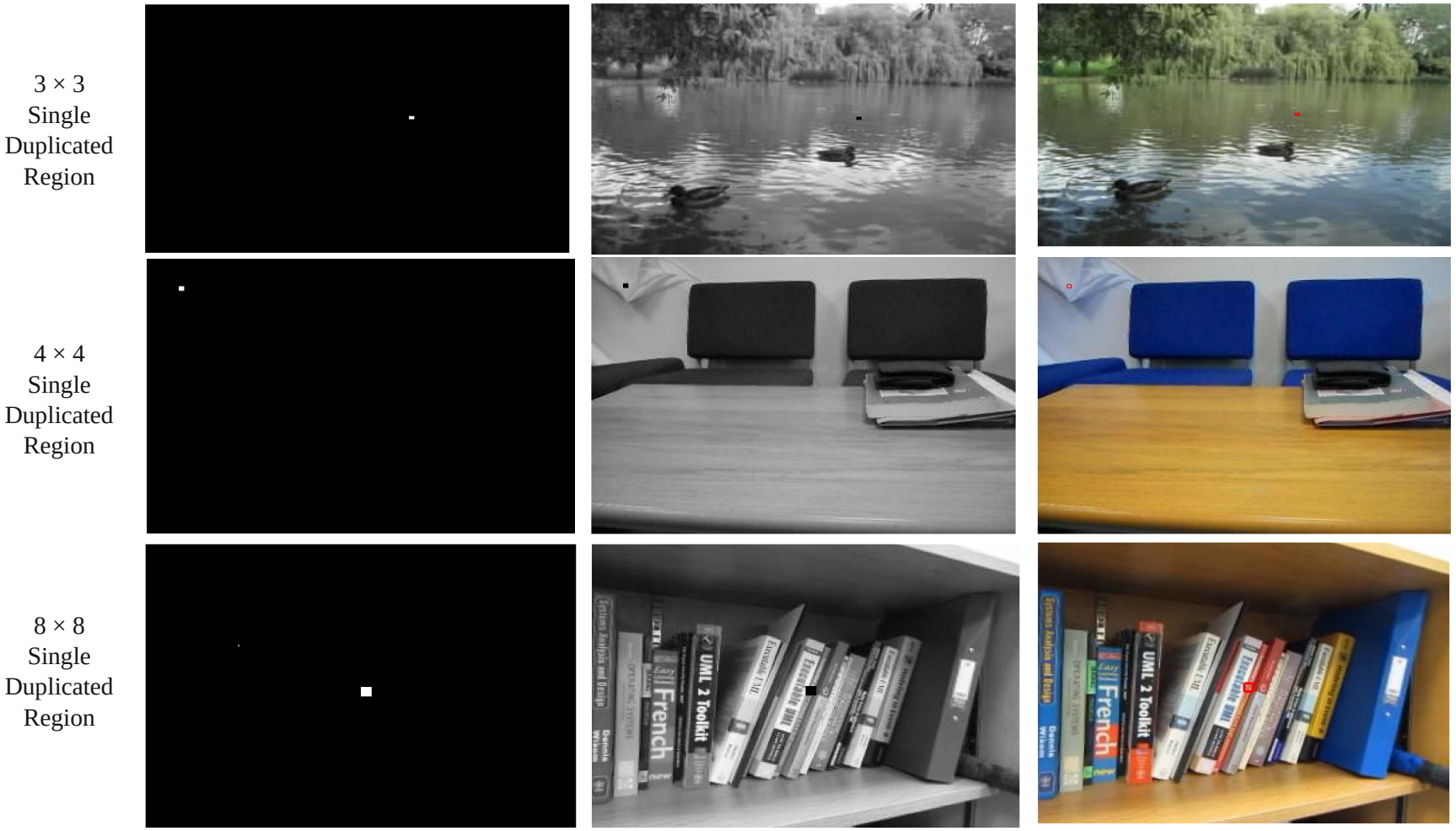


Figure 6.7: (a) Detection of single duplicated region with different region size (b) Localization of detected single duplicated region in grayscale frame (c) Tracking of detected single duplicated region in RGB frame of test digital videos

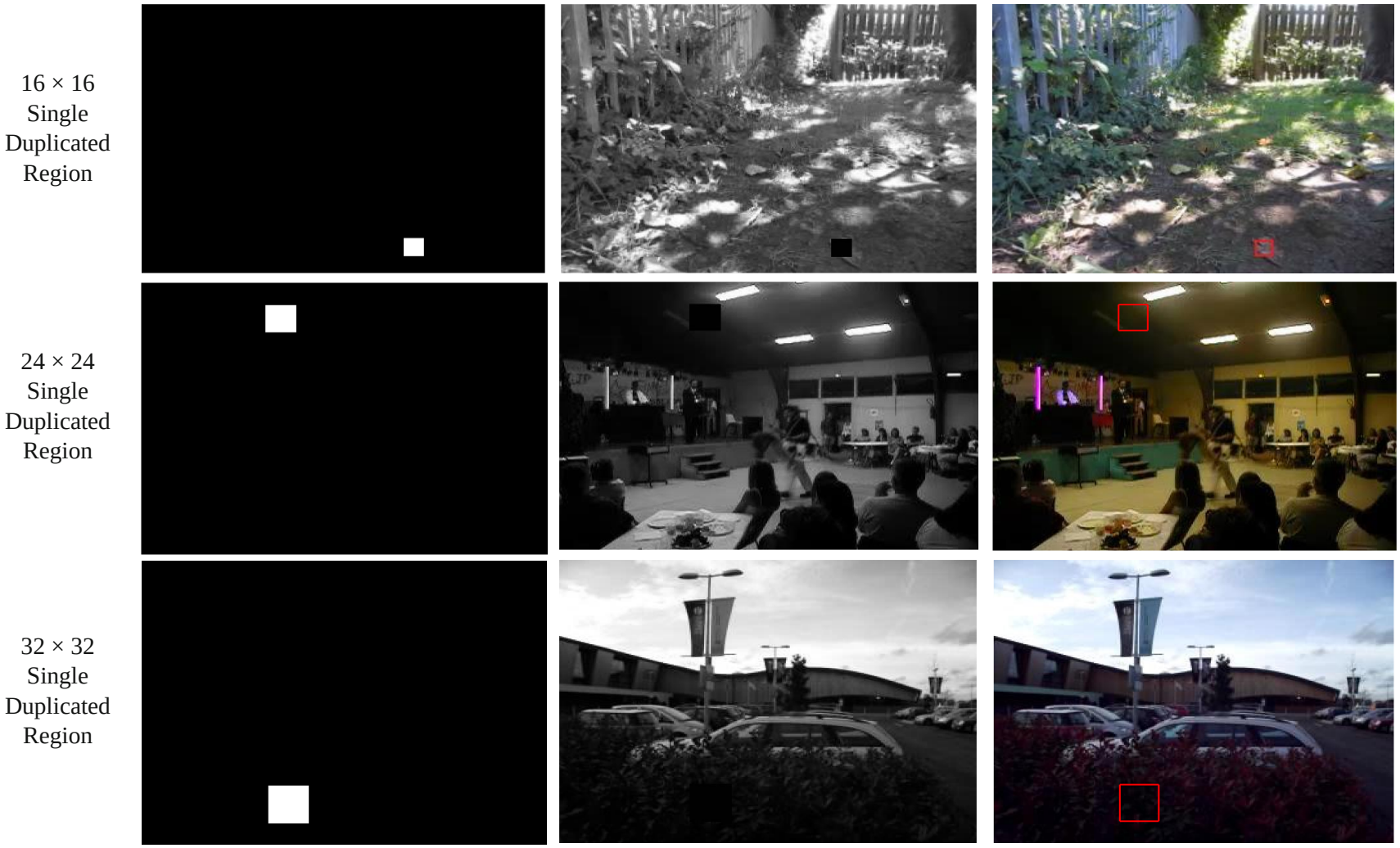


Figure 6.7: (a) Detection of single duplicated region with different region size (b) Localization of detected single duplicated region in grayscale frame (c) Tracking of detected single duplicated region in RGB frame of test digital videos

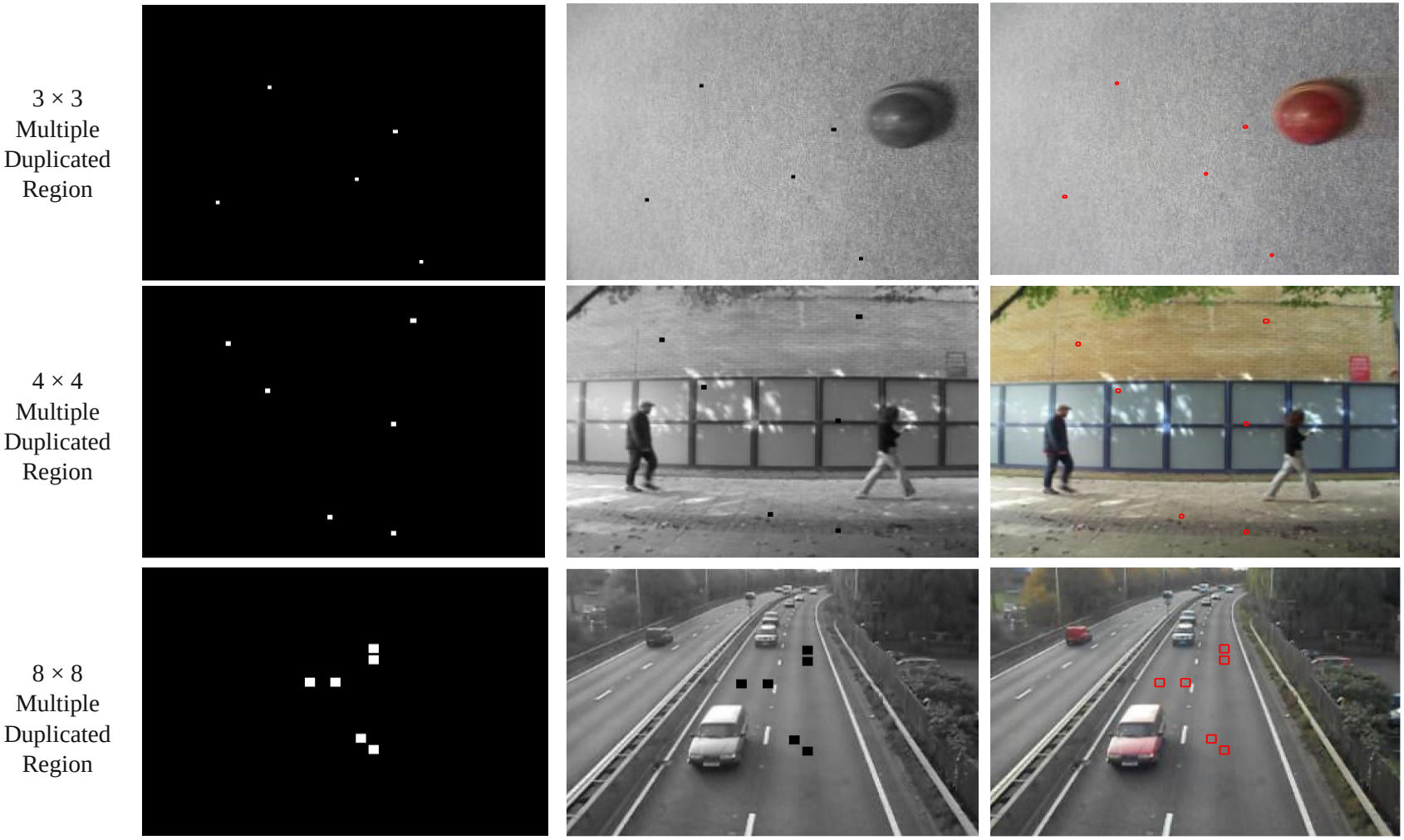


Figure 6.8: (a) Detection of multiple duplicated regions with different region size (b) Localization of detected multiple duplicated regions in grayscale frame (c) Tracking of detected multiple duplicated regions in RGB frame of test digital videos

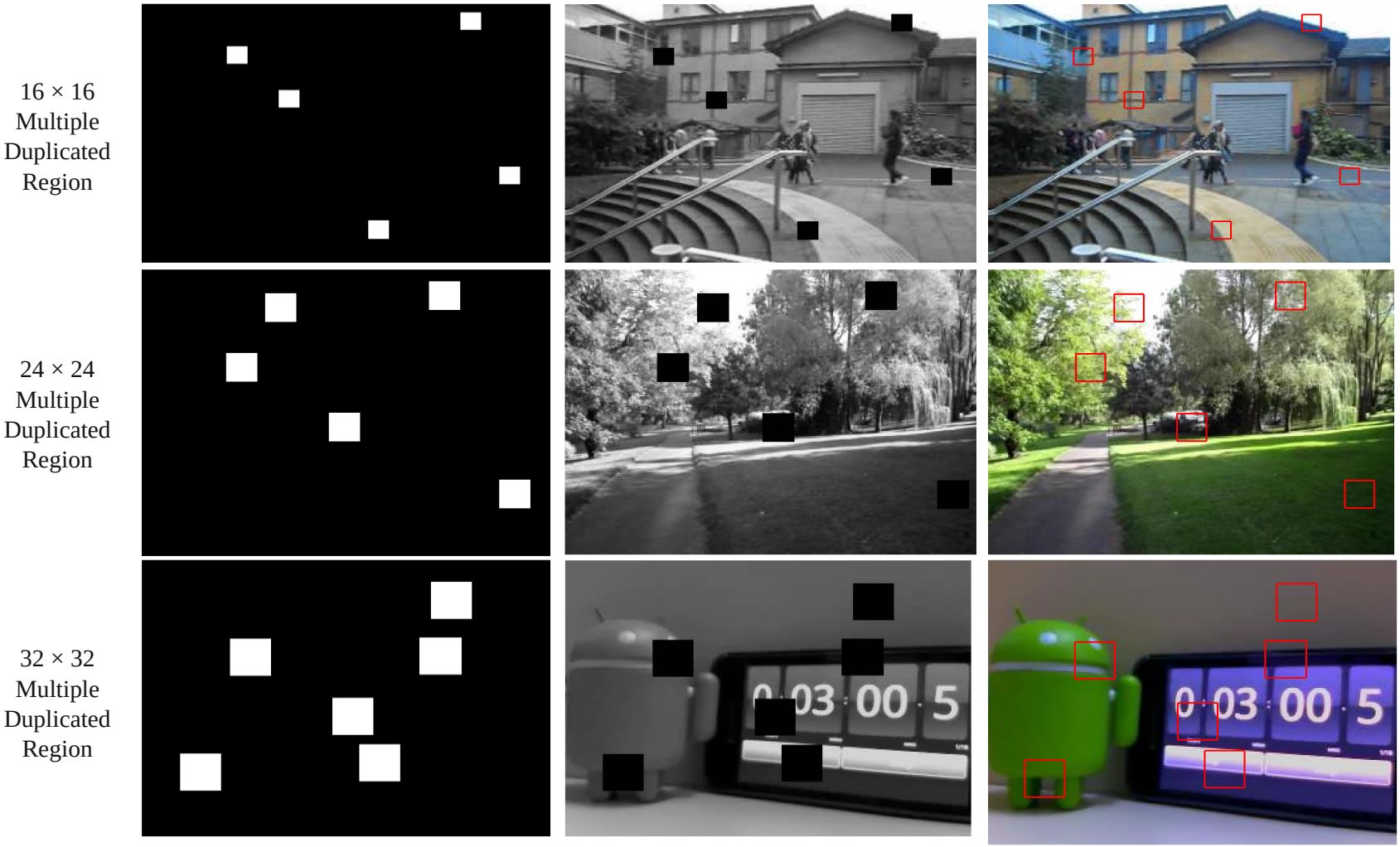


Figure 6.8: (a) Detection of multiple duplicated regions with different region size (b) Localization of detected multiple duplicated regions in grayscale frame (c) Tracking of detected multiple duplicated regions in RGB frame of digital videos

Figure 6.7 shows the detection results of single duplicated region within different region size in the test digital videos by the proposed approach. In first column (a) of Figure 6.7, the detection of single duplicated region within different region size such as 3 × 3, 4 × 4, 8 × 8, 16 × 16, 24 × 24, and 32 ×32 have been shown. The localization of detected single duplicated region in grayscale frames have been indicated in second column (b) of Figure 6.7. Also, the tracking of detected single duplicated region has been done in RGB frames of the digital videos which has demonstrated in third column (c) of Figure 6.7. Similarly, Figure 6.8 shows the detection results of multiple duplicated regions within different region size in the digital videos by multiple CMRD forgery detection approach. Figure 6.8 (a) shows the detection of multiple duplicated regions within different region size such as 3 × 3, 4 × 4, 8 × 8, 16 × 16, 24 × 24, and 32 × 32. The localization of detected multiple duplicated regions in grayscale frames has been demonstrated in Figure 6.8 (b). Figure 6.8 (c) indicates the tracking of detected multiple duplicated regions in RGB frames of the digital videos.

6.2.2.2 Quantitative Performance Analysis

After the simulation results, the multiple CMRD forgery detection approach is also measured quantitatively by taking into consideration various performance metrics. The proposed approach is subjected to evaluation on the basis of performance parameters in the digital videos such as PR, RR, DA, F1 score, F2 score, FPR, FNR, sensitivity, specificity and execution time [59], [77], [104], [108], [115], [121], and [123]. The generated dataset has been classified for the detection of multiple CMRD forgery in the digital videos which is based on the probability comparing and block filtering of identified forged blocks. For detecting single and multiple CMRD forgeries, each digital video has been identified by comparing the probability of frequencies in a histogram with other histograms and using block filtering of identified forged blocks. The outcomes are labelled as authentic digital video and forged digital video. The ROC curve has been shown in Figure 6.9

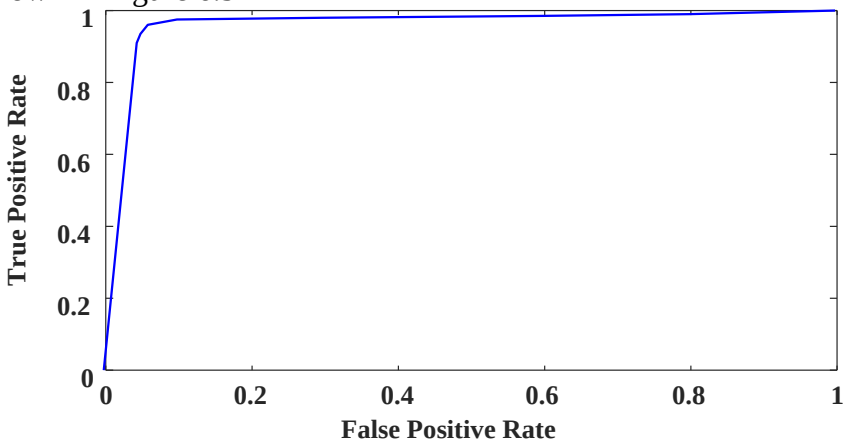


Figure 6.9: ROC curve for testing set of multiple CMRD forgery detection approach

The performance evaluation of multiple CMRD forgery detection approach for testing set of digital videos has been shown in Table 6.2 whereas, Table 6.3 provides the parameters evaluation of proposed approach. Table 6.4 indicates the DA of the proposed approach separately for detecting single and multiple CMRD forgeries within different region sizes in the digital videos.

Table 6.2: Performance evaluation of multiple CMRD forgery detection approach for testing set of digital videos

	Positive	**Negative**
True	0.982	0.990
False	0.018	0.010

Table 6.3: Different parameters evaluation of multiple CMRD forgery detection approach

PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Selectivity**
0.982	0.989	0.986	0.985	0.988	0.015	0.009	0.989	0.908

Table 6.4: DA of the proposed approach for detecting single and multiple CMRD forgery with different region size in the digital videos

Different region size in CMRD Forgery	**DA for single CMRD forgery**	**DA for multiple CMRD forgery**
3 × 3	0.973	0.956
4 × 4	0.977	0.964
8 × 8	0.986	0.970
16 × 16	0.994	0.978
24 × 24	0.995	0.983
32 × 32	0.997	0.988

Table 6.2 indicates the higher value of true negatives which shows that multiple CMRD forgery detection approach is more effective for detecting the forged digital videos having multiple CMRD forgeries. The values of different parameters such as PR, RR, DA, F1, F2, FPR, FNR, Sensitivity and Specificity of multiple CMRD forgery detection approach has been shown in Table 6.3 which provides the detection accuracy of 98.6% at a false negative rate of 0.9 %.

Table 6.4 shows that DA is decreased by reducing the size of duplicated region. When the proposed approach works on the small blocks then, sometimes, these blocks have equal pixel values. Due to this, these blocks are detected as forged blocks by the proposed approach. Therefore, FP occurred and PR decreases.

6.3 Comparative Analysis

The proposed approach has been compared with existing techniques in terms of PR, RR, DA, F1, F2, FPR, FNR, sensitivity and specificity as shown in Table 6.5. The existing techniques are represented such as Ojeniyi *et al.* [67], Bilal *et al.* [8], Hashmi *et al.* [34], Manu *et al.* [64], Nawaz et al. [66], and Singh *et al.* [101] in Table 6.5.

Table 6.5: Comparison between multiple CMRD forgery detection approach and existing techniques

	PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Specificity**
Hashmi et al. [34]	0.888	0.800	0.850	0.838	0.814	-	-	-	-
Manu et al. [64]	0.994	0.916	0.915	0.953	0.930	-	-	-	-
Ojeniyi et al. [67]	0.938	0.972	0.954	0.955	0.965	-	-	-	-
Singh et al. [101]	**1.000**	0.933	0.966	0.965	0.945	**0.00**	0.06	0.937	**1.000**
Bilal et al. [45]	0.964	0.810	-	0.880	0.836	1.74	6.03	0.810	0.964
Nawaz et al. [66]	0.972	0.961	-	0.934	0.952	-	-	-	-
Proposed	0.982	**0.989**	**0.986**	**0.985**	**0.988**	0.015	**0.009**	**0.989**	0.908

- means data has not been calculated in the existing techniques and bold indicates higher values of parameters.

It indicates higher RR of multiple CMRD forgery detection approach than existing techniques. The high value of DA of proposed approach shows its better performance for detecting the multiple CMRD forgeries than existing techniques. Table 6.5 shows the effectiveness of proposed approach with its higher values of F1 and F2 scores. The minimum FNR and higher sensitivity show better results than existing techniques. Thus, it indicates that the performance of the multiple CMRD forgery detection approach is more effective than existing techniques.

6.4 Computational Cost

The execution time of proposed approach is provided in Table 6.6 whereas, comparative analysis between execution time of proposed approach and existing techniques is given in Table 6.7.

Table 6.6: Execution Time of the multiple CMRD forgery detection approach

Video Resolution	Video Type	Execution Time (sec/frame)
1280 × 720	Forged	0.63
1024×768	Forged	0.49
640 × 480	Forged	0.41
320 × 240	Forged	0.29
720 × 576	Forged	0.43
240×160	Forged	0.25
384 × 288	Forged	0.37

Table 6.7: Comparison between the execution time of the proposed approach and existing techniques

Video Resolution	Video Type	Execution Time (sec/frame)	
		Singh *et al.*[101]	**Proposed**
1280 × 720	Forged	1.50	**0.63**
1024×768	Forged	0.70	**0.49**
640 × 480	Forged	0.62	**0.41**
320 × 240	Forged	0.46	**0.29**
720 × 576	Forged	0.65	**0.43**
240×160	Forged	0.46	**0.25**
384 × 288	Forged	0.599	**0.37**

Bold indicates higher values of parameters.

Table 6.6 shows the execution time of proposed approach on different resolutions such as 1280 × 720, 1024×768, 640 × 480, 320 × 240, 720 × 576, 240×160 and 384 × 288 for the detection of multiple CMRD forgeries. On other side, Table 6.7 indicates comparison between the execution time of proposed approach and existing techniques on different resolutions. It shows

minimum execution time than that of existing techniques because the proposed approach works on those blocks whose histograms have equal number of frequencies. It reduces more execution time of proposed approach. Therefore, the multiple CMRD forgery detection approach provides better efficiency than the existing techniques.

6.5 Summary

In this chapter, multiple CMRD forgery detection approach based on HE has detected single and multiple CMRD forgeries with different region sizes in the digital videos. This approach has also localized and tracked the single and multiple CMRD forgeries in the digital videos. The proposed approach has performed on the digital videos taken from SULFA dataset and the internet. It provides effective results on the detection of single and multiple CMRD forgeries having different region sizes in the digital videos. The proposed approach has also provided minimum execution time in the digital videos with different resolutions. Therefore, the performance of multiple CMRD forgery detection approach is better than the existing techniques. In the next chapter, the further work has been focused on the CKF forgery detection in the digital videos.

CHAPTER 7

CKF FORGERY DETECTION UNDER VARIOUS ATTACKS

This chapter is primarily dedicated to detect the CKF forgery in the digital videos. CKF forgery detection approach is proposed which is based on FEI for detecting this forgery. CKF forgery is presented in two different circumstances (settings) in the digital videos such as (i) all frames are forged with CKF forgery in the digital video and (ii) some of frames are forged with CKF forgery and some are authentic in the digital video. The performance of proposed approach is examined on the digital videos with different cases and circumstances which are taken from SULFA dataset. Then the proposed approach is evaluated on the digital videos under the various attacks for confirming its robustness. The proposed approach also performed efficiently on digital videos from the internet. The experimental results show the higher DA with less execution time and robustness of the proposed approach than those of existing techniques.

7.1 CKF Forgery Detection Based on FEI Approach

The existing techniques have certain drawbacks of lower detection and are not also immune to attacks. In this section, CKF forgery detection based on FEI approach has been introduced for detecting the CKF forgery in the digital videos. The flow diagram of proposed approach is shown in Figure 7.1 which extracts the number of frames f_T from an input digital video. After frame extraction, the number of frame pairs are made with two consecutive frames f_N and f_{N+1} such as f_1 and f_2, f_2 and f_3, f_3 and f_4 and so on. Frame f_N of each frame pair is subtracted from its next frame f_{N+1} such as f_{N+1}-f_N = f_P for creating a RGB difference frame f_P, and then frame f_{N+1} is subtracted from its previous frame f_N for generating another RGB difference frame f_Q as f_N -f_{N+1} = f_Q. These RGB difference frames provide the difference values between pixels of frames f_N and f_{N+1}. It is observed that in the circumstance (i), all pixel difference values are achieved in RGB difference frame by subtracting the consecutive frames of each frame pair such as f_{N+1}-f_N as shown in Figure 7.2 (a). However, in the circumstance (ii), all pixel difference values could not be obtained in the RGB difference frame by one side subtraction. Therefore, some of pixel difference values are attained by subtracting the consecutive frames like f_{N+1} - f_N as shown in Figure 7.2 (b) and remaining pixel difference values are achieved by subtracting the consecutive frames in opposite direction such as f_N - f_{N+1} shown in Figure 7.2 (c) for each frame pair of a digital video.

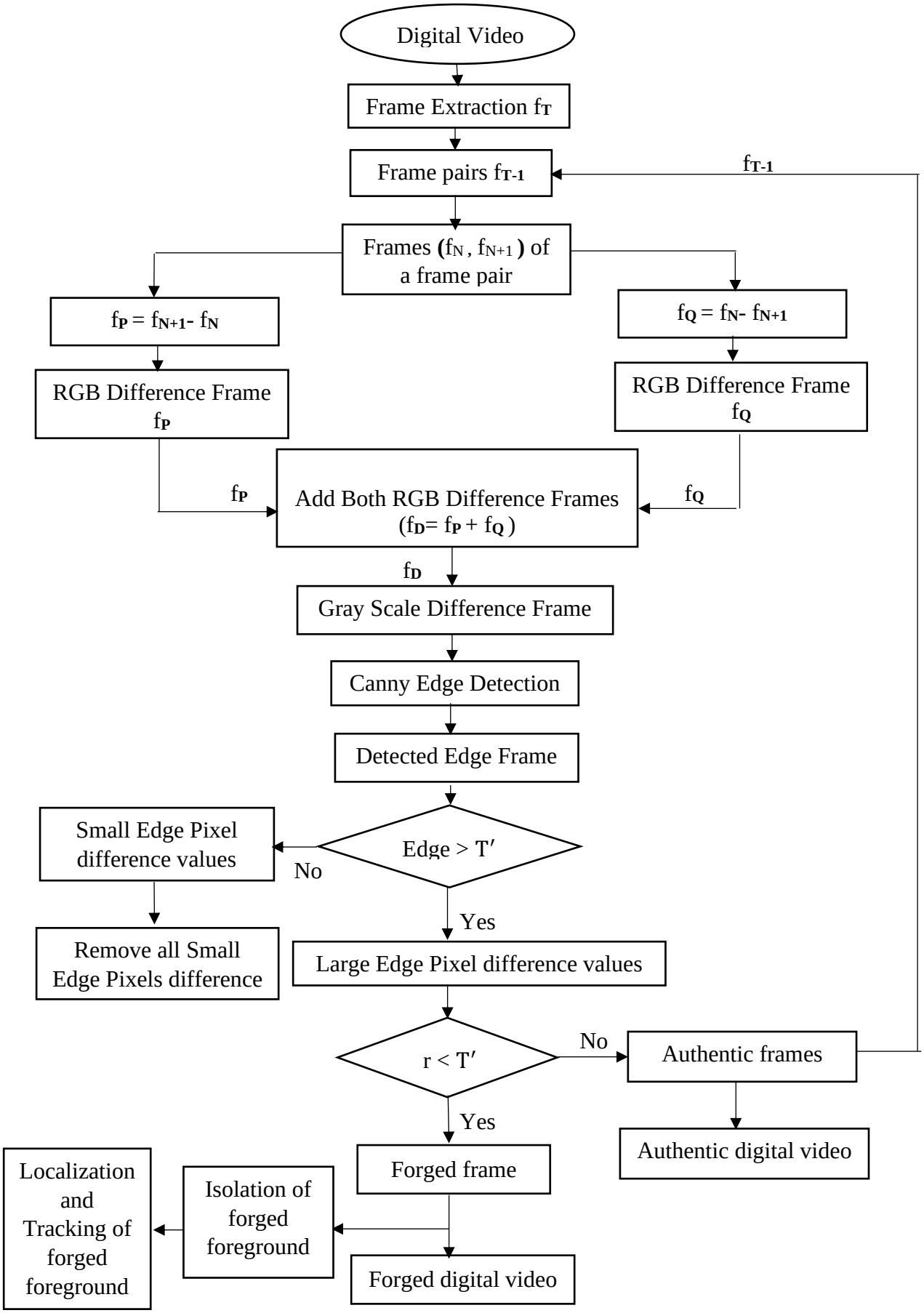


Figure 7.1: Flow diagram of CKF forgery detection based on FEI approach

Figure 7.2 (d) and 7.2 (e) are showing clearly that some of pixel difference values are not achieved in the edge frame of RGB difference frames for circumstance (ii). Therefore, for appearing all pixel difference values in these different circumstances (i) and (ii), two RGB difference frames are created for each frame pair of a digital video in the proposed approach.

f_N

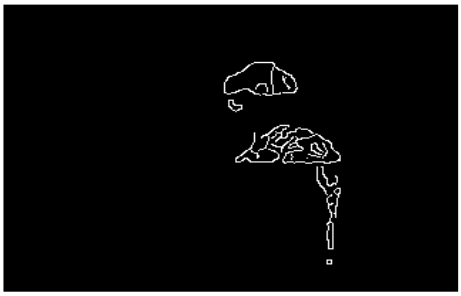
f_{N+1}

(a)

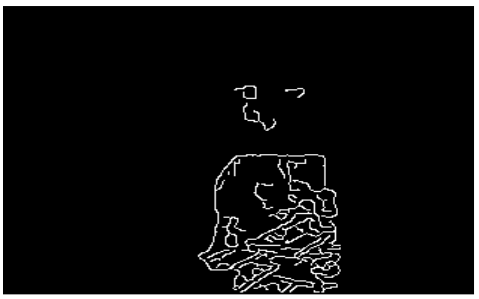
(b)

(c)

(d)



(e)



(f)

Figure 7.2: (a) Frames **(**f_N , f_{N+1} **)** of a frame pair, (b) Difference frame (f_{N+1} - f_N = f_P) of one frame pair for circumstance (i), (c) Difference frame (f_{N+1} - f_N = f_P) of one frame pair at one side for circumstance (ii), (d) Difference frame (f_N - f_{N+1} = f_Q) at other side for circumstance (ii), (e) Edge frame of difference frame in (b), (f) Edge frame of difference frame in (c)

Both RGB difference frames f_P and f_Q are added for making a combined RGB difference frame f_D such as $f_P + f_Q = f_D$ for each frame pair of the digital video as shown in Figure 7.3 (a). Then this combined RGB difference frame is converted into a grayscale difference frame as shown in Figure 7.3 (b).

(a) (b)

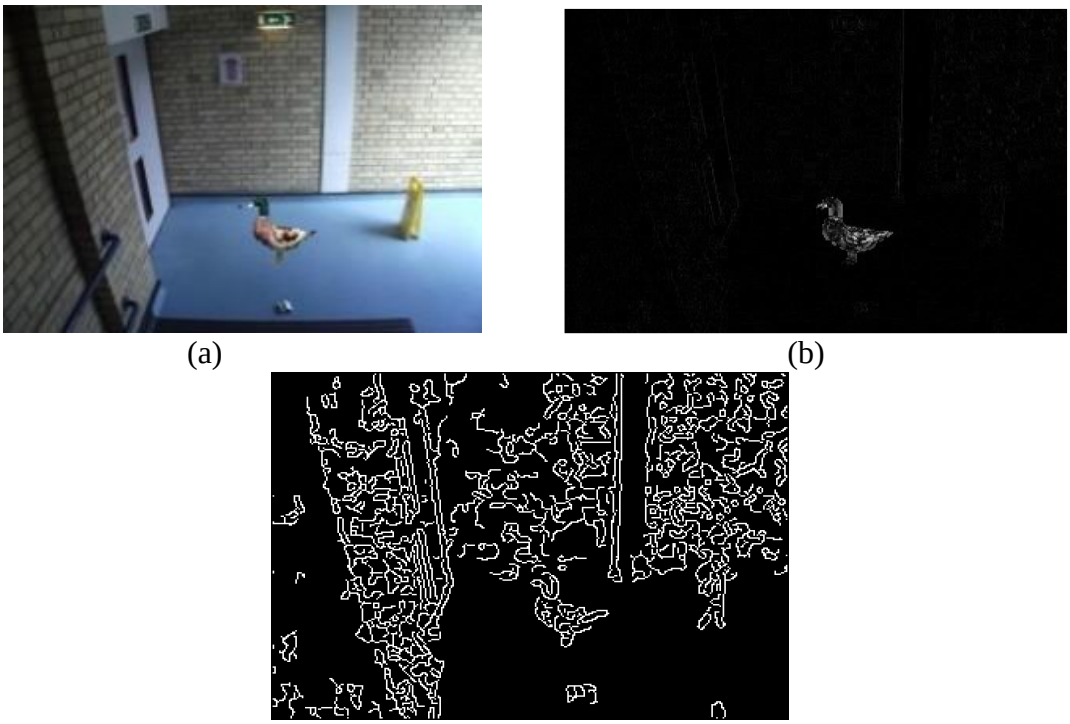
Figure 7.3: (a) Combined RGB difference frame (b) Grayscale difference frame

Now, canny edge detector is applied on grayscale difference frame of each frame pair. It detects edges of grayscale difference frame of each frame pair of the digital video as shown in Figure 7.4 in which some edges are more sharp due to large pixel difference values and some are smooth with small pixel difference values. These edges are useful footprints [23] for identifying the changes in illumination or color within each frame of the digital video.

Figure 7.4: Edge frame of grayscale difference frame

The canny edge detector detects the edges of each grayscale difference frame where the pixel intensity values are abruptly changed in a digital video. It has also been observed that the large edge pixel difference values are produced between the pixel intensities of forged foreground in CKF forgery and authentic background in each edge frame of a digital video. Therefore, the whole edge area of forged foreground becomes sharp in each edge frame. On the other side, the edges of authentic foreground and background become smooth in the edge frame due to small edge pixel difference values between their pixel intensities. Figure 7.5 shows the difference between authentic and forged foregrounds in which Figure 7.5 (a) indicates the frame with CKF forgery and original foreground whereas, its grayscale difference is shown in Figure 7.5 (b). Figure 7.5 (c) indicates that the edges of authentic foreground and background

are coincide with each other due to smooth edge in the edge frame whereas, in the case of CKF forgery, the edges of forged foreground do not coincide with the edges of authentic foreground and background due to sharpness of edges in the edge frame. Therefore, the forged foreground in CKF forgery appears as a different part within the edge frame.



(a) (b)

(c)

Figure 7.5: (a) Frame with CKF forgery and original foreground (b) Grayscale difference frame (c) Edge frame of difference frame

CKF forgery detection based on FEI approach is used OTSU algorithm [79] for setting the threshold value T' for each edge frame of the digital video. Each edge pixel difference value is compared with threshold value T' to differentiate them into large and small edge pixel difference values. The edge pixel difference values which are greater than T' are large edge pixel difference values in the edge frame whereas, the edge pixel difference values which are less than T' are small edge pixel difference values in the edge frame.

When the edge pixel difference values are differentiated into large and small edge pixel difference values in the edge frame, then the rate of large edge pixel difference values are calculated using Eq. (7.1) [89] for each edge frame of the digital video.

$$r(n) = \frac{\sum Q_n}{N_n} \tag{7.1}$$

where, $r(n)$ is the rate of large edge pixel difference values of n^{th} edge frame. $\sum Q_n$ is the sum of large edge pixel difference values of n^{th} edge frame and N_n is the total number of edge pixel difference values of n^{th} edge frame. If the rate of large edge pixel difference values is less than

T′ in the edge frame then the frame is identified as forged frame and input digital video is forged digital video. Due to large edge pixel difference values, a large threshold value is set by OTSU algorithm in the edge frame. Therefore, the proposed approach eliminates a large number of edge pixel difference values less than threshold value T′, and keeps the left behind less amount of edge pixel difference values of forged foreground which are large than T′. Thus, this less amount of edge pixel difference values decrease the rate of large edge pixel difference values which identifies the forged frame.

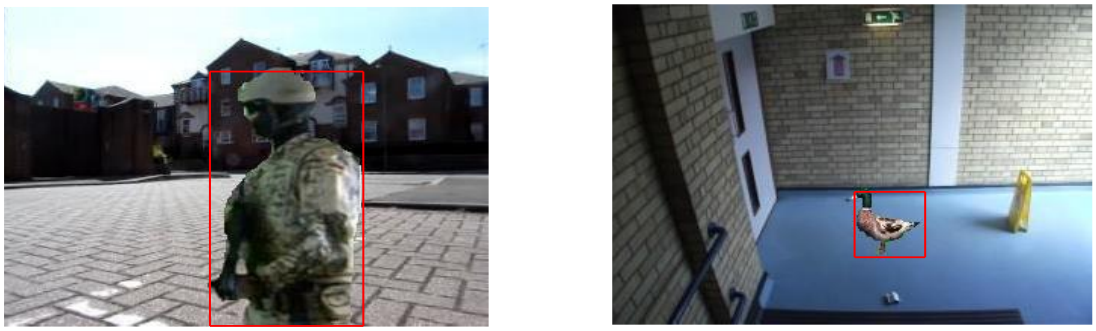
On the other hand, if the rate of large edge pixel difference values is grater than T′ in the edge frame, then the frame is an authentic frame. Now, the above complete process is repeated for each frame pair up to f_T-1 times. If edge frame of each frame pair is authentic then it is an authentic digital video. Due to small edge pixel difference values, a small threshold value is set by the OTSU algorithm in the edge frame. Therefore, the proposed approach eliminates very less number of small edge pixel difference values and keeps the left behind a large number of edge pixel difference values which increases the rate of large edge pixel difference values.

Now, the edges of forged foreground are isolated in the identified forged frame by removing its small edge pixel difference values. This isolated forged foreground is CKF forgery in the edge frame of the digital video as shown in Figure 7.6 (a) and Figure 7.6 (b). Thus, the proposed approach does not only detect the CKF forgery but it also isolates the forged foreground within each edge frame of a forged digital video.

(a) (b)

Figure 7.6: (a) and (b) detected and isolated CKF forgery in the digital videos

After isolating CKF forgery, the proposed approach discovers the edge positions of isolated CKF forgery in the edge frame and also tracks it in the forged frame of the digital video as shown in Figure 7.7 (a) and Figure 7.7 (b).



(a) (b)

Figure 7.7: (a) and (b) tracking of CKF forgery within the frame

7.2 Performance Analysis of CKF Forgery Detection Based on FEI Approach

The proficiency of proposed CKF forgery detection based on FEI approach is confirmed both qualitatively and quantitatively by taking digital videos from SULFA dataset in this section. This approach is evaluated on the digital videos taken from the internet. Some of SULFA dataset digital videos and the internet downloaded digital videos are detailed in Table 7.1 and Table 7.2 respectively. The proposed approach is also examined under various attacks to demonstrate its robustness. Moreover, the proposed approach is compared against the existing techniques of CKF forgery detection.

7.2.1 Dataset and Setting

For evaluating the proposed approach for the detection of CKF forgery in the digital videos, a dataset has been generated with the number of 202 digital videos. Out of 202 digital videos, there are 102 digital videos which are taken from the SULFA dataset [96] and remaining 100 digital videos are downloaded from the internet [39]. Out of 102 SULFA dataset digital videos, 51 digital videos are selected for training purpose and 51 digital videos are selected for the testing purpose. In testing digital videos, 25 digital videos are authentic and 26 digital videos are forged. These selected digital videos for the training and testing sets are non-overlapping. On other side, out of the remaining 100 digital videos from internet, 50 videos are selected for training purposes and 50 videos are selected for testing purposes.

Two kinds of digital videos are made in generated dataset as (1) authentic digital video and (2) forged digital video. In the set of authentic digital videos, there are authentic digital videos with different cases. On other hand, in the set of forged digital videos with CKF forgery, the digital videos are divided into two categories: (a) Forged digital videos with different cases and different circumstances (b) Forged digital videos under various attacks.

Table 7.1: Detail of some digital videos taken from SULFA dataset (Sample of 30 videos out of 102 and S_Video means SULFA dataset video)

Video Name	Resolution	Video Format	Different cases	Video Type	Camera Model
S_Video_01	320×240	.avi	MC	Forged	Nikon S3000
S_Video_02	320×240	.avi	MC	Forged	Nikon S3000
S_Video_03	320×240	.avi	MC	Forged	Nikon S3000
S_Video_04	720 × 480	.mov	MC	Forged	Nikon S3000
S_Video_05	720 × 480	.avi	MC	Forged	Nikon S3000
S_Video_06	320×240	.avi	MC	Forged	Nikon S3000
S_Video_07	320×240	.avi	SvC	Forged	Nikon S3000
S_Video_08	320×240	.mov	SvC	Authentic	Nikon S3000
S_Video_09	320×240	.mov	SvC	Forged	Nikon S3000
S_Video_10	320×240	.avi	SvC	Forged	Nikon S3000
S_Video_11	720 × 480	.avi	SvC	Forged	Canon SX200
S_Video_12	720 × 480	.avi	SvC	Forged	Canon SX200
S_Video_13	320×240	.avi	SC	Forged	Canon SX200
S_Video_14	320×240	.avi	SC	Forged	Canon SX200
S_Video_15	720 × 480	.mov	SC	Forged	Canon SX200
S_Video_16	320×240	.avi	SC	Forged	Canon SX200
S_Video_17	320×240	.avi	SC	Authentic	Canon SX200
S_Video_18	720 × 480	.avi	SC	Forged	Canon SX200
S_Video_19	320×240	.avi	CZIOF	Forged	Canon SX200
S_Video_20	320×240	.mov	CZIOF	Forged	Canon SX200
S_Video_21	720 × 480	.avi	CZIOF	Forged	Fujifilm 2800
S_Video_22	320×240	.avi	CZIOF	Forged	Fujifilm 2800
S_Video_23	320×240	.avi	CZIOF	Forged	Fujifilm 2800
S_Video_24	320×240	.avi	CZIOF	Forged	Fujifilm 2800
S_Video_25	320×240	.mov	EC	Forged	Fujifilm 2800
S_Video_26	320×240	.mov	EC	Forged	Fujifilm 2800
S_Video_27	320×240	.mov	EC	Forged	Fujifilm 2800
S_Video_28	720 × 480	.avi	EC	Forged	Fujifilm 2800
S_Video_29	320×240	. avi	EC	Authentic	Fujifilm 2800
S_Video_30	320×240	. avi	EC	Forged	Fujifilm 2800

Table 7.2: Detail of some of digital videos downloaded from the internet (sample of 22 videos out of 100 and Idv_Video means Internet downloaded digital video)

Video Name	Resolution	Video Format	Video Type
Idv_Video_01	638×360	.mp4	Forged
Idv_Video_02	480×360	.mov	Forged
Idv_Video_03	640×360	.mp4	Forged
Idv_Video_04	480×352	.mp4	Forged
Idv_Video_05	640×360	.avi	Forged
Idv_Video_06	640×360	.mov	Authentic
Idv_Video_07	720×576	.mp4	Forged
Idv_Video_08	490×360	.mp4	Forged
Idv_Video_09	640×352	.mp4	Forged
Idv_Video_10	640×360	.mp4	Authentic
Idv_Video_11	638×360	.avi	Forged
Idv_Video_12	638×360	.mov	Forged
Idv_Video_13	480×360	.mp4	Forged
Idv_Video_14	480×352	.avi	Forged
Idv_Video_15	720×576	.mov	Forged
Idv_Video_16	480×360	.avi	Forged
Idv_Video_17	720×576	.avi	Forged
Idv_Video_18	480×352	.mov	Forged
Idv_Video_19	490×360	.avi	Forged
Idv_Video_20	640×352	.mov	Forged
Idv_Video_21	490×360	.mov	Forged
Idv_Video_22	640×352	.avi	Forged

7.2.2 Simulation Results for Test Digital Videos of Dataset

Both qualitative and quantitative analysis is conducted on the test digital videos from the dataset for confirming the capability of the presented CKF forgery detection based on FEI approach.

7.2.2.1 Qualitative Performance Analysis

The proposed approach detects the CKF forgery of large and small size in digital videos having different case and circumstances as shown in Figure 7.8. The frames of digital videos are shown in Figure 7.8 (a) whereas, Figure 7.8 (b) shows grayscale difference frames. The edge frames of these grayscale difference frames are shown in Figure 7.8 (c). Figure 7.8 (d) shows the detection and isolation of the CKF forgery by the proposed approach. The tracking of CKF forgery in the frames of forged digital video is shown in Figure 7.8 (e).

In Case I, the proposed approach has performed effectively on the static camera videos in which the variation in the pixel intensity values of consecutive frames is very low in the digital video as shown in 1st row of Figure 7.8. In Case II, the proposed approach has also worked on the moving camera digital videos in which the pixel intensity values of each frame are varied with the camera position and its moving speed as shown in 2nd row of Figure 7.8. The proposed approach has also been tested on the surveillance videos in Case III. In this case, the pixel intensity values are varied due to noise and temperature where the camera is placed in ATM machine, inside the room, in the open area etc. The detection of CKF forgery for this case is shown in the 3rd row of Figure 7.8.

In Case IV, the proposed approach has been evaluated on those digital videos in which the pixel intensity values of some frames are varied abruptly according to camera zoom-in function at different times and some are varied according to camera zoom-out function at other times. The detection of CKF forgery of this case is shown in the 4th row of Figure 7.8. The proposed approach has performed effectively on the digital videos in which pixel values are varied with the movement of shadow of leaves of a tree in Case V. The detection of CKF forgery in this case is shown in the 5th row of Figure 7.8. The detection of CKF forgery of Case VI, in which pixel intensity values are varied with environmental conditions is shown in the 6th row of Figure 7.8. The detection of authentic digital video by the proposed approach has also been shown in the 7th row of Figure 7.8.

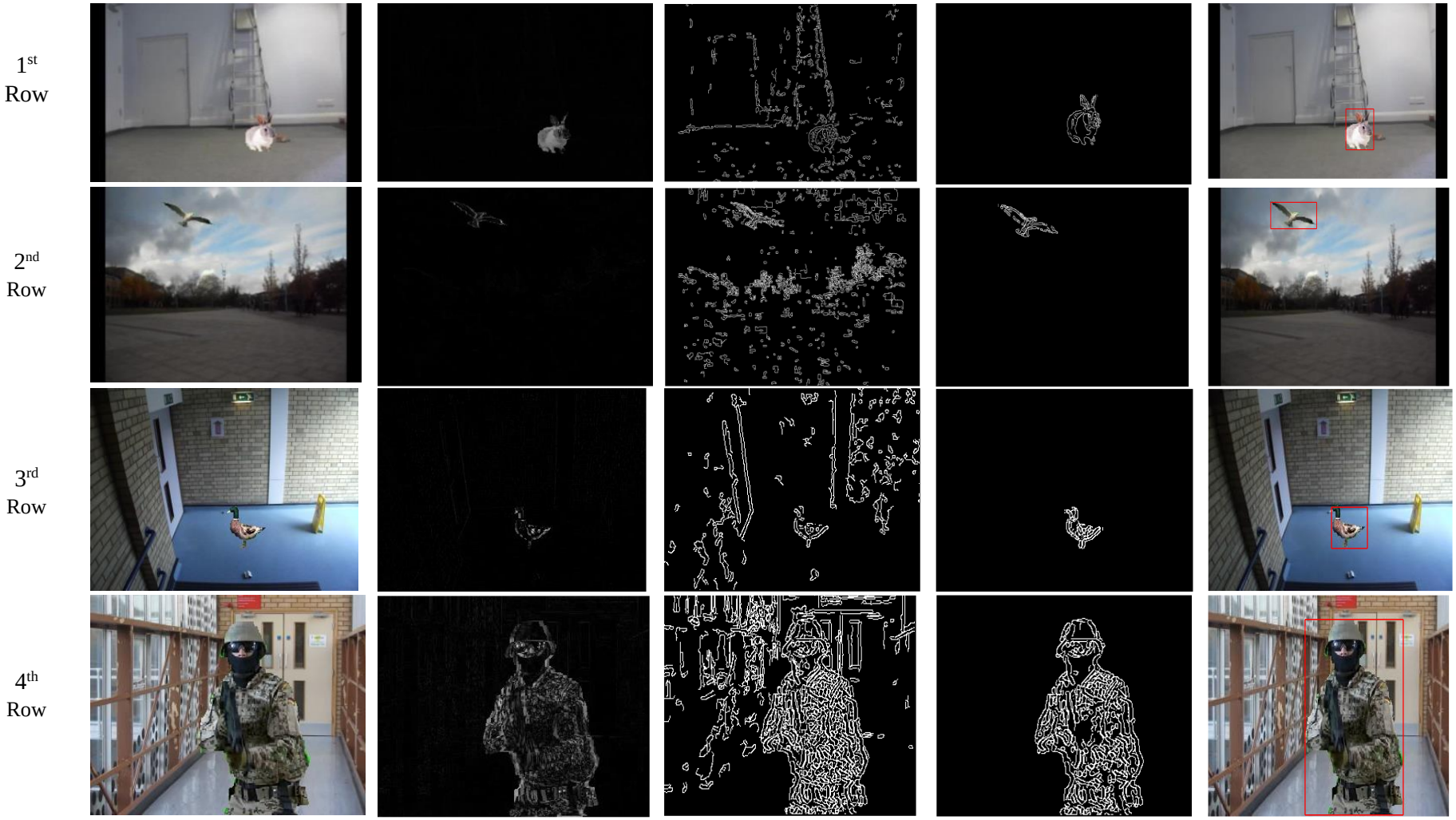


Figure 7.8: (a) Frame with CKF forgery (b) Grayscale difference frame (c) Edge frame of grayscale difference frame (d) Detection and isolation of CKF forgery (e) Tracking of CKF forgery

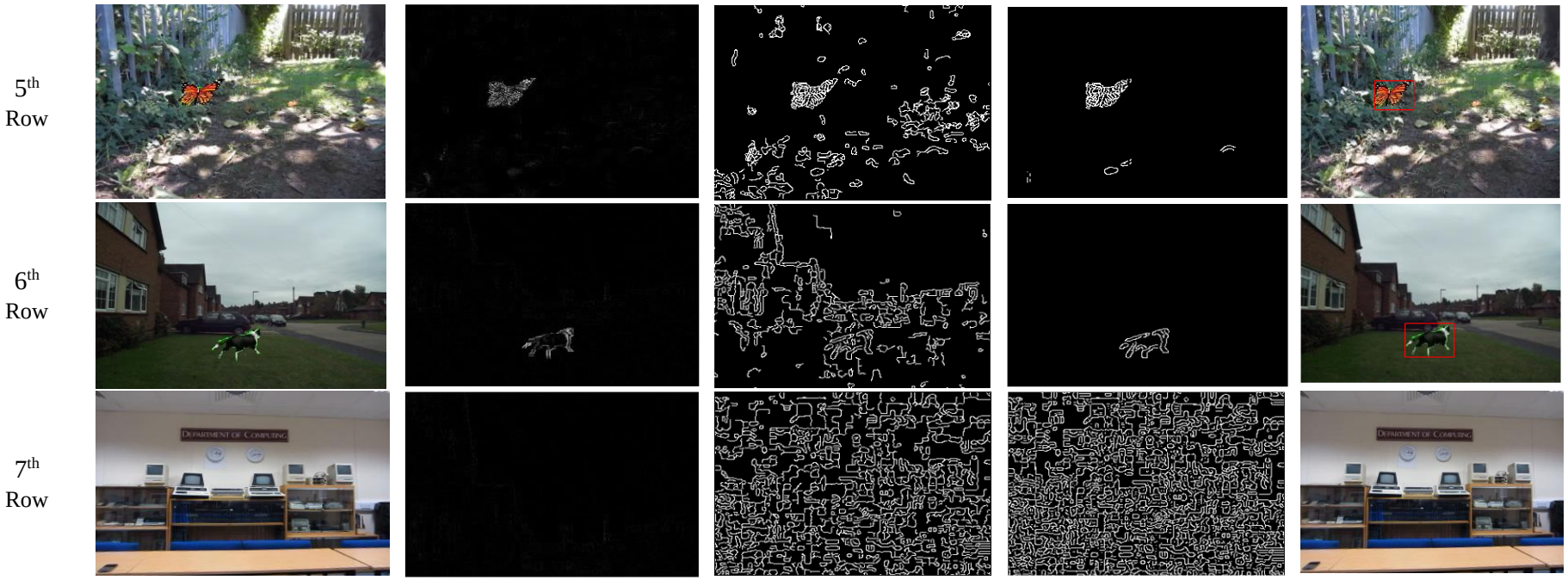


Figure 7.8: (a) Frame with CKF forgery (b) Grayscale difference frame (c) Edge frame of grayscale difference frame (d) Detection and isolation of CKF forgery (e) Tracking of CKF forgery

Similarly, the detction of CKF forgery in digital videos downloaded from the internet has been shown in Figure 7.9. Figure 7.9 (a) shows the frames of these digital videos with CKF forgery. The grayscale difference frames of these digital videos with CKF forgery have been shown in Figure 7.9 (b). Figure 7.9 (c) indicates the edge frames of these grayscale difference frames. The detection and isolation of CKF forgery have been shown in Figure 7.9 (d) whereas, Figure 7.9 (e) indicates the tracking of CKF forgery in frames of these digital videos.

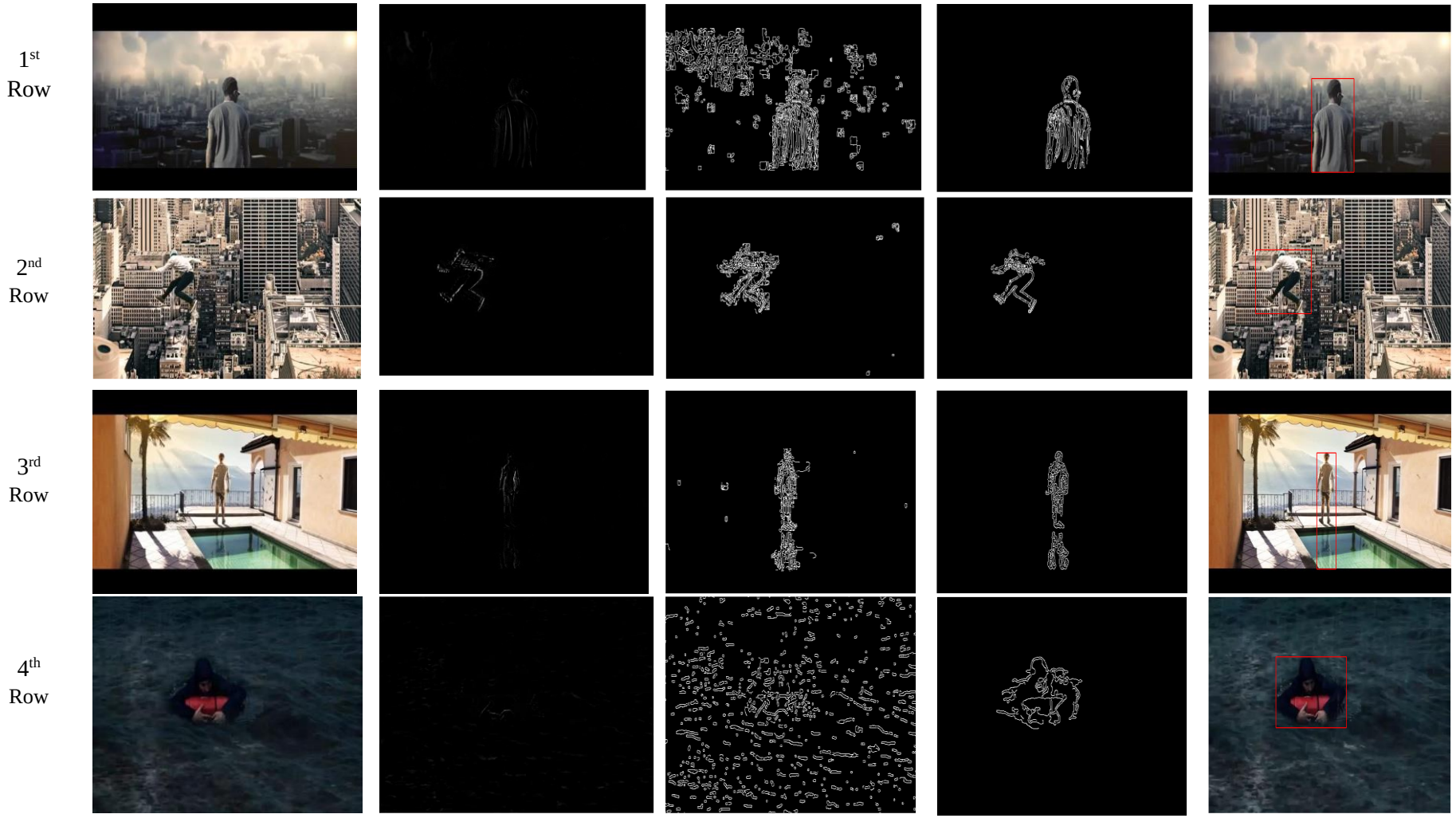


Figure 7.9: (a) Frames of digital videos with CKF forgery (b) Grayscale difference frame (c) Edge frame of grayscale difference frame (d) Detection and isolation of CKF forgery (e) Tracking of CKF forgery within the frame

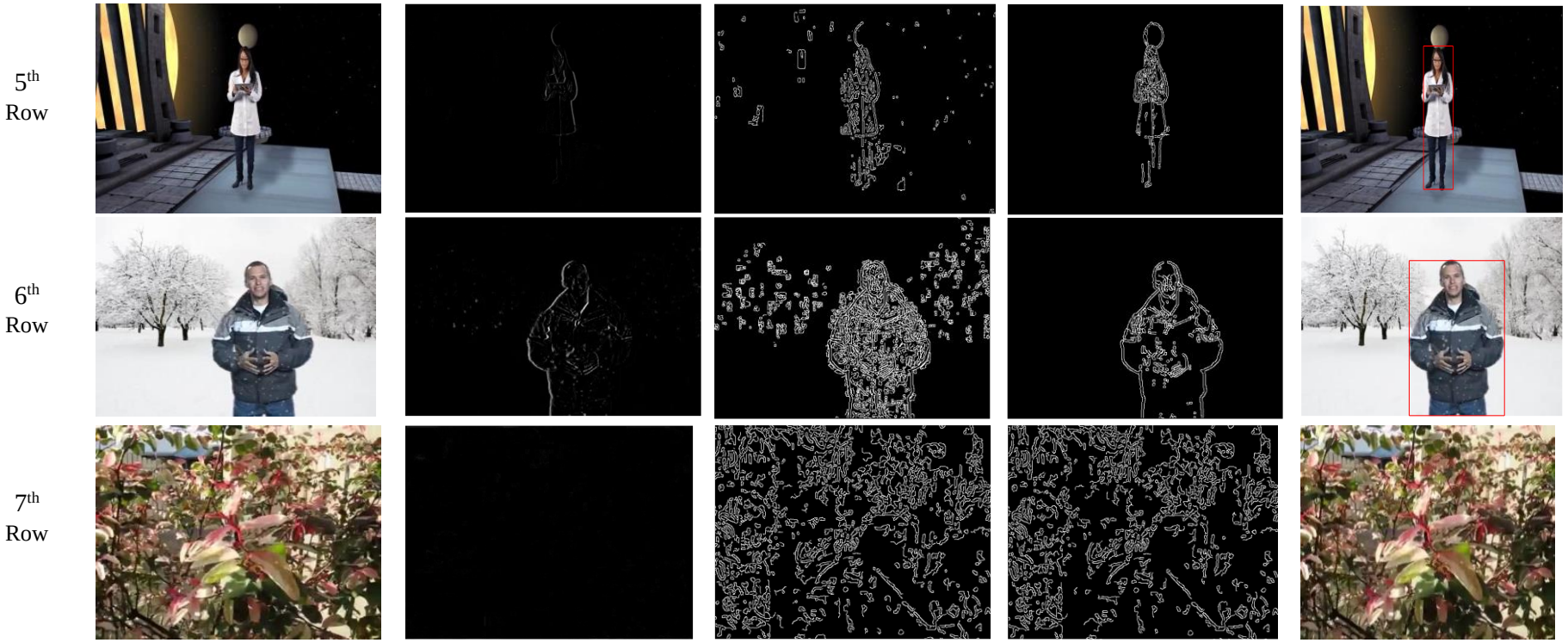


Figure 7.9 (a) Frames of digital videos with CKF forgery (b) Grayscale difference frame (c) Edge frame of grayscale difference frame (d) Detection and isolation of CKF forgery (e) Tracking of CKF forgery within the frame

CKF forgery detection based on FEI approach has also been performed to detect CKF forgery under various attacks such as Scaling attack, Rotational attack, Gaussian blurring attack, Compression attack, Gaussian noise attack with standard deviations, Poisson noise attack, Speckle noise attack, Salt & Pepper noise attack which are shown in Figure 7.10.

Figure 7.10 (a) shows the detection of CKF forgery by the proposed approach in the forged digital videos under Scaling attack with different scale factors (0.5, 1.0, 1.5, 2.0). The proposed approach has also detected CKF forgery under Rotational attack at different angles (10°, 20°, 30°, 40°, 50°, 60°, 70°, 80°, 90°) as shown in Figure 7.10 (b). Figure 7.10 (c) shows the detection of CKF forgery under Gaussian blurred attack with mask 3×3, 5×5, 7×7, 11×11 and $\sigma = 1$. The CKF forgery detection results of proposed approach under Compression attacks at different quantization factors (QF = 10, 30, 50, 70) have been shown in Figure 7.10 (d).

Figure 7.10 (e) shows the detection of CKF forgery under Gaussian noise attack with standard deviations (σ = 1.0, 1.5, 2.0, 2.5). CKF forgery in the forged digital videos which are affected by Poisson noise attack with different pixel scales (10^3, 10^7, 10^9, 10^{11}) are also detected as shown in Figure 7.10 (f). The detection of CKF forgery under the Speckle noise attack with different variances (0.0008, 0.003, 0.005, 0.01) and under Salt & Pepper noise attacks with different densities (d =0.0005, 0.0009, 0.005, 0.01) have been shown as shown in Figure 7.10 (g) and Figure 7.10 (h) respectively.

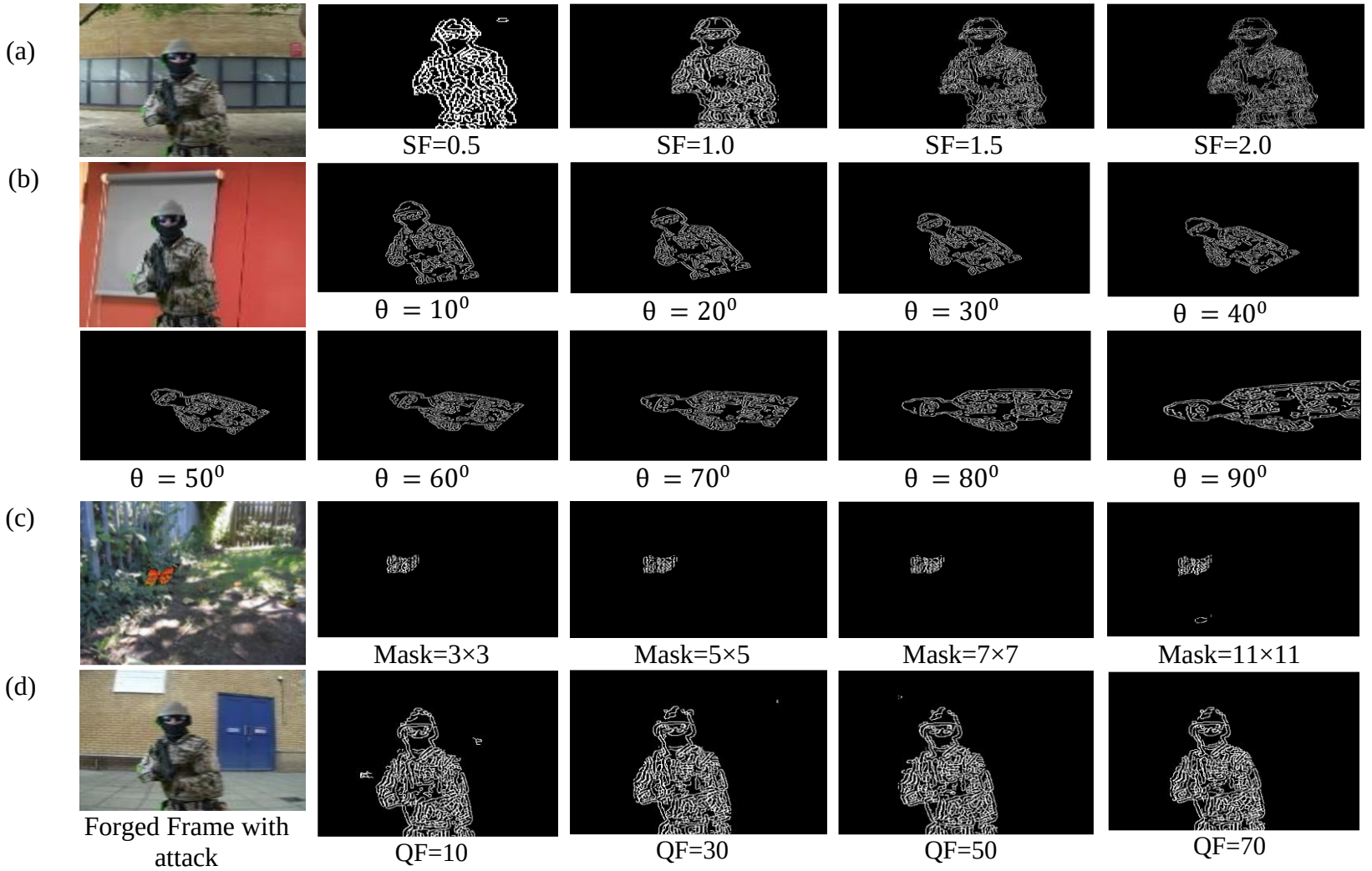


Figure 7.10: (a) Scaling attack (Scale factor = 0.5, 1.0, 1.5, 2.0) (b) Rotational attack (Angle = 10˚, 20˚, 30˚, 40˚, 50˚, 60˚, 70˚, 80˚, 90˚) (c) Gaussian Blurred attack with mask (3×3, 5×5, 7×7, 11×11) with σ = 1 (d) Compression attack (QF = 10, 30, 50, 70)

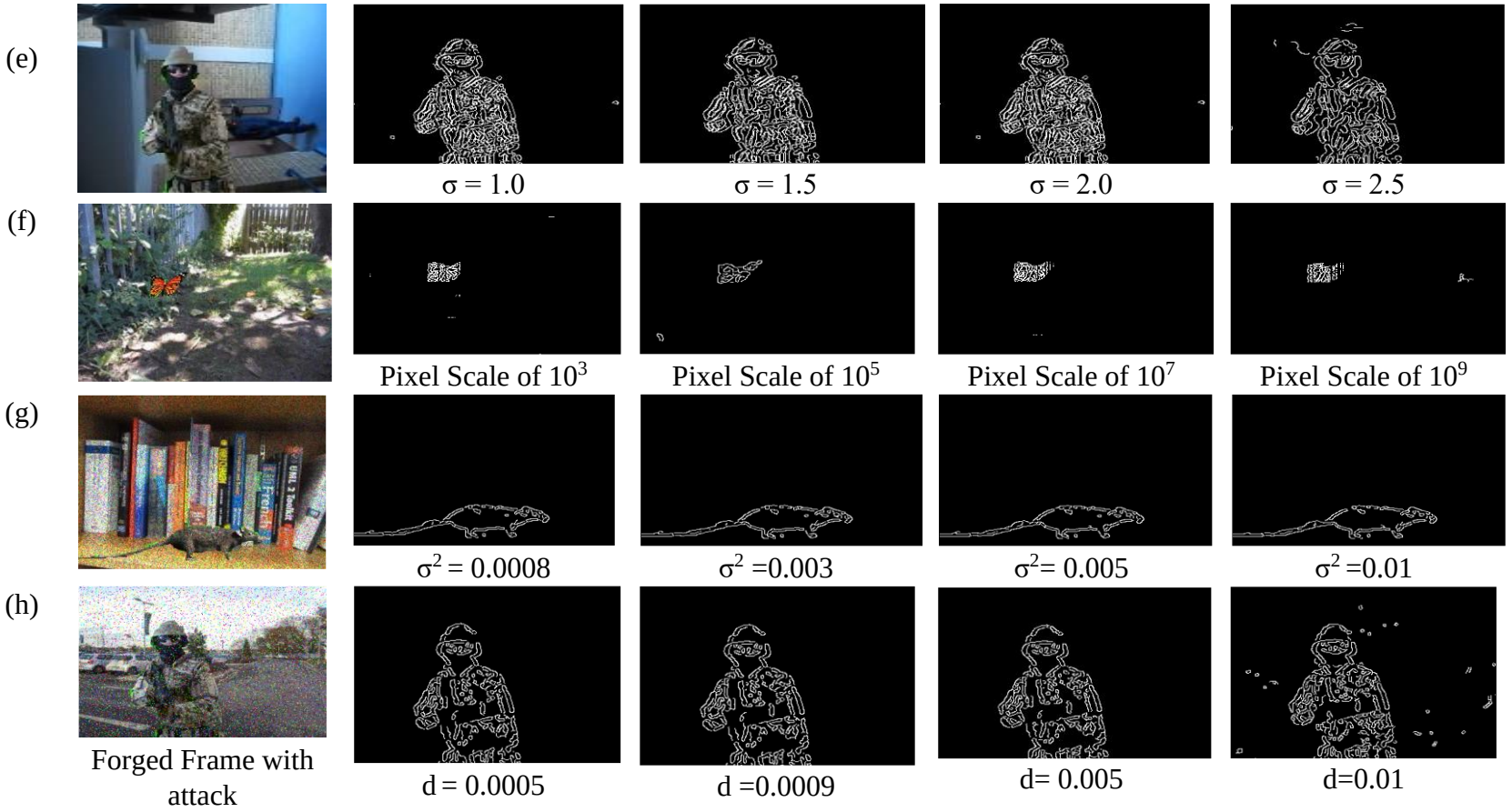


Figure 7.10 (e) Gaussion noise attack with Standard deviation (σ = 1.0, 1.5, 2.0, 2.5) (f) Poisson noise attack (pixel scales = 10^3, 10^5, 10^7, 10^9) (g) speckle noise attack (σ^2= 0.0008, 0.003, 0.005, 0.01) and (h) salt & papper noise attack (*d*= 0.0005, 0.0009, 0.005, 0.01)

7.2.2.2 Quantitative Performance Analysis

After the simulation results, CKF forgery detection based on FEI approach is also assessed quantitatively by taking into consideration various performance metrics. The proposed approach is subjected to evaluation on the basis of performance parameters such as PR, RR, DA, F measures (F1 score and F2 score), FPR, FNR, Sensitivity, Specifcity and execution time. The generated dataset is classified, which is based on the large edge pixel difference values of each edge frame, for the detection of CKF forgery in the digital videos. Each test video has been identified by comparing the rate of large edge pixel difference values with threshold value T′ which is obtained by OTSU algorithm. If the rate of large edge pixel difference values is less than T′ then outcomes are labelled as forged digital video. If the rate of large edge pixel difference values is more than T′ then outcomes are labelled as authentic digital video. Figures 7.11 and 7.12 indicate ROC curves for a testing set of SULFA dataset and internet videos.

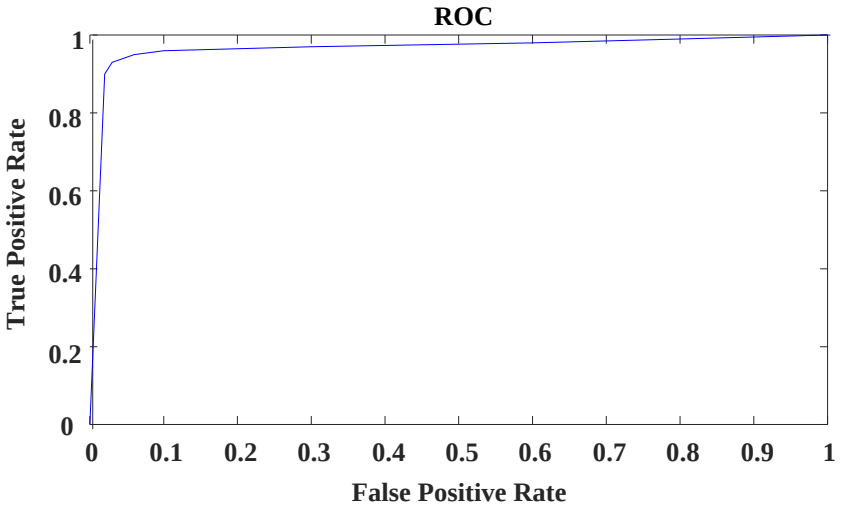


Figure 7.11 ROC curve for testing set of digital videos from SULFA dataset

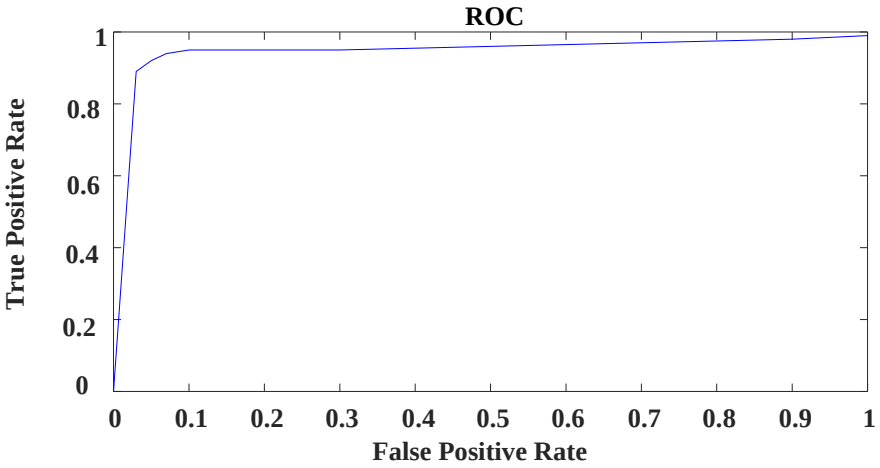


Figure 7.12 ROC curve for testing set of digital videos from the internet

Table 7.3 show the performance evaluation of CKF forgery detection based on FEI approach on SUFA dataset whereas, the perameters evaluation of proposed approach on SUFA dataset is shown in Table 7.4.

Table 7.3: Performance evaluation of CKF forgery detection based on FEI approach for testing set of digital videos from SULFA dataset

	Positive	**Negative**
True	0.968	0.984
False	0.032	0.016

Table 7.4: Parameters evaluation of CKF forgery detection based on FEI approach for testing set of digital videos from SULFA dataset

PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Specificity**
0.968	0.983	0.976	0.968	0.979	0.031	0.016	0.984	0.969

Table 7.3 shows the effective performance of CKF forgery detection based on FEI approach for detecting the authentic and forged digital videos. Table 7.4 provides better results which show the efficient capability of proposed approach for detecting CKF forgery in the digital videos. The proposed approach has also provided better performance for each separate case of digital videos as shown in Table 7.5.

Table 7.5: Parameters evaluation of the proposed approach for each separate case of test digital videos from SULFA dataset

Case	**PR**	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Specificity**
Case I	0.96	0.979	0.97	0.969	0.975	0.039	0.020	0.960	0.9607
Case II	0.928	0.966	0.948	0.947	0.959	0.069	0.033	0.966	0.9307
Case III	0.95	0.904	0.925	0.926	0.912	0.05	0.09	0.904	0.947
Case IV	0.916	0.923	0.919	0.919	0.921	0.08	0.07	0.923	0.916
Case V	0.875	0.879	0.877	0.876	0.878	0.124	0.120	0.879	0.875
Case VI	0.967	0.937	0.951	0.949	0.9408	0.034	0.062	0.937	0.965

Similarly, Table 7.6 show the performance evaluation of CKF forgery detection based on FEI approach on digital videos from the internet whereas, the perameters evaluation of proposed approach for these digital videos is shown in Table 7.7.

Table 7.6: Performance evaluation of CKF forgery detection based on FEI approach for testing set of digital videos from internet

	Positive	**Negative**
True	0.95	0.980
False	0.05	0.020

Table 7.7: Parameters evaluation of CKF forgery detection based on FEI approach for a testing set of digital videos from internet

PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensitivity**	**Specificity**
0.95	0.979	0.965	0.964	.0.973	0.048	0.020	0.98	0.952

Table 7.6 shows the actual performance of CKF forgery detection based on FEI approach on digital videos with CKF forgery from the internet. Table 7.7 provides superior results which show the capability of proposed approach for detecting CKF forgery in these digital videos.

DA of proposed approach has also been evaluated under various attacks with different parameters from Table 7.8 to Table 7.15. In Table 7.8, the proposed approach has been evaluated under Scaling attack with different scale factors (0.25, 0.50, 0.75, 1.0, 1.25, 1.50, 2.0). It indicates that DA is slightly decreased while the scaling factor is less than 1.0 and more than 1.5. Table 7.9 has been shown its better DA at different angles under the Rotational attack. Therefore, Table 7.8 and Table 7.9 show the effectiveness of proposed approach for detecting CKF forgery under Scaling and Rotational attacks at different scale factors and angles respectively. The proposed approach has detected CKF forgery efficiently under Gaussian blurred attack with mask 3×3, 5×5, 7×7, 9 × 9, 11×11 and $\sigma = 1$ as shown in Table 7.10. It shows that DA of the proposed approach has been affected with increase in mask size.

Table 7.8: Evaluation of proposed approach under Scaling attack with different scale factors (SF)

SF	**0.25**	**0.50**	**0.75**	**1.0**	**1.25**	**1.50**	**1.75**	**2.0**
DA	0.960	0.972	0.974	0.976	0.976	0.972	0.969	0.969

Table 7.9: Evaluation of proposed approach under Rotational attack with different angles **θ°**

θ°	**10°**	**20°**	**30°**	**40°**	**50°**	**60°**	**70°**	**80°**	**90°**
DA	0.976	0.976	0.976	0.976	0.976	0.976	0.976	0.976	0.976

Table 7.10: Evaluation of proposed approach under Gaussian blurred attack with masks of different size

Mask	**3 × 3**		**5 × 5**		**7 × 7**		**9 × 9**		**11 × 11**
DA	0.976		0.976		0.972		0.969		0.954

Table 7.11 shows that the DA of the proposed approach decreases with increase in the quantization factors (QF = 10, 20, 30, 40, 50, 60, 70, 80) and it becomes zero at quantization factors (QF = 90 and 100) because the quality of frame of a digital video is damaged at these quantization factors. Table 7.12 demostrates the effective performance of the proposed approach under Gaussian noise attack with standard deviations (σ = 0.005, 0.009, 0.05, 0.5, 1.0, 1.5, 2.0, 2.5). The proposed approach also provides better detection accuracy (DA) against poisson noise attack at different pixel scales (10^2, 10^3, 10^4, 10^5 10^7, 10^9, 10^{10}, 10^{11}) as shown in Table 7.13.

Table 7.11: Evaluation of proposed approach under Compression attack with different quantization factors (QF)

QF	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
DA	0.969	0.962	0.953	0.947	0.925	0.903	0.884	0.816	0.0	0.0

Table 7.12: Evaluation of proposed approach under Gaussian noise attack with different standard deviation (σ)

σ	**0.005**	**0.009**	**0.05**	**0.5**	**1.0**	**1.5**	**2.0**	**2.5**
DA	0.976	0.976	0.976	0.976	0.976	0.971	0.969	0.956

Table 7.13: Evaluation of proposed approach under Poisson noise with different pixel scale-up

Pixel Scale-up	$\mathbf{10^2}$	$\mathbf{10^3}$	$\mathbf{10^4}$	$\mathbf{10^5}$	$\mathbf{10^7}$	$\mathbf{10^9}$	$\mathbf{10^{10}}$	$\mathbf{10^{11}}$
DA	0.976	0.976	0.973	0.973	0.971	0.969	0.969	0.967

Similarly, Table 7.14 and Table 7.15 show the efficient performance of proposed approach in terms of DA under the Speckle noise attack with different variances (σ^2= 0.0002, 0.0004, 0.0006, 0.0008, 0.003, 0.005, 0.007, 0.01) and under Salt & Peppers noise attack with different densities (d= 0.0003, 0.0005, 0.0007, 0.0009, 0.001, 0.003, 0.005, 0.01) respectively.

Table 7.14: Evaluation of proposed approach under Speckle noise attack with different variances ($\boldsymbol{\sigma^2}$)

$\boldsymbol{\sigma^2}$	**0.0002**	**0.0004**	**0.0006**	**0.0008**	**0.003**	**0.005**	**0.007**	**0.01**
DA	0.976	0.976	0.974	0.974	0.972	0.969	0.965	0.963

Table 7.15: Evaluation of proposed approach under Salt & Peppers noise attack with different densities (*d*)

d	**0.0003**	**0.0005**	**0.0007**	**0.0009**	**0.001**	**0.003**	**0.005**	**0.01**
DA	0.976	0.976	0.976	0.972	0.972	0.970	0.969	0.965

After the implemetation of proposed approach under various attacks, it is observed that the proposed approach has also been performed effectively on the forged digital videos under the various attacks. It demonstrates that CKF forgery detection based on FEI approach also provides effective robustness under various attacks.

7.3 Comparative Analysis

The parameters of CKF forgery detection based on FEI approach have been compared with the existing techniques of CKF forgery detection such as Liu *et al.* [51] and Lichao *et al.* [59] in Table 7.16. It indicates higher DA of the proposed approach as compared to the existing techniques. The proposed approach has also improved more parameters such as RR, F1 score, F2 score, FPR, FNR, sensitivity and specificity than Lichao *et al*. as shown in Table 7.16.

Table 7.16: Comparison between CKF forgery detection based on FEI approach and existing techniques

	PR	**RR**	**DA**	**F1**	**F2**	**FPR**	**FNR**	**Sensiti -vity**	**Specifi -city**
Liu *et al.* [51]	**0.973**	0.925	0.947	0.948	0.934	**0.028**	0.074	0.925	**0.971**
Lichao *et al.* [59]	0.935	0.849	0.931	0.890	0.865	0.071	0.150	0.849	0.928
Proposed	0.968	**0.983**	**0.976**	**0.968**	**0.979**	0.031	**0.016**	**0.984**	0.969

Bold indicates the higher values of the parameters

The false alarm and DA are determined by calculating the percentage of digital videos that are incorrectly classified as forged digital videos and the percentage of correctly classified digital videos respectively. The DA of 97.6% has been achieved at a false alarm rate of 3.1% by the proposed approach for the SULFA dataset digital videos as shown in Table 7.16. On the other side, DA of 96.5% is achieved at a false alarm rate of 4.8% by the proposed approach for digital videos which are downloaded from the internet as shown in Table 7.7.

In the proposed approach, PR is slightly decreased by 0.5% due to decrease in its true positive values whereas, its FPR is slightly increased by 0.3% and specificity is decreased by 0.2% due to increase in false positive values than that of Liu *et. al.* Therefore, PR of the proposed approach is slightly lower than that of Liu *et al.* However, PR and FPR of the proposed approach is higher than that of Lichao *et al.* as shown in Table 7.16.

Due to increase in true negative values, the RR of proposed approach is increased and FNR is decreased than that of Liu *et al.* and Lichao *et al.* Thus, the proposed approach has detected many forged digital videos with higher DA than Liu *et al.* and Lichao *et al.* The higher F1 and F2 scores of proposed approach also indicate in Table 7.16 that the search effectiveness of proposed approach is more than that of Liu *et al*. and Lichao *et al*. F-scores are dependent on the values of PR and RR. The sensitivity of proposed approach is higher than Liu *et al.* and Lichao *et al.* because of less number of false negative values than the existing techniques. The specificity of proposed approach is slightly decreased than that of Liu *et al.* whereas, it is higher than that of Lichao *et al.* as shown in Table 7.16. Thus, these results indicate that the proposed approach has performed effectively for detecting CKF forgery in the digital videos.

7.4 Computational Cost

The execution time of CKF forgery detection based on FEI approach for detecting CKF forgery in the digital videos has been shown in Table 7.17 which indicates the minimum execution time for the digital videos having resolutions of 320 × 240 and 720 × 480.

Table 7.17: Comparison of the execution time of the proposed approach with existing techniques

Video Resolution	Video Format	Video Type	Execution Time (s/frame)	
			Liu *et al.* [51]	**Proposed**
720 × 480	.mov	Forged	1.87	**0.55**
320 × 240	.avi	Forged	-	**0.43**
720 × 480	.mov	Authentic	2.65	**0.52**
320 × 240	.avi	Authentic	-	**0.39**

- means data has not been calculated in the paper and bold indicates the higher values of the parameters

The proposed approach provides the average execution time of 0.43 s per frame for forged digital videos having 320× 240 resolution and 0.39 s per frame for authentic digital videos of 320×240 resolution. It also provides the average execution time of 0.55 s per frame for forged digital videos having 720× 480 resolution and 0.52 s per frame for authentic digital videos of 720×480 resolution. The execution time of proposed approach has also been compared with existing techniques in Table 7.17 which demonstrates that the execution time is less for the proposed approach than existing techniques. The fact is that the proposed approach has neither need of segmentation of the video frame nor a large number of blocks of foreground and background for the detection of CKF forgery in the digital videos. In the existing techniques, these processes take more time for their execution whereas, the proposed approach works on the identification of edges of CKF forgery in the edge frame which reduces a large amount of execution time efficiently. Thus, CKF forgery detection based on FEI approach provides minimum execution time for detecting CKF forgery in the digital videos.

7.5 Summary

In this chapter, CKF forgery detection based on FEI approach has detected large and small sized CKF forgery in different cases and circumstances of SULFA dataset digital videos. This approach has effectively detected CKF forgery in the relistic cases. The proposed approach has also efficiently detected CKF forgery in the digital videos under various attacks. It has capability of isolating and differentiating CKF forgery from the authentic foreground in the digital videos. The simulation results show that the proposed approach has performed

efficiently on different digital videos with higher DA and lower execution time as compared to the existing techniques. The performance of proposed approach under various attacks provides its effective robustness.

CHAPTER 8

CONCLUSIONS AND FUTURE SCOPE

The research work discussed in the previous chapters has been summarised in this chapter. Scope and future prospects of the work are also presented.

8.1 Conclusions

This research work is oriented towards detecting CMFD, CMRD and CKF forgeries in digital videos. The performance of each proposed approach has been evaluated on the digital videos from the SULFA dataset and internet. Results obtained from the research work have been stated as follows.

CMFD forgery detection approach is based on detecting the similarities between frame sequences that have been detected at the long continuous location and many different locations in the digital videos using CC. In contrast, the existing techniques have been detected small frames sequence duplication at a location. This approach has also detected frame sequences duplicated from other digital videos using CV. Thus, it is observed that the proposed approach is more effective for detecting the different ways of frame duplication in digital videos than the existing techniques. The experimental results indicate its effective performance for CMFD forgery detection with a better DA of 99.5%. It also indicates efficient results in execution time for different resolutions of the digital videos. This approach has the limitation that it can't detect fewer duplicated frames than the considered frame sequence in the digital videos.

The limitation of detecting the less number of duplicated frames has been removed in multiple CMFD forgery detection approach. This proposed approach is based on ECBV, which has efficiently detected multiple frame duplications in digital videos, such as single duplicated frame within the entire digital video, repetition of a frame in the form of sequence, shuffling of frame sequence and disordered frames in sequence. The comparison of the proposed approach with existing techniques clarifies that the proposed approach provides a higher DA of 99.85% and gives better results in terms of different evaluation parameters such as PR, RR, F1, and F2 than existing techniques. It is also noticed that the execution time of the proposed approach is much less than existing techniques for the different resolutions.

CMRD forgery detection approach is based on CC and CV, which has detected rectangular and square shape regular region duplications and irregular region duplications with many irregularities within the same frames and from the other frames of the digital videos. The experimental results show its effective performance for CMRD forgery detection with a better

DA of 96.6 % than existing techniques. Despite this, it has calculated more PR, RR, F1, and F2 parameters. It also indicates its better results in execution time for different resolutions of the digital videos. This approach is limited because it can't detect the smallest duplicated region in the digital videos.

The drawback of detecting the smallest duplicated regions in the digital videos has been eliminated by the multiple CMRD forgery detection approach based on HE and block filtering. This approach has detected the single and multiple CMRD forgeries of different region sizes such as 3× 3, 4× 4, 8×8, 16×16, 24× 24, and 32× 32 in digital videos. HE distributes the pixel intensity values uniformly over a large intensity range in the blocks of each frame, which enable to detect of a small forged region of frame in the digital video whereas, the block filtering is used to remove the false positives and false negatives, which makes this approach to be more effective. The proposed approach gives a higher DA of 98.6 % for detecting multiple CMRD forgeries having a different region size in the digital videos than existing techniques. This approach has also provided better results in the execution time for different resolutions of the digital videos. This approach has worked on digital videos of SULFA dataset and natural digital videos downloaded from the internet. It has not worked on CMRD from different frames of the digital video.

The CKF forgery detection approach is based on FEI, which has detected CKF forgery in digital videos. After the CKF forgery detection, this approach has isolated the forgery from the authentic part of the edge frame. This approach provides the localization and tracking of CKF forgery in each frame of the forged digital video. The proposed approach has performed efficiently on the digital videos with different cases taken from the SULFA dataset. The various attacks have evaluated this approach on the digital videos for its effective robustness. It has also been implemented on digital videos, which are downloaded from the internet. The experimental results indicate its higher DA of 97.6 % and lower execution time than the existing techniques. The results under various attacks also demonstrate better robustness of the CKF forgery detection approach than others. The proposed approach is not able to detect the chroma key foreground forgery under compression attack with a quantization factor of 90 and 100 because the quality of frame of a digital video is damaged at these quantization factors. It is also not capable for detecting very small sized forged foreground in the digital videos because it creates very few difference values.

8.2 Main Highlights of the Research Work

The major highlights of the presented work in the field of CM forgery detection in the digital videos are as follows:

- CMFD forgery detection approach based on CC and CV is proposed for detecting the CMFD forgery at the large continuous location, at different locations with different frame sequences, and other digital videos. Evaluating the proposed approach on digital videos taken from the SULFA dataset and internet provided promising results.
- ECBV based multiple CMFD forgery detection approach has been developed to detect multiple CMFD forgeries like SFD, RF, SFS, and DFS in digital videos. Its experimental results demonstrate that this approach achieved DA of 99.7% at an FNR of 0.05 %.
- Coefficients based CMRD forgery detection approach is designed to detect CMRD forgery as regular rectangular and square shape region duplication within the same frame and from another frame in the digital videos. This approach also detects irregular region duplication within the same frame and from another frame. This approach is provided effective detection results on digital videos from the SULFA dataset and internet.
- Multiple CMRD forgery detection approach is proposed to detect the multiple CMRD forgeries with different region sizes like 3× 3, 4× 4, 8×8, 16×16, 24× 24, and 32× 32 in digital videos. The performance of this proposed approach shows efficient results on the digital videos having different resolutions.
- CKF forgery detection based on the FEI approach is developed to detect CKF forgery. This approach isolated and differentiated the CKF forgery from the authentic foregrounds of the digital videos. Implementing this approach on the digital videos of the SULFA dataset, digital videos downloaded from the internet, and under various attacks has provided effective results with better robustness.

8.3 Future Scope

The research work in this thesis can be extended in the following directions for further explorations in this field:

- Future work can be dedicated to using CNN to improve CMFD, CMRD and CKF forgeries detection techniques.

- The presented work on CMFD forgery detection can be further expanded to detect the compressed duplicated frame sequences in digital videos.
- A framework can be designed to detect the CMRD forgery within an enhanced frame.
- The proposed work on CKF forgery detection can be stretched for detecting too small forged foregrounds in digital videos.

REFERENCES

[1] Anshida K. and Sabitha K., "Video Forgery Detection using RGB Color Correlation and Multiclass SVM Classifiers, *Int. J. Engg. Res. and Tech.*, vol. 3, no. 5, pp. 1-6, 2015.

[2] Abdalla Y., Iqbal T., and Shehata M., "Convolutional Neural Network for Copy-Move Forgery Detection," *Symmetry*, vol. 11, no. 10, pp.1–17, 2019.

[3] Bangare S. L. and Patil S., "Reviewing Otsu's Method For Image Thresholding," *Int. J. Applied Engg. Res.*, 2015, https://doi.org/10.37622/ijaer/10.9.2015.21777-21783

[4] Bao P., Zhang L. and Wu X., "Canny Edge Detection Enhancement by Scale Multiplication," *IEEE Tran. Pattern Analysis Machine Intell.*, vol. 27, no. 9, pp. 1485–1490, 2005.

[5] Bagiwa M.A., Wahab A.M.A., Idris M.Y.I., Khan S. and Choo K.K.R, "Chroma key background detection for digital video using statistical correlation of blurring artefact," *Digit. Investig.*, vol.19, pp. 29–43, 2016.

[6] Bozkurt I., M.H. and Ulutas G., "A new video forgery detection approach based on forgery line," *Turkish J. Elect. Engg. Comput. Sci.*, vol. 25, pp. 4558–4574, 2017.

[7] Bestagini P., Milani S., Tagliasacchi M., and Tubaro S., "Local tampering detection in video sequences," in *Proc. IEEE 15th Int. Workshop Multimed. Signal Process.*, pp. 488–493, 2013.

[8] Bilal M., Habib H.A., Mehmood Z., Yousaf R.M., Saba T. and Rehman A., "A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHESURF features and DBSCAN clustering," *Australian J. Forensic Sci.*, 2020. DOI: 10.1080/00450618.2020.1715479

[9] Bidokhti A. and Ghaemmaghami S., "Detection of regional copy/move forgery in MPEG videos using optical flow," in *Proc. IEEE Int. Symp. Artif. Intell. Signal Process.*, pp. 13–17, 2015.

[10] Bakas J. and Naskar R., "A Digital Forensic Technique for Inter–Frame Video Forgery Detection Based on 3D CNN," In: Ganapathy V., Jaeger T., Shyamasundar R. (eds) Inf. Syst. Security, Lecture Notes in Comput. Sci., vol. 11281. *Springer*, Cham. https://doi.org/10.1007/978-3-030-05171-6_16

[11] Bhardwaja S. and Mittalb A., "A Survey on Various Edge Detector Techniques," *Procedia Tech.*, vol. 4, pp. 220 –226, 2012.

[12] Biswasa R. and Sila J., "An Improved Canny Edge Detection Algorithm Based on Type-2 Fuzzy Sets," *Procedia Tech.*, vol. 4, pp. 820–824, 2012.

[13] Bakas J., Naskar R. and Dixit R., "Detection and localization of inter-frame video forgeries based on inconsistency in correlation distribution between Haralick coded frames," *Multimed. Tools Appl.*, vol. 78, pp. 4905–4935, 2019.

[14] Canny J., "A Computational Approach to Edge Detection," IEEE Trans. Pattern Analysis Machine Intell. 8 (6): 679–698.

[15] Chetty G., Biswas M., and Singh R., "Digital video tamper detection based on multimodal fusion of residue features," In *proc. IEEE Int. Conf. Network Syst. Security*, 2010, pp. 606–613.

[16] Chao J., Jiang X., and Sun T., "A novel video inter-frame forgery model detection scheme based on optical flow consistency," in *Proc. Int. Workshop digital watermarking*, Springer, 2012, pp. 267–281.

[17] Chen S., Tan S., Li B. and Huang J., "Automatic detection of object-based forgery in advanced video," *IEEE Trans. Circuits Syst. Video Tech*., 26 (11): 2138- 2151.

[18] Christlein V., Riess C., Jordan J., Riess C., and Angelopoulou E., "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[19] Cozzolino D., Poggi G., Sansone C., Verdoliva L. (2012) A Comparative Analysis of Forgery Detection Algorithms. In: Gimel'farb G. et al. (eds) Structural, Syntactic, and Statistical Pattern Recognition. SSPR /SPR 2012. Lecture Notes in Computer Science, vol 7626. *Springer*, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34166-376

[20] Dong Q., Yang G., and Zhu N., "A MCEA based passive forensics scheme for detecting frame-based video tampering," *Digit. Investig.*, vol. 9, no. 2, pp. 151–159, 2012.

[21] Ding L. and Goshtasby A., "On the Canny edge detector," *Pattern Recognit.*, vol. 34, pp. 721–725, 2001.

[22] Dataset available [online] Surrey University Library for Forensic Analysis (SULFA), http://sulfa.cs.surrey.ac.uk/videos.php

[23] Emam M., Han Q., and Niu X., "PCET based copy-move forgery detection in images under geometric transforms," *Multimed Tools Appl*. vol. 75, pp. 11513–11527, 2015.

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

[25] Fadl S.M., Han Q. and Li Q., "Authentication of surveillance videos: detecting frame duplication based on residual frame," *J. Forensic Sci*., vol. 63, no. 4, pp. 1–11, 2017.

[26] Fadla S., Hana Q., and Li Q., "CNN spatiotemporal features and fusion for surveillance video forgery detection," *Signal Process.: Image Commun.*, https://doi.org/10.1016/j.image.2020.116066

[27] Gavade J.D. and Chougule S.R., "Review of Techniques of Digital Video Forgery Detection," *Adv. Comput. Sci. Inf. Tech.*, vol. 2, no. 3, pp. 233–236, 2015.

[28] Gironi A., Fontani M., Bianchi T., Piva A. and Barni M., "A Video Forensic Technique for Detecting Frame Deletion and Insertion," in *Proc. IEEE Int. Conf. on Acoust., Speech, Signal Process*, 2014, pp. 6226–6230.

[29] Gandhi S.A. and Kulkarni C.V., "*MSE vs SSIM*," Int. J. Scientific Engg. Res., 4(7): 930–934, 2013.

[30] Hyun D.K., Ryu S.J., Lee H.Y. and. Lee H.K, "Detection of Upscale-Crop and Partial Manipulation in Surveillance Video Based on Sensor Pattern Noise," *Sensors*, vol. 13, no. 9, pp. 12605–12631, 2013.

[31] Hu Y., Li C., Wang Y., and Liu B., "An Improved Fingerprinting Algorithm for Detection of Video Frame Duplication Forgery," *Int. J. Digit. Crime Forensics*, vol.4, no. 3, pp. 20–32, 2012.

[32] Hsu C.C., Hung T.Y., Lin C.W., and Hsu C.T.. "Video Forgery Detection Using Correlation of Noise Residue. In *Proc. IEEE 10th Workshop Multimed. Signal Process.*, 2008, pp. 170-174.

[33] He J., Lin Z., Wang L., and Tang X., "Detecting doctored JPEG images via DCT coefficient analysis," in proc. European Conf. Comput. Vision, Graz, Austria, 2006.

[34] Hashmi M.F., Anand V., and Keskar A.G., "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform," *AASRI Procedia*, vol. 9, pp. 84–91, 2014.

[35] Jia S., Ku Z, Wang H., and Feng C., "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics*," IEEE Access*, 2017, DOI: 10.1109/ACCESS.2018.2819624

[36] Johnston P. and Elyan E., "A review of digital video tampering: From simple editing to full synthesis, *Digit. Investig*. vol. 29, pp. 67–81, 2019.

[37] Juneja M. and Sandhu P. S., "Performance Evaluation of Edge Detection Techniques for Images in Spatial Domain," *Int. J. Comput. Theory Engg*., vol. 1, no. 5, pp. 1793–8201, 2009.

[38] Kobayashi M., Okabe T., and Sato Y., "Detecting video forgeries based on noise characteristics," in *Pacific-Rim Symp. Image Video Tech.* Springer, 2009, pp. 306–317.

[39] Kobayashi M., Okabe T., and Sato Y., "Detecting forgery from static-scene video based on inconsistency in noise level functions," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 883–892, 2010.

[40] Kansal H., Purwar S., and Tripathi R.K., "Image Contrast Addusing Unsharp Masking and Histogram Equalization. *Multimed. Tools Appl*., vol. 77, pp. 26919–26938, 2018.

[41] Kim J.Y., Kim L.S., and Hwang S.H., "An advanced contrast enhancement using partially overlapped sub-block histogram equalization", *IEEE Trans. Circuits Syst. Video Tech*., vol. 11, no. 4, pp. 475-484, 2001.

[42] Kurita T., Otsu N., and Abdelmalek N., "Maximum likelihood thresholding based on population mixture models," *Pattern Recognit.*, vol. 25, pp. 1231-1240, 1992.

[43] Kaur J. and Kumar A., "Evaluating the Shortcomings of Edge Detection Operators," *Int. J. Adv. Res. Comput. Sci. Software Engg*., vol. 5, no. 5, pp. 235–241, 2015.

[44] Katiyar S.K. and Arun P.V., "Comparative analysis of common edge detection techniques in context of object extraction," *IEEE Trans. Geosci. Remote Sensing*, vol. 50, no.11, 2012.

[45] Kingra S., Aggarwal N. and Singh R.D., "Inter-frame forgery detection in H.264 videos using motion and brightness gradients," *Multimed. Tools Appl.,* vol. 76, pp. 25767–25786, 2017.

[46] Karthikasini G. and Prathiba T., "Video Forgery Recognition Using SIFT, SVD and DWT," in *Proc. national conf. innovation comput. commun. tech*., pp. 287-292, 2014.

[47] Kharat J. and Chougule S., "A passive blind forgery detection technique to identify frame duplication attack," *Multimed. Tools Appl*., vol. 79, pp. 8107–8123, 2020.

[48] Kaur H. and Jindal N., "Image and Video Forensics: A Critical Survey," *Wireless Pers. Commun.*, vol. 112, pp. 1281–1302, 2020.

[49] Kaur, H., Jindal, N., "Deep Convolutional Neural Network for Graphics Forgery Detection in Video." Wireless Pers Commun., 112, 1763–1781 (2020). https://doi.org/10.1007/s11277-020-07126-3

[50] Kingra S., Aggarwal N. and Singh R.D., "Video Inter-frame Forgery Detection: A Survey," *Indian J. of Sci. Tech*., vol. 9, no. 44, pp. 1–9, 2016.

[51] Liu Y., Huang T. and Lin Y., "A novel video forgery detection algorithm for blue screen compositing based on 3-stage foreground analysis and tracking," *Multimed. Tools Appl*., vol. 77, pp. 7405–7427, 2018.

[52] Lin G.S., Chang, J.F. and Chuang C.H., "Detecting frame duplication based on spatial and temporal analyses," In *Proc. IEEE Int. Conf. Comput. Sci. Edu*., 2011, pp.1396–1399.

[53] Liao S.Y., and Huang T.Q., "Video Copy-Move Forgery Detection and Localization Based on Tamura Texture Features," in *Proc. IEEE Int. Conf. Image Signal Process*., pp. 864–868, 2013.

[54] Liu Y. and Huang T., "Exposing video inter-frame forgery by Zernike opponent chromaticity moments and coarseness analysis," *Multimed. Syst*., vol. 23, pp. 223–238, 2017.

[55] Li F. and Huang T., "Video Copy-Move Forgery Detection and Localization Based On Structural Similarity," in *Proc. 3rd int. conf. Multimed. Tech.,* Springer, pp. 63–76, 2014.

[56] Lin G.S., and Chang J.F., "Detection of frame duplication forgery in videos based on spatial and temporal analysis," *Int. J. Pattern Recognit. Artif. Intell*., vol. 26, no. 7, pp. 1-18, 2012.

[57] Lukas J. and Fridrich J., "Estimation of primary quantization matrix in double compressed JPEG images," in *Digital Forensic Research Workshop,* Cleveland, Ohio, 2003.

[58] Li L., Li S., and Wang J., "Copy-move forgery detection based on PHT," *World Congress Inf. Commun. Tech.,* 2012, pp. 1061-1065.

[59] Lichao S., Luo H., and Wang S., "A Novel Forgery Detection Algorithm for Video Foreground Removal," *IEEE Acces, vol.* 7, pp. 109719 – 109728, 2019.

[60] Lin C.S., and Tsay J.J., "Passive Approach for Video Forgery Detection and Localization," in *Proc. Int. Conf. Cyber Security, Cyber Warfare and Digital Forensic,* pp. 107–112, 2013.

[61] Li Z., Zhang Z., Guo S., and Wang J., "Video inter-frame forgery identification based on the consistency of quotient of MSSIM," *Security Commun. Networks*, vol. 9, no, 17, pp. 4548–4556, 2016.

[62] Long C., Basharat A. and Hoogs A., "A Coarse-to-fine Deep Convolutional Neural Network Framework for Frame Duplication Detection and Localization in Forged Videos", Computer Vision and Pattern Recognition, 2018, https://doi.org/10.48550/arxiv.1811.10762

[63] Meena K.B., and Tyagi V., "A copy move image forgery detection technique based on tetrolet transform," J. Info. Security Appl., vol. 52, 2020. https://doi.org/10.1016/j.jisa.2020.102481

[64] Manu V.T. and Mehtre B.M., "Detection of Copy-Move Forgery in Images Using Segmentation and SURF," in: Thampi S., Bandyopadhyay S., Krishnan S., Li KC., Mosin S., Ma M. (eds.) Adv. Signal Process. Intell. Recognit. Syst. Adv. Intell. Syst. Comput., 2016, 425. *Springer,* Cham. https://doi.org/10.1007/978-3-319-28658-7_55

[65] Ndajah P., Kikuchi H., Yukawa M., Watanabe H., and Muramatsu S., "SSIM image quality metric for denoised images," in *Proc. 3rd Int. Conf. on Visualization, Imaging Simulation*, 2010, pp. 53-58.

[66] Nawaz M., Mehmood Z., Nazir T., Masood M., Tariq U., Munshi A.M., A. Mehmood and M. Rashid, "Image Authenticity Detection Using DWT and Circular Block-Based LTrP Features. Computers," *Materials & Continua*, vol. 69, no. 2, pp. 1927–1944, 2021.

[67] Ojeniyi J., Adedayo B., Idris I. and Abdulhamid S., "Hybridized technique for copy-move forgery detection using discrete cosine transform and speeded-up robust feature techniques," *Int. J. Image Graphics Signal Process*., vol. 10, pp. 22–30, 2018.

[68] Otsu N., "A threshold selection method from gray level histogram," *IEEE Trans. Syst., Man, Cybernetics*: *Syst.*, vol. 9, no. 1, pp. 62–66, 1979

[69] Online Available: Canny Edge Detection, March 23, 2009. http://www.cse.iitd.ernet.in/~pkalra/col783-2017/canny.pdf

[70] Online Available: https://en.wikipedia.org/wiki/Coefficient_of_variation

[71] Online Available: R. Dorothy, R.M. Joany, R. J. Rathish, S.S. Prabha, and S. Rajendran, "Image enhancement by Histogram equalization" ISSN Online: 2395-7018,https://www.researchgate.net/publication/283727396_Image_enhancement_by_Histogram_equalization

[72] Online Available: https://www.youtube.com

[73] Online Available: https://en.wikipedia.org/wiki/Variance

[74] Online Available: https://en.wikipedia.org/wiki/Average

[75] Online Available: https://en.wikipedia.org/wiki/Sensitivity_and_specificity

[76] Pandey R., S. Singh K., and Shukla K.K., "Passive Copy-Move forgery detection in videos," in *Proc. IEEE Int. Conf. Comput. Commun. Tech*., pp. 301–306, 2014.

[77] Pandey R.C., Singh S.K., and Shukla K.K., "Passive Copy- Move Forgery Detection Using Speed-Up Robust Features, Histogram Oriented Gradients and Scale Invariant Feature Transform," *Int. J. Syst. Dynamics Appl*., vol. 4, no. 3, pp. 70–89, 2015.

[78] Prakash CS, Panzade PP, Om H, Maheshkar S (2019) Detection of copy-move forgery using AKAZE and SIFT keypoint extraction. Multimed Tools Appl. 78:3535–23558.

[79] Pun C., Yuan X., and Bi X., "Image Forgery Detection Using Adaptive Over segmentation and Feature Point Matching," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1705–1716, 2015.

[80] Prakash S., Kumar A., Maheshkar S., and Maheshkar V., "An integrated method of copy-move and splicing for image forgery detection," Multimed. Tools Appl., vol. 77, no. 20, pp. 26939–26963, 2018.

[81] Qiao M., Sung A., Liu Q., and Riberio B., "A novel approach for detection of copy-move forgery," in *Proc. 5th Int. Conf. Adv. Engg. Comput. App. in Sci.*, 2011, pp. 44–47.

[82] Rong W., Li Z., Zhang W. and Sun L., "An Improved Canny Edge Detection Algorithm," in *Proc. IEEE Int. Conf. Mechatronics Automation*, Tianjin, China, 2014, pp. 577–582.

[83] Ren H., Atwa W., Zhang H., Muhammad S., and Emam M., "Frame Duplication Forgery Detection and Localization Algorithm Based on the Improved Levenshtein Distance," *Hindawi Sci. Program.*, 2021, https://doi.org/10.1155/2021/5595850

[84] Raju M. and Nair M. S., "Copy-move forgery detection using binary discriminant features," *J. King Saud University Comput. Inf. Sci.*, 2018, https://doi.org/10.1016/j.jksuci.2018.11.004

[85] Sitara K. and Mehtre B.M., "Digital video tampering detection: An overview of passive techniques," *Digit. Investig.*, vol.18, pp. 8–22, 2016.

[86] Singh R.D. and Aggarwal N., "Video content authentication techniques: A comprehensive survey," *Multimed. Syst.*, vol. 24, pp. 211–240, 2017.

[87] Shelke N.A. and Kasana S.S., "A comprehensive survey on passive techniques for digital video forgery detection," *Multimed. Tools Appl.* Vol. 80, pp. 6247–6310, 2020.

[88] Singh R.D., and Aggarwal N., "Detection of upscale-crop and splicing for digital video authentication. *Digit. Investig.*, 21, pp. 31-52, 2017.

[89] Su Y., Han Y., and Zhang C,, "Detection of Blue Screen Based on Edge Features," in *Proc. 6th IEEE Int. Conf. Inf. Tech. Artif. Intell.*, 2011, pp. 469-472.

[90] Shanableh T., "Detection of frame deletion for digital video forensics," *Digit. Investig.*,Vol. 10, no. 4, pp. 350-360, 2013.

[91] Singh V.K., Pant P. and Tripathi R.C., "Detection of Frame Duplication Type of Forgery in Digital Video Using Sub-block Based Features," In: James J., Breitinger F. (eds.) Digital Forensics and Cyber Crime. ICDF2C 2015. Lecture Notes of the Institute for Computer Sciences, *Social Inf. Telecommun. Engg.*, vol. 157. *Springer*, Cham, pp. 29–38, https://doi.org/10.1007/978-3-319-25512-5_3

[92] Subramanyam A.V. and Emmanuel S., "Video forgery detection using HOG features and compression properties," in *Proc. IEEE 14th Int. Workshop Multimed. Signal Process.*, 2012, pp. 89-94.

[93] Smith R. and Blinn J.F., "Blue screen matting," in Proc. *Int. conf. Comput. Graphics Interactive Techniq.*, pp. 259–268, 1996.

[94] Su L. and Li C., "A novel passive forgery detection algorithm for video region duplication," *Multidim.. Syst. Signal Process.*, vol. 29, pp. 1173–1190, 2018.

[95] Saddique M., Asghar K., Bajwa, U.I. Hussain M. and Habib Z., "Spatial Video Forgery Detection and Localization using Texture Analysis of Consecutive Frames.," *Adv. Elect. Comput. Engg.*, vol. 19, no. 3, pp. 97-108, 2019.

[96] Shelke N.A. and Kasana S.S., "Multiple forgery detection and localization technique for digital video using PCT and NBAP," *Multimed. Tools Appl.*, 2021, https://doi.org/10.1007/s11042-021-10989-8

[97] Su Y., Zhang J., and Liu J., "Exposing Digital Video Forgery by Detecting Motion-compensated Edge Artifact," in *proc. IEEE Int. Conf. Comput. Intell. & Soft. Engg.*, 2009.

[98] Su Y., Nie W., and Zhang C., "A frame tampering detection algorithm for MPEG videos," in Proc. *6th IEEE Joint Int. Inf. Tech. Artif. Intell. Conf.*, 2011, pp. 461–464.

[99] Stamm M.C., Lin W.S., and Liu K.J.R., "Temporal Forensics and Anti-Forensics for Motion Compensated Video," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1315-1329, 2012.

[100] Su L., Huang T. and Yang J., "A video forgery detection algorithm based on compressive sensing," *Multimed. Tools Appl.*, vol. 74, no. 17, pp. 6641–6656, 2015.

[101] Singh G., and Singh K., "Video Frame and Region Duplication Forgery Detection Based on Correlation Coefficient and Coefficient of Variation," *Multimed. Tools Appl.*, vol. 78, pp. 11527–11562, 2019. DOI: 10.1007/s11042-018-6585-1

[102] Singh V.K., and Tripathi R.C., "Fast and efficient region duplication detection in digital images using sub-blocking method," *Int. J. Adv. Sci. Tech.*, vol. 35, pp. 93–102, 2011.

[103] Teerakanok S. and Uehara T., "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," *IEEE Access*, vol. 7, pp. 40550–40568, 2019.

[104] Thakur A. and Jindal N., "Video Forgery Detection Using Deep Convolution Neural Network," *J. Critical Reviews*, vol. 7, no. 9, pp. 751–759, 2020.

[105] Tan H.L., Li Z., Tan Y.H., Rahardja S., and Yeo C., "A perceptually relevant MSE-based image quality metric," *IEEE Trans. Image Process.*, vol. 22, no. 11, pp. 4447-4459, 2013.

[106] Ulutas G., Ustubioglu B., Ulutas M. and Nabiyev V., "Frame duplication/mirroring detection method with binary features," *IET Image Process.*, vol. 11, no. 5, pp. 333–342, 2017.

[107] Uliyan D.M and Al-Husainy M.A.F., "Detection of Scaled Region Duplication Image Forgery using Color based Segmentation with LSB Signature," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 126–132, 2017.

[108] Ulutas G., Ustubioglu B. and Ulutas M., "Frame duplication detection based on BoW model," *Multimed. Syst.*, vol. 24, pp. 549–567, 2019.

[109] Vahora S., Chauhan N., and Prajapati N., "A Robust Method for Moving Object Detection Using Modified Statistical Mean Method," *Int. J. Adv. Info. Tech.* vol. 2, no. 1, 65–73, 2012.

[110] Vijayarani S. and Vinupriya M., "Performance Analysis of Canny and Sobel Edge Detection Algorithms in Image Mining," *Int. J. Innovative Res. Comput. Commun. Engg.*, vol. 1, no. 8, pp. 1760–1767, 2013.

[111] Wu Y., Jiang X., Sun T., and W. Wang, "Exposing video inter frame forgery based on velocity field consistency," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process*., pp. 2674–2678, 2014.

[112] Wang W. and Farid H., "Exposing digital forgeries in video by detecting duplication," in *Proc. 9th Workshop Multimed. & Security*, 2007, pp. 35–42.

[113] Wang Q., Li Z., Zhang Z. and Ma, "Video Inter-frame Forgery Identification Based on Optical Flow Consistency," *Sensors & Transducers*, vol. 166, no. 3, pp. 229-234, 2014.

[114] Wei W., Fan X., Song H., "Video tamper detection based on multi-scale mutual information," *Multimed Tools Appl.*, vol. 78, pp. 27109–27126, 2019.

[115] Wang W., Farid H., "Exposing digital forgeries in video by detecting double quantization," in *Proc. 11th ACM Workshop Multimed. Security*, Princeton New Jersey USA 2009, pp. 39–48.

[116] Wang W., Jiang X., Wang S., Wan M., and Sun T., "Identifying video forgery process using optical flow," in: Shi Y, Kim HJ, Pérez-González F (eds.) Digital-Forensics and Watermarking. Lecture Notes in Comput. Sci., *Springer*, Berlin, Heidelberg, vol. 8389, pp. 244–257, 2014.

[117] Xiong J., Yu D., Wang Q., Shu L., Cen J., Liang Q., Chen H., and Sun B., "Application of Histogram Equalization for Image Enhancement in Corrosion Areas", *Shock Vibration*, 2021, https://doi.org/10.1155/2021/8883571

[118] Xu J, Yu Y., Su Y., Dong B., and You X., "Detection of Blue Screen Special Effects in Videos," *Phys. Procedia*, vol. 33, pp. 1316 -1322, 2012.

[119] Yu L., Wang H., Han Q., Niu X., Yiu S.M., Fang J. and Wang Z., "Exposing frame deletion by detecting abrupt changes in video streams," *Neurocomput*., vol. 205, pp. 84-89, 2016.

[120] Yang J., Huang T. and Su L., "Using similarity analysis to detect frame duplication forgery in videos," *Multimed. Tools Appl*. Vol. 75, pp. 1793–1811, 2016.

[121] Yao H., Song S., Qin C., Tang Z., and Liu X., "Detection of Double-Compressed H.264/VC Video Incorporating the Features of the String of Data Bits and Skip Macroblocks," *Symmetry*, vol. 9, no. 12: 313, 2017, doi:10.3390/sym9120313.

[122] Yao Y., Shi Y., Weng S., and Guan B., "Deep Learning for Detection of Object-Based Forgery in Advanced Video", Symmetry, vol. 10, no. 3, 2018, doi:10.3390/sym10010003

[123] Yang B., Sun X., Guo H., Xia Z. and Chen X., "A copy-move forgery detection method based on CMFD-SIFT," *Multimed. Tools Appl*., vol. 77, pp. 837–855, 2018.

[124] Yedidia A. (2016) Against the F-score. https://adamyedidia.files.wordpress.com/2014/11/f_score.pdf

[125] Zhang D., Wang X., Zhang M., and Hu J., "Image splicing localization using noise distribution characteristic," *Multimed. Tools Appl.*, vol. 78, pp. 22223–22247, 2019.

[126] Zhang Z., Hou J., Ma Q. and Li Z., "Efficient video frame insertion and deletion detection based on inconsistency of correlations between local binary pattern coded frames," *Security Commun. Networks*, vol. 8, pp. 311–320, 2015.

[127] Zhang J., Feng Z., and Su Y., "A new approach for detecting copy-move forgery in digital images," in *Proc. IEEE Int. Conf. on Comm. Syst*., China, pp. 362–366, 2008.

[128] Zheng L., Sun T. and Shi Y.Q., "Inter-frame Video Forgery Detection Based on Block-Wise Brightness Variance Descriptor," in: Shi YQ., Kim H., Pérez-González F., Yang CN. (eds.) Digital-Forensics and Watermarking. IWDW 2014. Lecture Notes in Comput. Sci., vol. 9023. *Springer*, Cham. https://doi.org/10.1007/978-3-319-19321-2_2

[129] Zhang Z.Z., Hou J.J., Li Z.H. and Li D.D., "Inter-frame forgery detection for static-background video based on MVP consistency," Lecture Notes Comput. Sci., vol. 9569, pp. 94–106, 2016.

[130] Zhao D.N., Wang R.K. and Lu Z.M., "Inter-frame passive-blind forgery detection for video shot based on similarity analysis," *Multimed. Tools Appl*., vol. 77, pp. 25389–25408, 2018.