PASSIVE VIDEO FORGERY DETECTION USING FRAME CORRELATION STATISTICAL FEATURES

AMINU MUSTAPHA BAGIWA

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2017

PASSIVE VIDEO FORGERY DETECTION USING FRAME CORRELATION STATISTICAL FEATURES

AMINU MUSTAPHA BAGIWA

THESIS SUBMITTED IN FULFILMENTOF THE REQUIREMENTSFOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2017

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: Aminu Mustapha Bagiwa

Registration/Matric No: WHA130056

Name of Degree: PhD Computer Science (Digital Forensic)

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):**PASSIVE VIDEO FORGERY DETECTION USING FRAME CORRELATION STATISTICAL FEATURES**

Field of Study: Computer Science (Digital Forensic)

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University ofMalaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:

Subscribed and solemnly declared before,

Witness's Signature Date:

Name:

Designation:

ABSTRACT

The use of digital videos in criminal investigation and civil litigation has become popular, this is due to the advancement of embedded cameras in handheld devices such as mobile phones, PDA's and tablets. However, the content of digital videos can be extracted, enhanced and modified using inexpensive and user friendly video editing software, such as; Adobe Photoshop, Sefexa, etc. Thus, the influx of these video editing softwarelead to the creation of serious problems that are associated with the authenticity of digital videos by making their validity questionable. In order to address these problems, two approaches for the authentication of digital videos were proposed by digital forensic researchers. The approaches are either active or passive. Active approaches are the earliest form of video authentication techniques; an active approach is based on digital watermark technology that is used for video authentication and ownership verification. A digital watermark is a hidden digital marker embedded in a noise tolerant video signal. However, the problem with the active approach to video authentication is that it can only be applied in limited situations and it requires the use of a special hardware. Moreover, an authorized person responsible for the watermark insertion can tamper with the video before inserting the digital watermark. Furthermore, techniques for encryption can be used to prevent an unauthorized person from tampering with the content of the video, however, these encryption techniques donot prevent the file owner from tampering with his own video. This limits the ability of digital watermark to ensure authenticity in digital videos. In response to these limitations, passive approaches were introduced. Passive approaches rely on the behaviour of features embedded in a video for forgery detection purposes. Thus, the aim of this doctoral study as a contribution to the field of digital forensic is to develop techniques based on selected video features that can be used to detect tampering of a

digital video. In this study, passive forensic techniques are proposed to detect (1) Digital video inpainting forgery, and (2) Chroma key forgery in digital videos. Each of these techniques focus on the specific features that can be used to detect that kind of forgery. Firstly, a technique for the detection of video inpainting forgery is proposed using the statistical correlation of hessian matrix features extracted from the suspected video. Secondly, another technique is proposed for the detection of chroma key forgery in a digital video using the statistical correlation of blurring features extracted from the suspected video. Results from these experiments conducted have proven that hessian matrix features can effectively be used to detect video inpainting forgery with 99.79% accuracy whilst the blurring feature can effectively detect chroma key forgery in digital videos with 99.12% accuracy.

ABSTRAK

Penggunaan video digital dalam penyiasatan jenayah dan tindakan undang-undang sivil telah menjadi popular dengan kemajuan kamera tertanam dalam peranti bimbit seperti telefon bimbit, PDA dan tablet.Walaubagaimanapun, kandungan video digital boleh diekstrak, dipertingkatkan dan diubahsuai menggunakan perisian berpatutan dan pengguna video penyuntingan mesra perisian seperti Adobe Photoshop, Sefexa, dan lain-lain. Dengan kemasukan perisian penyuntingan video ini ia telah mencetus kepada masalah yang lebih serius yang berkaitan dengan kesahihan video digital dengan kesahihan. Bagi menangani masalah ini, dua cadangan telah dikemukakan iaitu pendekatan bagi pengesahan video digital oleh penyelidik forensik digital.Pendekatan ini merupakan pendekatan aktif dan pasif.Teknik pengesahan video merupakan pendekatan aktif bentuk yang paling awal.Pendekatan aktif adalah berasaskan kepada teknologi digital watermark yang digunakan untuk pengesahan video dan pengesahan hak pemilikan.Digital watermark merupakan penanda digital tersembunyi yang dibenam dalam isyarat video bunyi toleran.Walaubagaimanapun, masalah dengan pendekatan aktif bagi pengesahan video adalah hakikat bahawa mereka hanya boleh digunakan dalam keadaan terhad dan memerlukan penggunaan perkakasan khas sahaja. Selain itu, orang yang bertanggungjawab menyelitkan watermark boleh mengganggu video sebelum memasukkan digital watermark. Tambahan pula, teknik untuk penyulitan boleh digunakan untuk mencegah pengguna yang diberi kuasa daripada gangguan kandungan video itu, Selain itu, teknik-teknik penyulitan tidak menghalang pemilik fail daripada gangguan dengan video itu sendiri.Ini menghadkan keupayaan digital watermark dalam memastikan kesahihan video digital.Sebagai tindak balas kepada batasan ini, pendekatan pasif telah diperkenalkan.Pendekatan pasif bergantung kepada tingkah laku ciri-ciri yang terbenam dalam video bagi tujuan pengesanan pemalsuan.Oleh itu, tujuan kajian kedoktoran ini merupakan sumbangan

kepada bidang forensik digital.Tujuannya adalah untuk membangunkan teknik berasaskan kepada ciri-ciri video terpilih yang boleh digunakan untuk mengesan gangguan dalam video digital.Dalam kajian ini, kami mencadangkan teknik forensik pasif untuk mengesan (1) Video Digital pemalsuan, dan (2) Kunci Chroma pemalsuan utama dalam video digital.Salah satu daripada teknik ini memberi tumpuan kepada ciri-ciri tertentu yang boleh digunakan untuk mengesan jenis pemalsuan.Teknik pertama meruapakan teknik mengesan video pemalsuan dengan menggunakan korelasi statistik ciri "matriks hessian" yang diekstrak dari video yang dikhuatiri.Teknik kedua, kami mencadangkan teknik mengesan kunci Chroma pemalsuan menggunakan korelasi statistik kabur bersama ciri yang diekstrak dari video yang dikhuatiri.Keputusan daripada percubaan yang dijalankan telah membuktikan bahawa ciri "matriks hessian" boleh berkesan untuk digunakan bagi mengesan video pemalsuan.Manakala ciri yang kabur pula sesuai digunakan bagi mengesan kroma pemalsuan utama dalam video digital.

ACKNOWLEDGEMENTS

I would like to extend my thanks and immense gratitude to Allah for spearing my life with good health to witness the successful completion of my PhD study. I would also like to extend many thanks to my supervisors Dr. Ainuddin Wahid Abdul Wahab and Dr. Yamani Idna Idris, whom despite their busy schedule spent time to help me through the completion of this research study. Your advice and guidance have been of enamors importance to the success of this three year journey.

Furthermore, my sincere gratitude goes to my parent Alhaji Aminu Idris Bagiwa and Hajiya Hadiza Aminu Bagiwa whom have sacrifice their time, efforts and resources to train me both physically, mentally and intellectually to become a person of importance and value to the society.

My gratitude also goes to my darling wife Halima Kabir and son Al Amin Mustapha Bagiwa for their patience throughout my studies. Thank you for your inspiration and goodwill.

A special acknowledgement also goes to the Tertiary Education Trust Fund (TETFund), Ahmadu Bello University, Zaria-Nigeria for the financial support towards the success of this PhD study.

Finally, my gratitude also goes to my co-researchers for their help and contributions to the success of this research.

This project is dedicated to my father Alhaji Aminu Idris Bagiwa, my mother Hajiya Hadiza Aminu Bagiwa, and the family of Mustapha Aminu Bagiwa.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

3D	:	3 dimension
ADQMBs	:	Analysis of double quantization macro blocks
CSI Cyber	:	Crime Scene Investigation cyber
EPZS	:	Enhance predictive zonal search
FBI	:	Federal Bureau of Investigation
FN	:	False negative
FP	:	False positive
FPR	:	False positive rate
GMM	:	Gaussian mixture model
GOP	:	Group of picture
GSA	:	Ghost shadow artifacts
JPEG	:	Joint photographic expert group
LESH	:	Local Energy based Shape Histogram
LTI	:	Luminance transition improvement
MPEG	:	Moving picture expert group
NSCT	:	Non sample contourlet
PDA’s	:	Personal digital assistants
PDAs	:	Personal digital assistants
PKIDEV	:	Public key infrastructure based digital evidence verification
RGB	:	Red, green and blue
SA-DWT	:	Shape adaptive –discrete wavelet transform
SCHM	:	Statistical correlation of hessian matrix
SCQDT	:	Statistical correlation of quantized discrete cosine transform

STCA	:	Spatio temporal slicing and coherence analysis
SULFA	:	Surrey university for forensic analysis
SVM	:	Support vector machine
TN	:	True negative
TP	:	True positive
TPR	:	True positive rate
VLC	:	Variable length codeword

CHAPTER 1 : INTRODUCTION

In this chapter, an introduction is presented to digital video forgery, digital video forgery detection and the motivation behind this research work. Next, problem statement, research questions, objectives and scope are defined. Also presented is a brief description of the contributions and significance of this research work. Finally, the outline of this thesis is described.

1.1 Introduction

In the digital age of the 21st century, devices such as mobile phones, personal digital assistants (PDA's) and digital camcorders are granting almost everyone with easy access to acquire and save digital video.Moreover, the acquired digital video can easily be redistributed using the inexpensive internet connection for various purposes such as; video conferencing, information dissemination in media houses, surveillance system, traffic lights, hospitals etc. Likewise, the quality of the digital videos can be upgraded and their content extricated by the utilization of various video editing software.However, the influx of the affordable and user friendly video editing software has made it possible for irresponsible digital attackers to alter the content of a digital video for malicious purposes, making the authenticity and validity of the digital video extremely difficult to identify using the naked eye. This is because an altered digital video leaves minimal clues of tampering and can elude human detection. An example of a tampered video is shown in Figure 1.1 created in 2003 that shows a British soldier in Iraq trying to control a crowd of civilians in an organized and peaceful manner, however, this moment never existed, rather it is a combination of two different videos as mentioned in (BROAD, 2009). Figure 1.1a depicts a video of a soldier at a particular moment and Figure 1.1b is another video of the same soldier but in a different context.

In order to conceal the gunpoint used by the soldier, a photomontage of Figure 1.1a and 1.1b was done to create a forged video as shown in Figure 1.1c.

A **B** **C**

Figure 1.1: Montage (2003) of a British Soldier Trying to Control a Crowd of Civilians in Iraq[1]

Cases of illegal video alteration are recently being identified and reported in many areas, such as, scientific publications, politics, social media, security, criminal investigations and civil litigation as discussed in (Fridrich, Soukal, & Lukáš, 2003; Gopi et al., 2006).All these areas are now demanding ways to authenticate and validate digital videos as mentioned in (Grigoras, 2009). The demand to authenticate a digital video helpsto minimize the rate of false information dissemination, avoid wrong convictions in court and reduce acts of terrorism as discussed by (Chuang, Su, & Wu, 2011; Rocha et al., 2011).

There are different types of forgeries that can be performed on a digital video. The most common forgery attacks include; copy move forgery, duplication forgery, object removal forgery using inpainting and video composition forgery using the chroma key technology.

In this study, the focus is on video inpainting and chroma key forgery detection respectively.This is because video inpainting and chroma key forgeries are more difficult to detect than other types of forgery attacks. Perhaps, because all the components used for the forgery purpose originated from a genuine video. Furthermore,

[1]http://www.famouspictures.org/altered-images/

features that were previously proposed for video inpainting detection such as the noise features take a reasonable time to extract from a digital video and do not address temporal domain. The use of ghost shadow artifacts has also been proposed for video inpainting forgery detection, but this feature was found to be susceptible to compression as such cannot be applied to non compressed videos. The technique proposed for chroma key forgery was based on different encoding of the two source videos, however, the technique fails when the two videos used for the chroma key forgery have the same encoding.

Thus, if any of these forgery videos are used as evidence incriminal investigations and civil litigations, it will misdirect theviewer'sperception. Therefore, it is important to propose better and effective featuresto identify videos associated with inpainting and chroma key forgery respectively.

1.2 Problem Statement

Video forgery affects digital video contents in a persuasive manner.In order to detect video forgery, one may think of extending the existing image forgery detection algorithms to each frame in a video sequence. However, some kinds of forgeries are undetectable using that approach because of the relative relationship that exists between frames in the video. For example, video inpainting and chroma key forgery span across frames and within different frame regions. In this case, existing image forgery detection algorithms may not be feasible to detect these kinds of forgeries, as each frame is analysed independently. Also, the origin of the pixels used for filling the region of object removal in the case of inpainting forgery may come from different frames of the video. Thus, the region of object removal may be filled using multiple pixels originating from different regions in the video. Subsequently, video inpainting and chroma key forgery poses a great research problem.

Existing passive techniques used to detect video forgery focus on the use and analysis of different features extracted from a video. Examples of these features include; readout noise, independent noise characteristics, ghost shadow artefacts, motion estimation features, temporal artifacts, blur artefacts andlocal energy based shape histogram (LESH) features.However, the detection performance of these features behaves differently with respect to the type of forgery detected. Compression also affects the robustness of these features for video forgery detection; some features are robust to compression whilst others are not.Furthermore, some features are robust to static objects whilst others are robust to moving objects. Based on literature, no feature has been proposed to detectvideo inpainting for static and moving object removal at the same time, or considers chroma key forgery detection for compressed and non-compressed videos.Furthermore, most of the features proposed in the literature for video inpainting forgery and chroma key forgery detection take a reasonable amount of time to extract and analyse during the detection process.This necessitates the need for a fast and reliable feature that can be used for video inpainting and chroma key forgery detection respectively.

1.3 Research Questions

This research study is set up to answer the following questions for video inpainting and chroma key forgery detections respectively:

1. Video Inpainting
    i. How does video inpainting forgery affect the behaviour of a genuine video?
    ii. What features in a video are likely to be affected by inpainting forgery?
    iii. Can the affected feature in the video be used in a technique to detect inpainting forgery?

iv. Can the new technique based on the selected feature improve the detection accuracy for digital video inpainting forgery by increasing the detection precision and reducing the false positive detection results?

2. Chroma key

i. How does chroma keying affect the behaviour of a genuine video?

ii. What features in a video are likely to be affected by chroma key forgery?

iii. Can the affected feature in the video be used in a technique to detect chroma key forgery?

iv. Can the new technique, based on the selected feature, improve the detection accuracy for chroma key forgery in digital videos, by increasing the true positive detection result and reducing the false positive detection results?

1.4 Research Objective

In this study, two main research objectives are addressed which include:

1. To detect inpainting forgery in digital videos using the statistical correlation of Hessian matrix features. The sub objectives under this main objective include:
   a. To investigate the effect of inpainting forgery on the Hessian matrix features in a digital video.
   b. To develop and implement a technique for detecting video inpainting forgery in digital videos using the analysis of Hessian matrix features.
   c. To evaluate the performance of the technique against other inpainting detection techniques from the literature.
2. To detect chroma key forgery in digital videos using the statistical correlation of blurring features. The sub objectives under this main objective include:
   a. To investigate the effect of chroma key forgery on the blurring features in a digital video.

b. To develop and implement a technique for detecting chroma key forgery in a digital video using the analysis of blurring features.
c. To evaluate the performance of the technique against other chroma key forgery detection techniques from the literature.

1.5 Thesis Contribution

This research study proposed efficient features in a technique to detect and localize inpainting and chroma key forgery in a digital video. Below lists the contributions to the domain of digital forensics:

1. The conducted literature exposes the limitations of the existing techniques for video inpainting and chroma key forgery detection respectively.
2. A new technique is implemented using a novel proposed Hessian matrix feature for the detection of video inpainting forgery in digital videos.
3. A new technique is implemented using a novel proposed blurring feature for the detection of chroma key forgery in digital videos.
4. Finally, future research directions in the domain of digital video forensic are provided.

1.6 Significance of Research

This research provides robust features that are implemented in a technique for the detection of video inpainting and chroma key forgery respectively.The output of this research will benefit the societies whom conduct research in the area of digital video forgery detection. The current issues associated with video inpainting and chroma key forgery detection is highlighted in detail in the literature review section. Furthermore, this research will also help digital investigators, forensic experts and other relevant cyber authorities determine the authenticity of a digital video very quickly, without relying on reviewing the video processing history.

1.7 Thesis Organization

This thesis is segmented into six chapters. Chapter 2 reviews the related work of digital video inpainting and chroma key forgery. Chapter 3 provides a general discussion of the research methodology that is employed in carrying out the research study. A proposed solution to video inpainting forgery detection is discussed in Chapter 4. Chapter 5 discusses a solution to chroma key forgery detection in digital videos. Finally, Chapter 6 summarizes and concludes the research findings.

1.8 Chapter Summary

In this chapter, the motivation behind this research work is discussed. The problem this research intends to address is already clearly defined. Research questions, objectives and scope were also outlined previously. The next chapter discusses an overview of digital video inpainting and chroma key forgeries and the associated detection techniques proposed in the literature which highlights the strength and weakness of each technique.

CHAPTER 2 : LITERATURE REVIEW

In this chapter, historical knowledge of digital forensic research domain is discussed to effectively understand the remaining chapters of this thesis. The backgroundof digital forensics is introduced, including its different classification, importance and operation scenario. Similarly, digital inpainting and chroma key forgery is discussed. First, concepts of digital inpainting and various digital video inpainting forgery detection algorithms were identified from the existing literature. The detection algorithms identified for digital video inpainting forgery detection are reviewed for their detection ability and limitations. Secondly, the concept of chroma keying for video composition forgery is discussed in detail. The detection algorithms identified for video composition using chroma key are also reviewed for their detection ability and limitations.

2.1 Forensic Background

The word forensic has its origin from the Latin word (forensis), meaning debate or public discussion. However, recently the word forensic is widely applied in the context of the courts and the judicial system. Using the word forensic with science, described the topic; forensic science, which is the application of scientific methods and processes to aid solving crimes. The concept of forensics started as far back from Archimedes in 287BC (Aaboe & Aaboe, 1964). Archimedes, during his time, examined water displacement using a combination of density and buoyancy tests to measure the gold content of a crown and determined the crown maker, this was embezzling. Later in the year 1822, Francis Galton established the first intrinsic fingerprint classification system, by identifying common patterns in fingerprints, which led to the birth of forensic science in general. The use of intrinsic fingerprints invented by Francis Galton has now formed the basis of forensic investigations in different areas and applications. Examplesof these areas include; forensic pathology, medical forensics, trace evidence

analysis, forensic archaeology, forensic anthropology, criminalistics, and digital forensics amongst others.

In this research, the focus is on digital forensics involving the use of scientific methods and processes to validate the authenticity of digital evidence.

2.2 Digital Forensic

Digital forensics is a category of forensic science concerned with the systematic recovery, verification, authentication, and investigation of a digital data, mostly in relation to a crime as defined in (van Houten et al., 2010). Digital evidence is an electronic digital document that portrays the truth of an event or issue. However, the weight of that evidence needs to be carefully examined and verified using viable legal arguments in order to be admissible in a court of law. This is where digital forensics came into play. Digital forensics is mainly divided into stages namely digital evidence recovery, verification and authentication as shown in Figure 2.1.

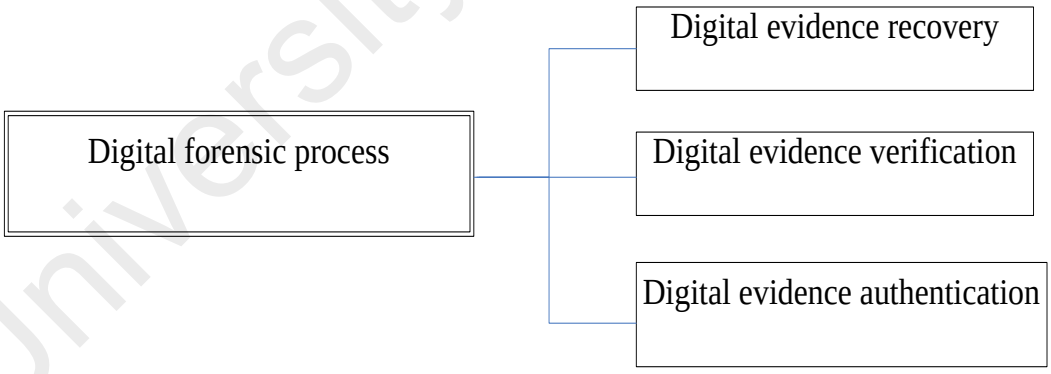

Figure 2.1: Digital Forensic Processes

2.2.1 Digital Evidence Recovery

Digital evidence recovery involves the ability to create a forensic twin or copy of the digital content. This is to forbid an unintended modification or loss of the original digital document during analysis.In variety of court cases, digital evidence used during

forensic investigation procedures are kept in a secured place as digital files for safe keeping (Casey, 2011; Pilant, 1999; Silberschatz, Galvin, & Gagne, 2013).

2.2.2 Digital Evidence Verification

The use of digital evidence during legal court proceedings is now rampant (Boddington, Hobbs, & Mann, 2008). However, the modality to verify the digital evidence and its admissibility is a problem that needs to be addressed especially when dealing with the change of custody. Hence, in order to address the problem of digital evidence verification, forensic experts' use the hashing technique and Public Key Infrastructure based Digital Evidence Verification Model (PKIDEV) (Uzunay, Incebacak, & Bicakci, 2007)to verify the content of a digital evidence during the change of custody.

2.2.3 Digital Evidence Authentication

In another definition, digital evidence in a court case is referred to as; any legitimate information in the form of a digital recording, transmission or storage of information that may be presented and used during a trial to relate suspects to a crime that has been committed (Adams, 2012). However, prior to the acceptance of any digital evidence, the relevancy of the digital evidence often needs to be examined for its authenticity (Ryan & Shpantzer, 2002). Therefore, the domain of digital forensics over the years has been busy in the development of techniques and models for the authentication of any form of digital evidence. This thesis' contribution in this area is not an exception, since a method that can validate and authenticate a digital video is proposed.

2.3 Branches of Digital Forensics

Digital forensics is divided into many sub branches as shown in Figure 2.2. A brief explanation of the branches of digital forensic is now discussed.

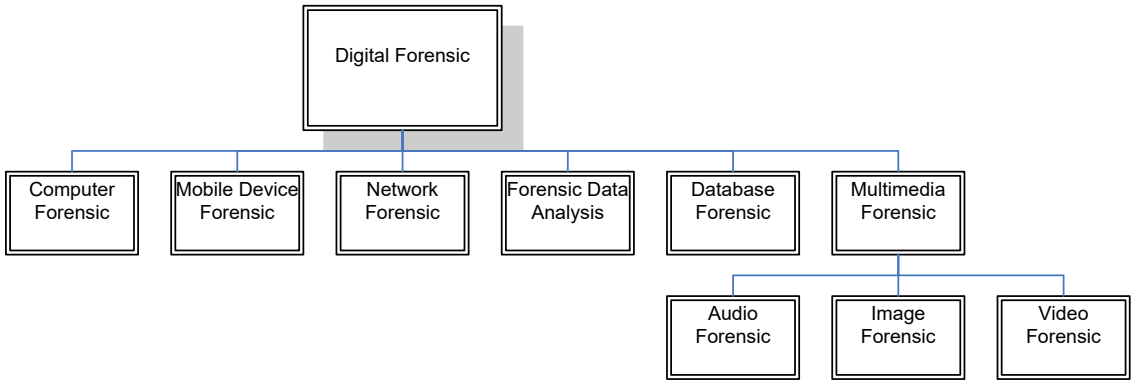

Figure 2.2: Branches of Digital Forensic

2.3.1 Computer Forensics

Computer forensics is a sub branch in the domain of digital forensics that is concerned with obtaining, preserving, and documenting evidence from a computer storage medium. The objective of computer forensics is to discover evidence of digital attacks or tampering in a computer system, digital storage medium or electronically saved digital document (Yasinsac et al., 2003).

2.3.2 Mobile Device Forensics

Mobile device forensics is another sub branch in digital forensics that is concerned with the systematic reclaiming of data from mobile phone. Forensics of mobile devices is different from forensics in computers because of its inbuilt communication system. The objective of mobile device forensics is on digital data sets such as phone logs, call records, text messages, audio, images, and videos (Adams, 2012).

2.3.3 Network Forensics

Network forensics is another sub branch of digital forensics that is concerned with the systematic analysis, detection and monitoring of computer network traffic in both local area networks, wireless area network, and the internet (Khan et al., 2014b). The objective of network forensic is information gathering, as digital evidence for review in a court of law, digital evidence collection and analysis, or network intruder

detection (Palmer, 2001). Network forensic differs from other forensic sub branches because network data can be fragile and difficult to analyse without an expert. (Khan et al., 2014a).

2.3.4 Forensic Data analysis

Forensic analysis of data stored in a digital format is another sub category of digital forensic. Forensic data analysis is concerned with the analysis of structured data. The objective is to discover traces of illegal activities involving financial crimes.

2.3.5 Database Forensics

This is a sub branch of digital forensic that is concerned with the forensic analysis of databases, data models and their schema (Olivier, 2009). The main objective is to analyse the contents of the database, user activity logs, and storage data to identify an attack timeline or recover relevant information.

2.3.6 Multimedia Forensics

This is a branch of digital forensics that is concerned with the analysis of digital media assets such as audios, images, and videos. This is to give an assessment on the digital content in terms of verification, authentication or the extraction of useful information to address, link or support an investigation of a crime.

This research is focused on the verification of digital video in multimedia forensics, because of its widespread useas digital evidence (Rocha et al., 2011). The aim of this research study is to evaluate the authenticity of suspect videos whereby inpainting or chroma key forgery has been applied, by distinguishing features from the video, based on the kind of forgery performed.

Digital forgery with an attempt to falsely create a digital scenario that has not happened or existed started with the beginning of digital images (Fridrich et al., 2003;

Gopi et al., 2006). Furthermore, the attempt to detect forgeries in digital media contents also started with digital images with the first clue of forgery found on a digital image after the creation of the first digital photograph in 1814 by Nic´ephoreNiepce (Coe, 1977). Figure 2.3 shows one of the earliest example of digital image forgery which is created by Oscar G. Rejland in 1857. It is a Photomontage, consisting of 32 separate photographs.

Figure 2.3: Early Example of Analog Forgeries

However, because of the recent advancements in the production of powerful cameras and digital editing software,there have been great improvements in image and video forgery with hundreds of images and videos forged on daily basis. Therefore,in order to verify the authenticity of digital video content, the area of digital video forensics was born. So far it has witnessed a great deal of research over the years (Poisel & Tjoa, 2011) with many articles proposing different kinds of video forgery detection techniques. Thus, in the next section, the techniques for the detection of digital inpainting and chroma key forgery respectively are discussed.

2.4 Overview of Digital Video

A digital video is an electronic recording that is based on a digital signal rather than an analogue signal. It is used to generate a sequence of images that can be understood by humans and can easily be analysed using computer algorithms. The major areas of digital video application include; the creation of movies, reporting news events, surveillance systems and admissible court evidence.

However, in order to provide a digital video with high quality and appreciable graphics, the movie industries and media houses are demanding powerful and robust video editing software. Therefore, in order to meet with the demand for better and high quality videos, society is now witnessing an explosion in the number of both freely and commercially available video editing software. Thus, with the explosion of these video editing software products, digital video manipulation can easily be performed using different types of forgery techniques onto a digital video. Examples of suchforgeries include; the use of digital inpainting mechanisms to remove an object from a video, or chroma key technologies that can be used to compose two different videos into a single video.

Right now many video inpainting and chroma key forgery related cases have been uncovered, and as such people question the trustworthiness and the authenticity of digital video. Digital video inpainting allow the restoration of missing or deteriorated parts of a video or the removal of unwanted objects from the video in order to minimize distraction when the video is played (Bertalmio et al., 2000). Thus, since inpainting provides the ability to remove objects from a video with some ideal and quality degradation, it can as well be used to alter the semantic content of a digital video. Varieties of digital video inpainting detector techniques have been proposed in the literature. However, these previous techniques depends on the filling scheme of the inpainting technique to detect blocks whose difference is very minimal or non existence between suspicious and non suspicious areas. This relatively indicates that existing video inpainting techniques are inpainting scheme dependant. Moreover, compression also affects the robustness of the previous inpainting detection techniques. This is because compression affects the selected features statistics that were used in the detection techniques.

On the other hand, little importance has been given to chroma key forgery detection as such making it an understudied topic. Chroma key forgery is a technique that allows two videos from different sources to be composed into one video based on color hues. The chroma key technique is sometimes called green screen, blue screen or color separation overlays. It is very useful in media industry and cinemas in order to cut cost during a media show or movie production. Since chroma key provides the ability to mate two videos together as one video with some ideal and quality degradation, it can as well be used to alter the semantic content of a digital video by superimposing one video into another. The only technique that was directly proposed for chroma key forgery detection relies on the difference between the encoding of a video foreground and background. However, the accuracy of this technique fails when the two videos used for the matting process are not compressed or have the same encoding. Time is also important during forensic analysis, as such there is still the need for fast and reliable features for the detection of video inpainting and chroma key respectively.

Therefore, it is critical for scientists to think of strategies for authenticating and validating digital videos. The focus of this research study is on the detection of video inpainting forgery and chroma key forgery respectively.

2.5 Background of Digital Inpainting

Digital inpainting is as old as digital image photography. It is a concept that is used for digital content restorationwhich exploits neighbouring pixel information in a digital image or video to restore some of its damaged parts (Cole, 1991).

Digital inpainting is mainly used in cinemas, digital image photography and digital forgery. In cinemas, digital inpainting is used for scene reconstruction or restorations, logo removal in movies, replacement of deleted blocks as a result of coding or transmission of videos (Shen & Chan, 2002). However, in a forgery process, digital

inpainting is used for red eye removal, time stamp removal or an entire object removal in both images and videos (Criminisi, Perez, & Toyama, 2003).

Variety of algorithms for the achievement of digital inpainting has been proposed in the literature. However, these algorithms are mainly categorized into one of five categories namely:

1. Texture based inpainting
2. Structure based inpainting
3. Hybrid based inpainting
4. Exemplar based inpainting
5. Automatic based inpainting

2.5.1 Texture Based Inpainting

Texture based inpainting is the early approach used for filling broad regions in a video using texture information from neighbouring pixels. Initially, inpainting algorithms based on texture synthesis are used for guessing damaged region parameter models that are used as an input for the texture synthesis process (Heeger & Bergen, 1995). Example of such algorithms can be seen in the work of (Efros & Leung, 1999) whose inpainting algorithm uses the sampling of texture patterns for inpainting. As time goes on, texture synthesis processes were further used for filling in small hole regions in a video frame which were damaged due to deterioration, or the director needed some objects removed from a video in order to minimize distraction when the video is played.

Inpainting algorithms based on texture synthesis performs well when dealing with simple motion types in a video. However, these algorithms are found to behave poorly when dealing with structural information and complex motion types in a video for object removal. This necessitated the need for an improved inpainting approach to effectively deal with structural regions in videos.

2.5.2 Structure Based Inpainting

In order to address the limitation of structural region filling that is associated with texture inpainting, a structure based inpainting technique was proposed that can be used for filling an inpainted region in an image or video. The structural inpainting algorithm utilizes the concept of geometry for filling missing information in the region that is to be inpainted. Structural inpainting algorithms have recorded a great success in variety of applications such as editing images during image retouching, object removal from images and video for privacy protection (Arai et al., 2010). The aim of structural inpainting algorithms is to reproduce video frame isophotes which include lines having the same intensity reaching the inpainting region boundary in a smooth fashion while maintaining an exact intensity arrival angle.

2.5.3 Hybrid Based Inpainting

Hybrid based inpainting algorithms are a combination of texture and structural based inpainting. The rationale behind hybrid inpainting algorithms' is that it divides the regions of inpaint into two individual parts, texture region and structure region. The decomposed parts are filled by a combination of structural edge propagation techniques and texture based techniques. Hybrid inpainting algorithms have the advantage of large area completion. Furthermore, to achieve a desired inpainting result, structural completion accompanied with texture inpainting has greatly influenced the ability to remove objects from a scene in a digital video with less effects to the edges of the inpainted region (Muthukumar, 2010).

2.5.4 Exemplar Based Inpainting

Exemplar based inpainting is another class of inpainting algorithms. It defines an easy and efficient algorithm for inpainting large target areas. Exemplar based inpainting algorithms are normally classified into two stages involving priority assignment and

best matching spot selection. Inpainting in exemplar based algorithms is done by selecting the matching spot that is best based on certain metrics and then inserting it into target inpainting spots in the damaged areas. The same technique is used to fill structures in the missing regions in which an object is removed from a video using spatial information of neighbouring regions (S Mahajan & Vaidya, 2012).

2.5.5 Automatic Based Inpainting

In automatic inpainting algorithms, a user assists the system by providing structural guidelines for completing the region of inpaint. A general procedure for automatic inpaint was proposed in (Xu & Sun, 2010) using structural reproduction. The procedure involves the user providing information pertaining to the missing gaps using a regional sketch surrounding the inpaint region boundaries, a texture based inpaint method is then used to fill in the missing portions. The major disadvantage of automatic inpaint for object removal is time, due to its complexity for successful completion, which mainly depends on the size and the area of occupancy of the object being removed.

2.6 Digital Video Inpainting Forgery

The application of inpainting algorithms for video restoration and object removal is referred to as digital video inpainting. Digital video inpainting has a significant prospect in the digital world. It has been a great achievement in multimedia signal processing (Bornard et al., 2002) with several tools and algorithms implemented for video inpainting. Although, the use of inpainting is an achievement in the digital world, it is however not such good news to the forensic community as it has resulted in the creation and distribution of a greater quantity of forgeries-into the world of digital videos.An example is shown in Figure 2.4, whereby the flying man has been removed from Figure 2.4a and the region automatically completed using some portion of the image in Figure 2.4b.

A **B**

Figure 2.4: Example of an Inpainted Frame in a Video

2.7 Chroma key Forgery

Chroma key (Foster, 2010) is a technology that is used to compose two different videos from the same or different sources to look like an original video based on colour hues. The purpose of chroma key composition is to super impose a non-existent object from one video to another in an attempt to make it look like a real video. The technology of chroma key composition allow its users to insert imaginary objects into a video or can be used to show the existence of certain objects that are not present in the original video (Xu et al., 2012). The composition process involves the matting of a video foreground element with a constant background colour as shown in Figure 2.5a. Thus, during the matting process, the foreground elements extracted from the uniform coloured background video are embedded on the desired background video as an imagination of reality as shown in Figure 2.5b.

A B

(a) Person on a constant green background colour[2]

(b) Result of green screen composition on to a new background

Figure 2.5: Example of Green Screen Composition

[2]http://www.shutterstock.com/home

Thus, when falsified videos resulting from either digital inpainting or chroma key composition forgery are presented as evidence during a court trial, or distributed over a social media, the videos can create serious problem such as convicting an innocent person, or tarnishing the social status of the victim associated with the video.

2.8 Techniques for Video Forgery Detection

The solutions to digital video authentication and validation in the domain of digital forensic for forgery detection are divided into two approaches, namely; active and passive, as shown in the taxonomy detailed in Figure 2.6

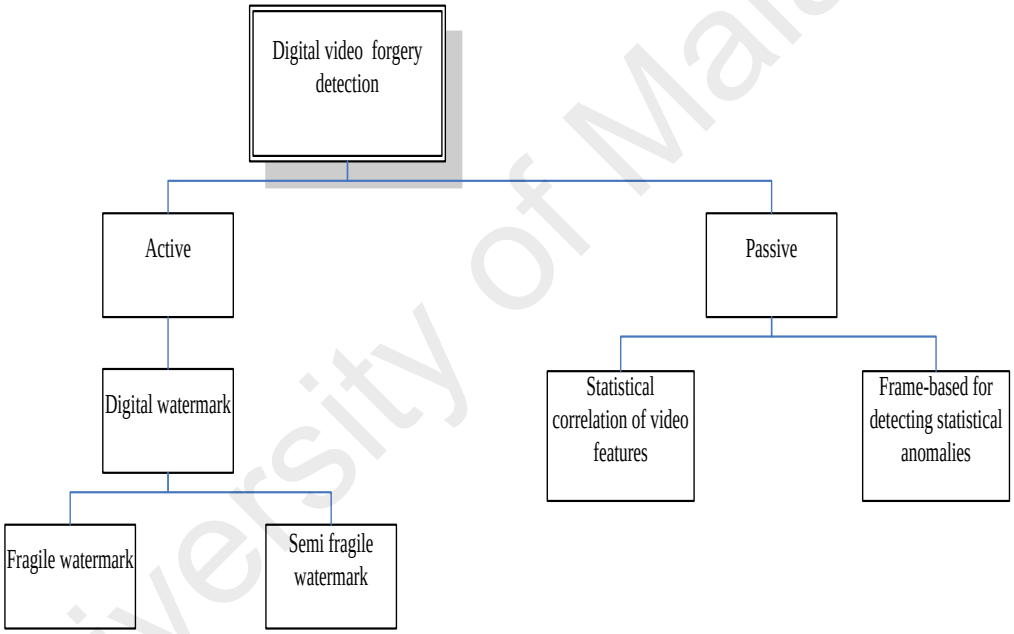

Figure 2.6: Digital Video Forgery Detection

2.8.1 Active Approaches

Active approaches for digital video forgery detection rely on the use of a digital watermark as digital signature for forgery detection (Zhi-yu & Xiang-hong, 2011). A digital watermark is a hiddeninformation embedded into a digital video for tampering detection (Lie, Lin, & Cheng, 2006; Lu & Liao, 2001). There are different types of

digital watermarks. However, among them, two are most commonly used for digital video authentication purpose; these are the fragile and semi fragile watermark.

2.8.1.1 Fragile watermarking

Fragile digital watermarking works by embedding vague data that will be modified if there is any attempt to alter the content of the digital video. Thus, the inserted data used as the watermark can be removed to confirm the realness of the digital video.

2.8.1.2 Semi-fragile watermarking

The semi-fragile watermark works in a comparative manner against the fragile watermark. The presumption of semi-fragile watermark is that alterations will not have effect on the integrity of the video. Thus, semi-fragile watermarks are less robust to alteration, for example compression.

However, notwithstanding, all watermarks whether fragile or semi-fragile are expected to meet the following design requirements for it to be 100% robust:

- Imperceptibility: This refers to the degree at which the watermark is difficult to be perceived by a mind or senses.
- Robustness: This refers to the ability of the watermark to change given the slightest modification of the content to which it is inserted.
- Security: This refers to the degree at which the watermark can withstand an internal or external attack.
- Payload: This refers to the degree at which the actual data is not affected by the insertion of a watermarking scheme with regards to perpetual visibility.
- Bit Error Rates: This refers to the degree at which a watermark can be extracted from an original content with no error rates.
- Complexity: This refers to the degree of difficulty of watermark insertion.

Watermark techniques are now reviewed for active approaches to video authentication based on the watermarking design requirements constraints and the intended use for video forgery detection.

The early work for watermark insertion in digital videos started with (Adelson, 1990) that proposes a technique based on digital to analogue quantization to determine different decoder quantization functions. Although, the technique from (Adelson, 1990) serves as an effective watermarking process for digital video ownership verification, it is unsuccessful in detecting video inpainting and chroma key forgery because different videos have different quantization sizes.

A technique was proposed by (Brassil et al., 1995) for watermark insertion in a digital video which is used to prevent unauthorized copying of a digital video. The technique was found to be useful for inpainting and copy paste forgery detection but could not detect chroma key forgery. The technique is based on line shift coding scheme in a vertical fashion with high reliability for forgery detection involving inpainting and copy paste forgery with respect to digital videos even with the presence of noise. However, the drawback of the technique is high computational complexity when detecting inpainting forgery in compressed videos, even for small search areas.

The work of (Hartung & Girod, 1998) proposed a watermarking technique for video authentication in both compressed and uncompressed videos. A noise pattern is added to the digital video, which in practice is not visible, but statistically unobtrusive, and robust against the slightest tampering. An extension of the watermarking technique in (Hartung & Girod, 1998) was proposed in (Kalker & Haitsma, 2000) for forgery detection in MPEG videos. However, both techniques are reported to have large memory and processing resource requirements.

To address the problem of resource requirement, a watermarking insertion technique for digital video authentication was proposed by (Su, Kundur, & Hatzinakos, 2001) that uses localized pixel frame footprints with regular neighbouring frame structures by inserting watermarks into areas with low expectation to tampering. However, this technique is susceptible to video inpainting and chroma key delusion because most inpainting forgery occurs almost always at the centre of a video frame.

To overcome the delusion problem in (Su et al., 2001), (Zhang, Li, & Zhang, 2001) proposes a technique for embedding a watermark in less frequently changing areas of a video frame using motion vector estimation. This technique was effectively used for the insertion of a watermark in a digital video. However, it degrades the video quality which in most cases introduces artefacts similar to ghost shadows. The inability to distinguish between the introduced artefacts and ghost shadow artefacts limits the capability of this technique for video inpainting and chroma key forgery detection.

Furthermore, a watermark technique using shape adaptive-discrete wavelet transforms (SA-DWT) was proposed in (Kong et al., 2004). The focus of the technique is not only to embed a watermark on video frames but also on objects within the frames. A quantized visual model is used to embed the watermark into the video frame weighted mean in order to achieve a required invisibility. Once a video is tampered, the watermark is affected and thus signifies the tendency of forgery. However, the ability to insert a watermark using this technique requires a reasonable amount of time to achieve.

Another watermarking technique was presented in (Lu, Chen, & Fan, 2005) for the authentication of compressed video that are transmitted over a network. The watermarking technique operates using Variable Length Code-word (VLC) frame wise. The scheme has shown to be robust only with respect tocollusion and copy paste forgery and not for an inpainting forgery detection purpose.

A variable time watermarking technique for digital video was presented in (Levy, 2007) which inserts a watermark in a video frame across locations with variable degree of strength. The technique uses a time dependent masking method for the watermark insertion. This watermark has a record of high imperceptibility but can only successfully be used for video authentication in uncompressed videos.

A watermarking technique used for the authentication of H.264/AVC compressed videos was proposed in (Su et al., 2011). The technique use video segment numbers as watermarks by embedding them into the frames with non-zero quantization indices. The experimental results of this technique have proven the technique to be robust with regards to transcoding and can successfully determine tampered segments of a video easily.

A recent work that extends the work of (Su et al., 2011) was presented in (Li et al., 2015). However, the focus of the work in (Li et al., 2015) is on video recordings from a digital camcorder. The technique uses the relationship of luminance across all frames for embedding watermark information using an adaptive pattern technique. Experimental result of this technique proves a decrease in error rates compared to other techniques. Moreover, the technique proves to be robust with respect to transcoding, recording, and attacks such as copy move forgery but not inpainting and chroma key forgeries.

In conclusion, active approaches using the aforementioned methods to digitally watermark videos, cannot ascertain a forgery in 100% of instances, and therefore these methods on their own cannot guarantee authenticity. However, they can identify forgeries in the scenarios for which they were designed to function.

Another major weakness of active approaches for any kind of video forgery detection and authentication is the insertion of the watermark onto the video. The watermark has to be inserted into the video either during the video acquisition phase, or needs an individual to manually insert the watermark after acquisition. This has been found to be a limitation to active approaches because of the following reasons:

1. The ability of a person responsible for the digital video to deliberately alter the video before watermark insertion.
2. Several encryption techniques prevent unauthorized persons from accessing and changing the content of a video file, however, these encryption techniques do not prevent the file owner from manipulating his video file before encryption.
3. The need for a special hardware for post processing of the digital video for the insertion of a watermark.

Other issues of concern include compression, noise, scaling which also affect the robustness of the watermark.

Table 2.1 shows a summary of the watermarking techniques discussed as evaluated using the six requirements constrains for a watermark design.

Table 2.1: Summary of Systemic Evaluation of Watermarking Techniques for Video Forgery Detection

Author	Technique	Evaluation Criterion																	
		Interceptibility			Robustness			Security			Payload			Error Rates			Complexity		
		H	M	L	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
(Adelson, 1990)	Quantization function	✓					✓			✓			✓	✓			✓		
(Brassil et al., 1995)	Shift line coding		✓		✓				✓				✓		✓		✓		
(Hartung & Girod, 1998)	Noise signal	✓			✓					✓			✓		✓				✓
(Kalker & Haitsma, 2000)	MPEG coding	✓				✓				✓		✓			✓				✓
(Su et al., 2001)	Pixel localization and regular frame structures			✓			✓			✓			✓	✓					✓
(Zhang et al., 2001)	Motion vector	✓			✓					✓			✓		✓			✓	
(Kong et al., 2004)	Shape adaptive-discrete wavelet transform	✓			✓			✓				✓				✓	✓		
(Lu et al., 2005)	Variable length codeword		✓			✓		✓				✓				✓		✓	
(Levy, 2007)	Time dependant masking	✓			✓				✓				✓			✓	✓		
(Su et al., 2011)	Video segments numbers	✓			✓					✓			✓			✓		✓	
(Li et al., 2015)	Adaptive pattern	✓			✓				✓				✓			✓		✓	

H: High, M: Medium, L: Low

The combined weakness of active techniques has made the effective design and insertion of watermark on to a digital video difficult and challenging to use for video forgery detection purpose, as such making it a priority for researchers to devise passive or blind approaches for video authentication. Thus, the area of passive approaches for video authentication and forgery detection was introduced.

2.8.2 Passive Approach

The attempt to overcome the weakness associated with active approaches for digital video forgery detection led forensic researches to devise a better, more robust means of authenticating digital video content. The new approach for the authentication of digital video content is thus referred to as a passive or blind approach as stated in (Wexler, Shechtman, & Irani, 2007; Zhi-yu & Xiang-hong, 2011).

Passive approaches for digital video authentication and validation add a new dimension to video forensics. They are scientific approaches whose techniques do not rely on digital watermark embedded within a digital video for the authentication and validation of a digital video content. Moreover, techniques based on passive approaches do not require any first-hand knowledge of compression types or lightening about the digital video.

The hypothesis behind techniques under passive approaches is the assumption that digital videos are possessed with some hidden patterns which are introduced into them either during the video processing or forgery processing stage. These patterns are often interchangeably called features, artefacts or intrinsic fingerprints. The features are statistically consistent in a non-tampered video. However, the consistency of these features has been often likely to change with a high degree of probability after an alteration process. Although the features are not visible to the human eye, passive approaches extract these features from a video and analyse them for different forgery

detection purposes. Hence the approaches are named passive and blind. In the next section a detailed description of feature extraction is given and how it can be achieved for video forensic analysis.

A number of features and techniques based on passive approach have been proposed in the literature for different forgery detection purpose with regards to a digital video authentication. Different features can only be used to detect different kind of forgeries. This is because every type of forgery leaves a different feature as a clue just like a normal crime scene and each feature is designed to address that specific kind of forgery and as such cannot be used for another forgery problem. This is because features are forgery dependent.

2.9 Features Extraction

In image and video processing, features are referred to as certain interest points in an image or video. These interest points are expected to maintain a certain degree of consistency across several images or videos from the same scene. Therefore, features from an image or video should be invariant to image or video transformation, changes in illumination and insensitive to signal disturbance, such as noise.

Features assume an essential part in the area of video processing. Prior to extracting features from a video, several pre-processing steps may be applied to the video. Examples of pre-processing include noise removal, binarization, thresholding, segmentation etc. Once the pre-processing is successfully achieved, feature extraction techniques are then used on the video to extract the desired features for the video analysis process.

Feature extractions are useful in different video processing applications. Examples of these video processing applications include object detection (Bay et al., 2008), character

recognition (Cheng et al., 2015), behaviour analysis (Dollár et al., 2005), medical imaging and digital forensic analysis.

In the next sub sections, different feature extraction techniques are examined and then clarified pertaining to the best situations to apply each extraction technique.

2.9.1 Video Feature Overview

A good video feature contains segregating data, which can recognize one item from different items. It must be as powerful as could reasonably be expected with a specific end goal to counteract producing distinctive features for the objects in the same class (Kumar & Bhatia, 2014). The chosen set of features should be small whose qualities effectively separate among examples of distinctive classes, yet are the same inside of the same class. Features can be divided into global and local features as identified in (Lisin et al., 2005):

1. Local features
2. Global features

2.9.1.1 Local Features

Local features are descriptors of the local neighbours of each video frame that are obtained from multiple interest points (Kumar & Bhatia, 2014). Example of local feature includes edges, end points, joint etc. The main advantage of local features is the fact that they do not require segmentation during pre-processing before extraction.

2.9.1.2 Global features

Global features in a video are characteristics that describe the whole video. Shape descriptors, textual information, contour representation and statistical properties are example of global features. Global features have the advantage of compact representation of a video. Thus the entire video is considered as an independent point

within a high dimensional space. However, global features are sometimes touchy to clutter. In this work, the use of a Hessian matrix and blurring features is proposed, as global features for video inpainting forgery detection and chroma key forgery detection respectively.

2.9.2 Feature Extraction Methods

There are various types of feature extraction algorithms that are proposed in the literature. However, these feature extraction algorithms use a common extraction method which is either by key point based or block based feature extraction mechanisms.

2.9.2.1 Key Point Based Feature Extraction

One mechanism for the extraction of features from a video is through the use of Key points (Steder et al., 2011). A Key point is commonly referred to as interest points in spatial areas or points in a video that characterizes what is fascinating or what is unique in the video. The motivation behind the use of key point features is based on the fact that regardless of how the video is altered, it does not affect the key points in the video. Examples of key point are corners, circles etc. These key points, once extracted from a video or image, can be used for 3D reconstruction, Robot navigation (Visual Odometry / SLAM) (Rusu & Cousins, 2011), Motion tracking (Sinha et al., 2006), Object recognition (Lowe, 1999), Image alignment for panoramas (Li, Zhang, & Xu, 2003), Indexing and database retrieval (e.g. Google Images) and forgery detection such as copy move forgery for images and videos (Amerini et al., 2011). However, key point based features cannot be effectively used for small region video forgery detection. This is because lines, corners or circles may not span over multiple frames in the video.

2.9.2.2 Block Based Feature Extraction

A different method used for feature extraction is the block based method. In block based method, a video is divided into block of squares usually of the same sizes. The features are then extracted from each block (Wang, Wang, & Feng, 2006). As such feature can be extracted even across the smallest region within a video.

2.9.3 Feature Application

Once the method for feature extraction is decided upon and the desirable portions of the video, which in this case are referred to as features, are selected. The features can then be used for several applications in the area of digital video processing.

Techniques that are proposed in the literature for digital video inpainting forgery detection and chroma key forgery detection based on passive approach are now discussed, by summarizing and analyzing each technique, describing its strength and limitations.

2.10 Passive Techniques for Video Inpainting Forgery Detection

In this section, the passive techniques for video inpainting forgery detection are divided into two categories namely; techniques based on the statistical correlation of video features and techniques based on the statistical anomalies between video frames.

2.10.1 Statistical Correlation of Video Features

Previously, features such as specific hidden structures or patterns found in a digital video as a result of acquisition or alteration or manipulation process were defined. Examples of such features include noise, ghost shadows, dominant light sources, etc. These features exhibit a certain degree and type of relationship between them and any attempt to alter a digital video content will disturb that relationship. A number of techniques as a solution to video inpainting forgery detection based on the analysis of

the relationship of video features have been proposed in the literature over the years. Each of these techniques will be highlighted and the merit or demerit of each solution discussed.

The earliest techniques for video inpainting forgery detection was first proposed in (De, Chadha, & Gupta, 2006) to address a forgery detection problem whereby an object is removed from a single frame within a video. The authors propose a detection technique by the extraction and analysis of readout noise feature from the video. Readout noise is the quantity of electrons in a pixel during readout by a camcorder. The authors calculated the average readout noise over all frames within a video and then compare the mean noise with other frames to detect forgeries. In order to calculate the noise in each frame, the authors applied a de-noising filter to the captured frame by subtracting the noise from the original frame; a noise pattern for a particular frame is then obtained. The process is repeated for all frames and the average is obtained. The variation between the average noise and the noise of a particular region within a frame iscalculated, so that a region from a frame with a high variance from the mean is termed a tampered region in the video. Although, the technique proposed by the authors is only theoretical with no experimental details, it is still considered as the early work on digital video inpainting detection.

Another technique for the detection of video inpainting forgery with a more detail experimental backup based on noise feature was proposed in (Hsu et al., 2008). Noise is referred to as the presence of pixels in an image or a video whose colour and brightness has no relation to the subject. Noise is a characteristic that affects the visibility of images and video; and is more noticeable when there is very little illumination reaching the camera's sensor during the video acquisition process. The authors in their study proposed a technique to utilize the correlation of noise residue

between regions in a video to detect inpainting forgery. This is based on their assumption that there will always be a change in correlation of noise residue between tampered and non-tampered region in a video. The authors present their technique in four different stages as shown in Figure 2.7.

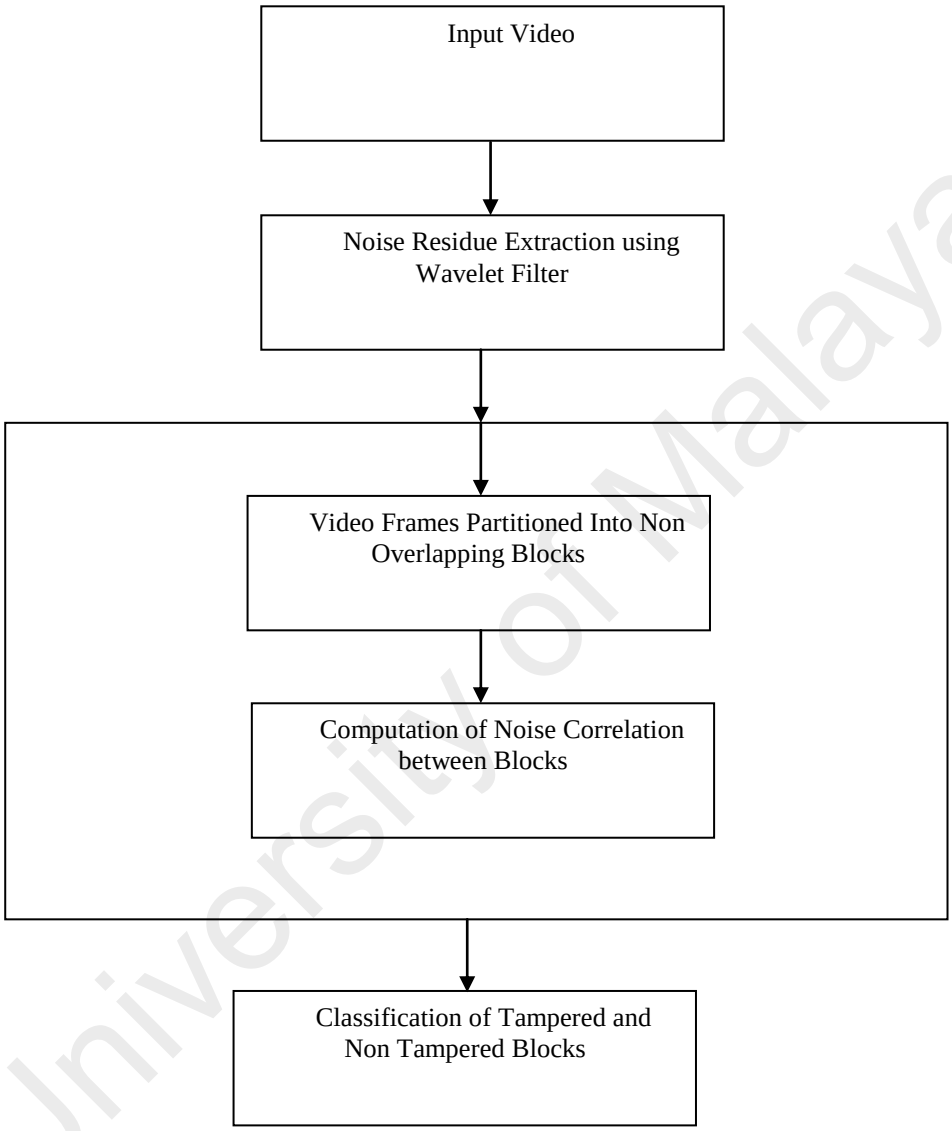

Figure 2.7: Stages for Video Forgery Detection Using Noise Residuary

In the early stage of the technique in Figure 2.7, the authors divides the video into multiple independent frames, then extract the residuary noise for each video frame using a wavelength de-noising filter proposed in (Mıhçak, Kozintsev, & Ramchandran, 1999). In the second stage, the video frames are further partitioned into blocks. The extracted noise correlations between blocks of two frames that are neighboursto each other are calculated in the third stage, while the final stage locates tampered places in the video by analysing the characteristic behaviour of the block by correlating the noise residuals. The experimental results of this technique for video inpainting forgery detection have proven that the technique has a faithful detection accuracy of 96.61% for smooth-display videos. However, videos that have been compressed pose a serious challenge to the technique, this is because compression affects the noise feature distribution of a video, making it a less significant feature for forgery detection purpose. Moreover, noise residue extraction from a video still remains a complex task to achieve.

In order to detect inpainting in a compressed video, (Kobayashi, Okabe, & Sato, 2009)proposed a more robust technique for identifying video inpainting forgery based on noise level characteristic points. The authors suggest the means and variance are determined at individual pixel points rather than at pixel blocks as opposed to the technique of (Hsu et al., 2008). The noise level function is determined by supplying a bias probability function to individual pixel characteristic points. Individual pixels are then examined by their distance from the noise level function. Experimental results of this technique were reported to achieve an average detection accuracy of 91.37% for both compressed and uncompressed videos. However, the technique only detects forgery on videos that are recorded with inpainted objects that are static with a lossless compression.

In (Zhang, Su, & Zhang, 2009), a technique was proposed for detecting forgeries involving moving objects using ghost shadow artefact (GSA) that are introduced on to a video from the effect of inpainting. Ghost shadows are flickers that are introduced into a video as a result of temporal discontinuity arising from an inpainted area. The technique of (Zhang et al., 2009) partitions each frame into a moving foreground and a static background block match as shown in Figure 2.8. A panoramic image called mosaic is formed by joining a number of frames together. Accumulative difference and a mathematical morphological operation are used to obtain a track of the moving foreground. The consistency between the foreground mosaic and the track of the moving object indicates the video is authentic otherwise it is a forgery with ghost shadow artefacts.

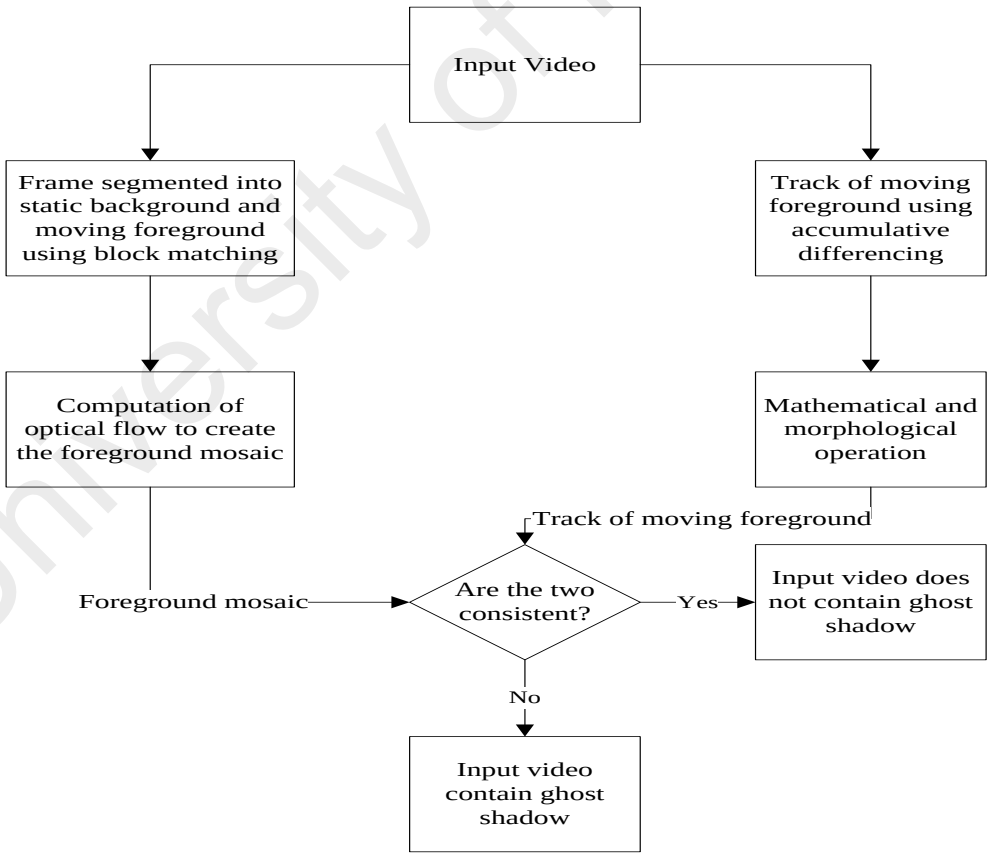

Figure 2.8: Block Diagram of GSA Approach

The GSA technique provides a promising result for video inpainting forgery detection with a detection accuracy of 93.4%, but experiments have shown that the method is more robust to MPEG compression and recompression.

To address the problem of inpainted videos that have not undergone compression and recompression, a technique for inpainting forgery detection in digital videos that make use of zero or null connectivity features and fuzzy membership function was proposed in (Das, Shreyas, & Devan, 2012).The technique is divided into stages as shown in Figure 2.9.

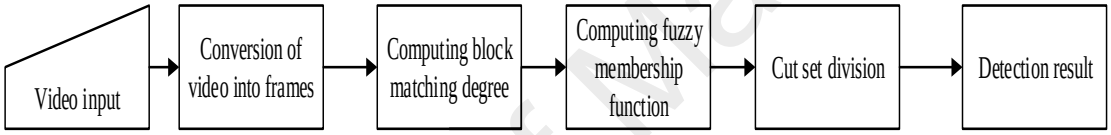

Figure 2.9: Block Diagram for Zero Connectivity and Fuzzy Set Membership

In the first stage, a video is divided into multiple frames; each frame is then further partitioned into smaller blocks. In the second stage, a zero or null connectivity tag is used on blocks to get a fitting degree for blocks around forged areas. In the third stage, a construction of a trapezoid function is done which is used for the computation of the fuzzy membership function. Finally, tampered regions are determined using a cut set. The experimental result from the technique for video inpainting forgery detection was reported to achieve 95% detection accuracy. However, the limitation of this work is the fact that it can only be applicable to uncompressed videos.

A technique that addresses both compressed and uncompressed videos for the detection of video inpainting forgery using features extracted from blocked motion estimation analysis was proposed in (Li et al., 2013). The technique extracts moving

features crosswise over nearby frames. The correlation of the moving vector magnitude between nearby frames is utilized as the determinant for tampered and un-tampered regions within the video. Experimental tests have demonstrated that the technique is efficient in identifying inpainting manipulation in both compressed and uncompressed videos with a moving background. However, modern inpainting algorithms that include complex interpolations, for example, spline interpolation still remain a challenge for this technique. This challenge emerges due to the disparity in motion vector estimation.

The challenge identified due to the disparity in motion vector estimation from the technique in(Li et al., 2013) was tackled in the technique proposed by (Subramanyam & Emmanuel, 2013) by introducing the concept of practical quantization estimation theory. A group of pixels from a video frame is evaluated over a collection of pixels that are extracted from different video frames in a Group of Picture (GOP). The relative error that exists between the exact value and evaluated value is analysed against a pre-characterized threshold for the identification of inpainting forgery in a GOP. Experimental result of the technique has demonstrated its efficiency to detect inpainting forgery of interlaced, progressive, or lower bit rate frames in a GOP that involve complex inpainting. In any case, small area tamper identification remains a challenge to this technique.

The detection and localization of inpainting forgery by analysingartefacts extracted from temporal domain of a 3D video was proposed in (Lin & Tsay, 2013). Analysis has demonstrated the technique has a sensible video inpainting detection accuracy of 96.3% only for good quality videos. However, the technique does not localize the exact region of inpaint in the video.

An improvement of the technique in (Lin & Tsay, 2013) was proposed in (Lin & Tsay, 2014). The improved technique locates the exact region of inpainting in a video.

This is achieved by utilizing spatio-temporal slicing and coherence analysis (STCA). The disparity in spatio-temporal coherence between inpainted and non inpainted region within the video is used as evidence for inpaint region identification. The technique is reported as having a detection accuracy of 97.52%. However, the technique is also reported as having a high computational complexity.

Table 2.2 shows a summary of the techniques under passive approach based on the analysis of the statistical correlation of video features for inpainting forgery detection. The goal of techniques under this category is to identify and analyse the statistical behaviour of features in a video in order to detect the presence or absence of inpainting forgery.

Table 2.2: Summary of Techniques for Video Inpainting Forgery Detection Based on Video Feature

Reference	Technique Used	Detection (%)	Miss (%)	F-Positive (%)	Limitations
(De et al., 2006)	Variation in read out noise	-	-	-	Lack experimental backup
(Hsu et al., 2008)	Statistical correlation of noise residue (STCA)	96.61	37.46	1.18	Inefficiency with compressed videos Noise residue - extraction a complex task
(Kobayashi et al., 2009)	Independent noise characteristics	91.37	-	-	Only considers videos that are recorded from static scenes with a lossless compression
(Zhang et al., 2009)	Analysis of Ghost shadow artifacts	93.4	-	6.60	Only robust to MPEG compression and recompression
(Das et al., 2012)	Zero connectivity and fuzzy membership theory	95.0	-	5	Only applicable to uncompressed video
(Li et al., 2013)	Motion estimation features	98.0	-	2	Efficient to video with a moving background
(Subramanyam & Emmanuel, 2013)	Practical quantization estimation theory	-	-	-	Small area temper identification remains a challenge to this technique
(Lin & Tsay, 2013)	Temporal artifacts	96.3%	-	-	Good detection efficiency only for good quality videos
(Lin & Tsay, 2014)	STCA	97.52	-	3.22	High computational complexity.

2.10.2 Frame-Based for Detecting Statistical Anomalies

A video contains a combination of sequential frames that are captured at different time domains. Video inpainting quite often involves the removal of an object from a frame or a group of frames during the forging process. However, studies have shown that video frames are made up of pixels which, when grouped together form a normalized correlation. These normalized correlation values are often used in many video inpainting forgery detection techniques as a similarity metric for the detection of inpainting.

A detection technique for video inpainting forgery was proposed in (Porter, Mirmehdi, & Thomas, 2000). The technique exploits video frame correlation using a regular spatial decomposition. The authors partition a video frame into a size of 32 X 32 blocks. For a given block in the frame, a best matching block is taken. This is achieved by calculating the normalized correlation between blocks and then locating the correlation coefficients with the largest magnitude. A single similarity metric is then derived for each frame by calculating the standard deviation from an obtained pronominal mean of the correlation peak. A new mean is calculated for the peaks that fall outside the original mean. The mean between the two frames are compared with the average match of the previous frame. If there is a significant inter-frame decrease, a forgery is then detected. Experimental result of this technique has witnessed a 92.54% detection rate in high quality videos but has a high computational complexity. Moreover, the technique does not trend well with videos that are blurred and blocks with higher partition.

A detection technique for logo removal forgery that is done using inpainting that uses inconsistency of blurring artifacts frame wise was proposed in (Zhang & Su, 2009) to address the video quality issue in (Porter et al., 2000). The technique estimates the

blurriness across video frames using regularity characteristics in a wavelet domain. The order of blurriness across forged areas in a frame is modelled as a Gaussian Mixture Model GMM while an estimated maximum likelihood algorithm is used for blur parameter estimation. A Bayesian classifier is used to distinguish between a forged and un-forged region in the video. The technique records a promising result for high and low quality videos of up to 90.86% detection accuracy. However, the technique is only robust to small region inpaint detection.

Block partitions size problem from (Porter et al., 2000), was addressed in a technique proposed by (Kancherla & Mukkamala, 2012). The information from objects in a video is extracted using the concept of collusion on sequential frames to obtain a base frame. A Markov chain model is then applied to the motion information residuary by adapting the concept of support vector machine (SVM) in a practical experiment. The experimental results of this technique were reported to achieve an average detection accuracy of 87%. However, the major limitation of this technique is its computation expense especially for small number of feature sets.

Feature set size was addressed in a technique proposed by (Chen et al., 2012). The technique focuses on object contour in a video frame and how the adjustable width object boundary is affected when an object is removed from a video using the method of inpainting. This allows the identification of inpainting forgery in a video by analyzing the co efficient of non-sub sampled contourlet (NSCT) and gradient information out of which a set of features are extracted and combined as input to support vector machine (SVM) for a fine classification of inpainted and non inpainted region. The technique was reported as having achieved an accuracy of 95% correct detection rate. Nevertheless, the features used in the technique heavily rely on the training sample due to the complexity and diversity of digital videos.

In (Bestagini et al., 2013) a technique for detecting object removal and insertion forgery by cross correlating small 3D frame blocks was proposed. The technique detects regions of object removal with no assumption of prior knowledge. The authors compute a residual matrix R from a given video sequence by scaling it to a fraction of 5 while retaining its full temporal resolution. R is analyzed to remove the effect of linear operation that may have occurred due to an inpainting operation. R is then split into non overlapping 3D blocks of B_m^n of size $\boldsymbol{d_i X d_j X d_k}$ where n is the starting time index of a block and $\boldsymbol{m\mathcal{E}}$ $[\mathbf{1}, \boldsymbol{m}]$ is the block index. Analysis of the frame blocks is done in time intervals to detect forgery. The detection uses the correlation between $\boldsymbol{B_m^n}$ and R. The peak value of each is calculated as$\boldsymbol{pB_m^n}$**.** The block with the largest value of $\boldsymbol{pB_m^n}$ is likely to contain forgery. The results of the technique were validated using 20 realistic video sequences created by the authors and others adopted from surrey university library for forensic analysis (SULFA) data set. The authors recorded an accuracy of 90%. However, the technique does not handle complex video inpainting forgery such as spline inpainting.

A technique for detecting different kind of forgeries that also includes inpainting based on variance in luminance and signal to noise ratios, using a LESH feature was proposed in (Pathak & Patil, 2014). A test video is converted into group of pictures (GOP) based on frame rates. The luminance of the GOP is calculated upon RGB component separation. For every frame in the GOP, the local and average entropy are determined. The frames are then compared for anomaly in the entropy values. If there is no anomaly between the entropy value of all frames, then the video is original otherwise it is presumed to have been tampered. The limitation of this technique is its lack of ability to detect inpainting forgery in moving objects.

Table 2.3 shows a summary of the techniques under passive approach based on video frame anomalies for inpainting forgery detection. The goal of techniques under this category is to identify and analyze the anomalies that exist between frames in a video in order to detect the presence or absence of inpainting forgery.

Table 2.3: Summary of Techniques for Video Inpainting Forgery Detection Based on Frame Inconsistencies

Reference	Technique Used	Detection (%)	Miss (%)	F-Positive (%)	Limitations
(Porter et al., 2000)	Regular spatial decomposition	92.54	-	-	High computational complexity Technique does not trend well with low quality videos and frame blocks with higher partition
(Zhang & Su, 2009)	Blur inconsistency	90.86	-	-	Only robust to small region inpaint detection
(Kancherla & Mukkamala, 2012)	Markov Chain	87	-	-	Compute extensive for small number of feature set
(**Chen, Dong, Ren, & Fu, 2012**	Non sub-sampled contourlet (NSCT) and gradient information	95	-	-	Features used rely on the training sample
Bestagini, Milani, Tagliasacchi, & Tubaro, 2013)	Cross correlating small frame blocks	90	-	-	Technique is not robust to complex video inpainting
(Pathak & Patil, 2014)	Variance in luminance and signal to noise ratio using LESH features	93.6	-	-	Lack the ability to detect inpainting forgery in moving objects

2.11 Passive Techniques for Chroma key Forgery Detection

Digital video matting or composition utilizing chroma key technology permits imaginary objects to be included into a video, which when goes unnoticed may be mistaken for an original video. If such a mistake happens, it will often cause a handful of problems to society such as convicting an innocent person. As such, in order to detect video composition forgery using chroma key technology, (Xu et al., 2012) proposed the only directly known technique, to the best of our knowledge, based on the statistical correlation of quantized discrete cosine transform (SCQDCT). To detect chroma key forgery in a video, SCQDCT relies on upon the distinction of the video quality between its background and foreground. This depends on a suspicion that the videos utilized for the matting process during composition are compressed with variable compression bit rates. Then again, this presumption restricts the capacity of the technique, as not all videos may have variable compression rates. What if the compression rate is the same? In any case, the performance of the technique has been accounted for as accomplishing a detection precision of 88% for chroma key forgery detection in digital videos that have variable compression rates.

There are other techniques that by implication can indirectly be utilized for chroma key forgery detection in digital videos. However, these techniques were initially proposed for the detection of video splicing forgery. Video splicing is a forgery strategy for video compositing that consolidates two distinct videos together, either from the same or diverse sources, into a single video. The strategy for video splicing forgery is nearly the same idea that is utilized for chroma key forgery in digital videos.Notwithstanding, the distinction between video splicing and chroma key forgery is that in video splicing, non of the video utilized for the matting process, is relied upon to have a uniform background, for instance green or blue.

A good number of techniques have been proposed for the detection of video splicing forgery. In any case, our experiments have demonstrated that only one chosen technique, that can detect splicing involving videos from various sources, can also be utilized for chroma key forgery identification.A splicing detection technique that can be used for chroma key forgery detection is the technique that is proposed in (Wang & Farid, 2009). The technique is based on the analysis of double quantization of macro blocks that are extracted from video frames ADQMBs, whereby a double quantization analysis is then performed independently for each frame macro block. This technique is embraced from its underlying use in JPEG image forensic examination, thus the technique works well only for a video that have been encoded twice. The inventors of the technique assume that motion JPEG encoding has been performed on the video. In any case, this assumption strongly confines the appropriateness of their technique. Besides, the two-fold quantization analysis that is done on the video makes the technique computationally intensive.

The common problem of these existing techniques for chroma key forgery detection is their sole dependence on the distinction in source video encoding. However, when the two source videos, used for the mating process, are of the same encoding and having the same bit rate, the detection ability of these techniques eventually fails.

2.12 Chapter Summary

In this chapter, a general overview of video forensics is discussed. The methods for inpainting and chroma key forgeries are also discussed. A general review of related literature for digital inpainting and chroma key forgery detection techniques was reported. The detection techniques identified from the literature for the two forgery problems in digital video were analysed for their detection ability and limitations.

CHAPTER 3 : RESEARCH METHODOLOGY

In this chapter, the general methodology used is discussed, for the development of our proposed solution, for inpainting forgery detection and chroma key forgery detection in digital videos respectively.

3.1 Introduction

In the previous chapter (Chapter 2), the various techniques developed were reviewed for inpainting forgery and chroma key forgery detection in digital videos, respectively.However, it will be noted from the output of our literature review that the success of any video forgery detection technique depends on the strength, speed and robustnessof the features used to detect forgery in compressed and uncompressed videos. Thus, the identification of more robust features to detect inpainting and chroma key forgery for digital videos has become essential. This study will help obtain an improved reliability and better detection accuracy with respect to video inpainting and chroma key forgery detection. Therefore, in this chapter, the general step-by-step implementation of our proposed technique for inpainting and chroma key forgery detection techniques, respectively, is discussed.

3.2 System Requirement

The proposed system for both video inpainting and chroma key forgery detection for digital video was developed using matlab programming version R2011bon an IntelCeleron computer having a 1.83 GHz processor speed, 64 bit operating system, and 4GB RAM. The requirements were determined as appropriate for this methodology based on the fact that matlab provides significant functions that can simulate the analysis of a digital video. Moreover, since we are dealing with feature matrix dataset, the use of matlab as a simulation tool help provide functions that would be applied for

matrix operations such as the cross correlations which form the base for our extracted feature analysis.

3.3 Methodology

The methodology that is used in this study is divided into stages as shown in Figure 3.1 that consist of the input stage, pre-processing stage, feature extraction stage and then the statistical feature correlation computations stage. The process of the methodology in Figure 3.1 follows a statistical correlations analysis. It is established in order to analyze even the smallest region of a video frame by extracting different features from regions in the video in order analyze the correlation that exist between the features for the purpose of forgery detection. Moreover, the proposed methodology was designed on the basis that no prior probability about a video being original or forged is needed or the prior probability of any trace of forgery. Thus, in the proposed methodology, the probability of a region being forged is determined by the block level correlation analysis of the extracted features from a video.

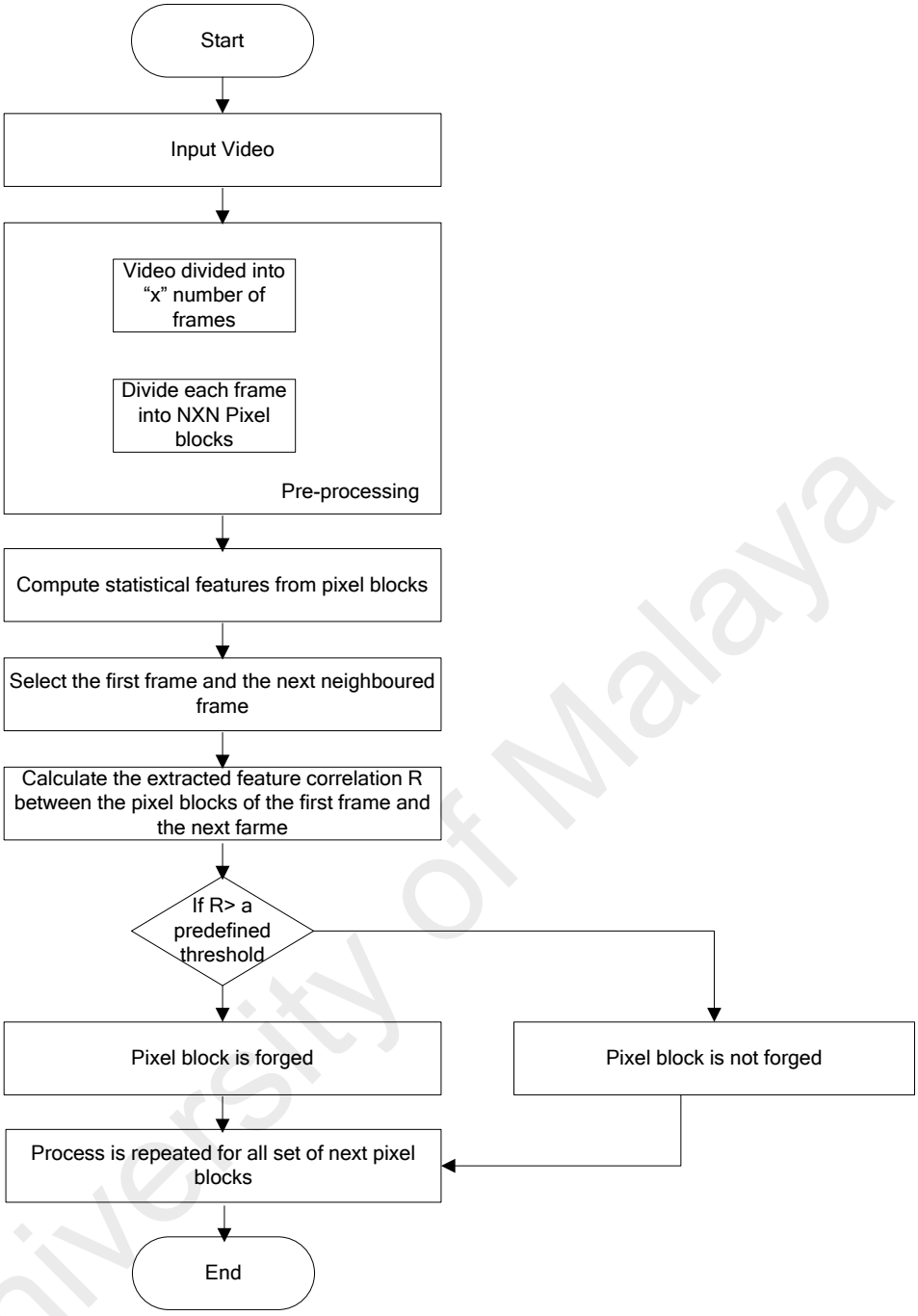

Figure 3.1: Stages of Research Methodology for Video Forgery Detection

3.3.1 Input Stage

In this section, the video data sample acquisition is performed. This is because digital videos are saved using different format encodings. Video format encoding is an important factor to be considered while collecting any video data used for experimental analysis.This factor may have an influence on the performance of the output result, especially the features that might be used for the forgery identification mechanism.

This research study for video inpainting and chroma key forgery detection used both videos that are compressed and uncompressed. Videos that are victims of small and big region forgery were also used. However, the matlab code requires a certain number of parameter definitions from the user during the reading and framing processes of the video. These include the physical location of the video in the computer storage medium. Another parameter is the format with which the frames will be stored in the system.

3.3.2 Pre- Processing Stage

Once the video is successfully read into the system, the next step of our methodology is to pre-process the video in order improve the video efficacy in preparation for a clean feature extraction.The pre-processing stage can take the form of segmentation or noise removal depending the forgery problem been addressed. Furthermore, after the pre-processing stage,the video is divided into multiple independent frames of fixed sizes so as to be able to perform a statistical correlation analysis between the frames as shown in Figure 3.2 where F1 represents frame 1, F2 represents frame 2 and Fn represents frame n.

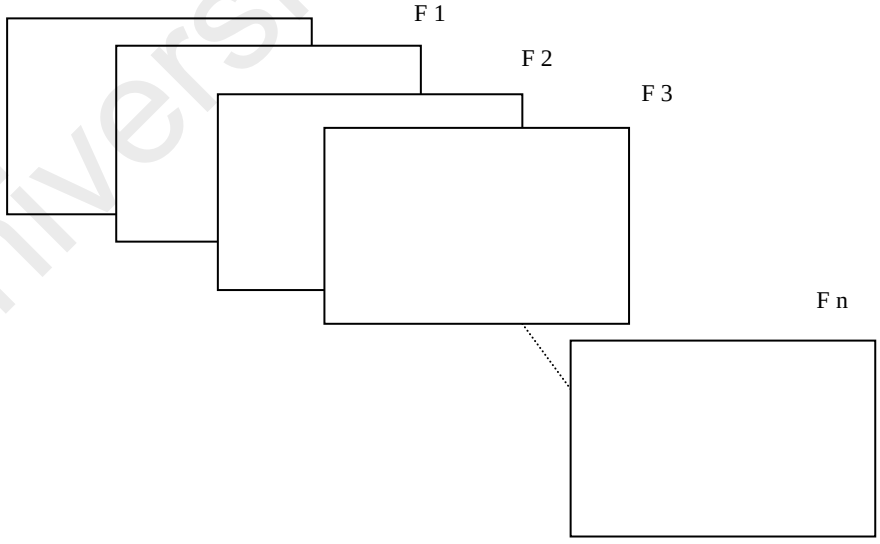

Figure 3.2: Video To Frames

The video frames are further divided into block sizes of $N \times N$ partitions where the value of N is 8. This is to obtain a minimal representation of block sizes that can effectively be analyzed to detect even the smallest region of forgery within a video frame. Example of the $N \times N$ blocks is shown as shaded portions in Figure 3.3.

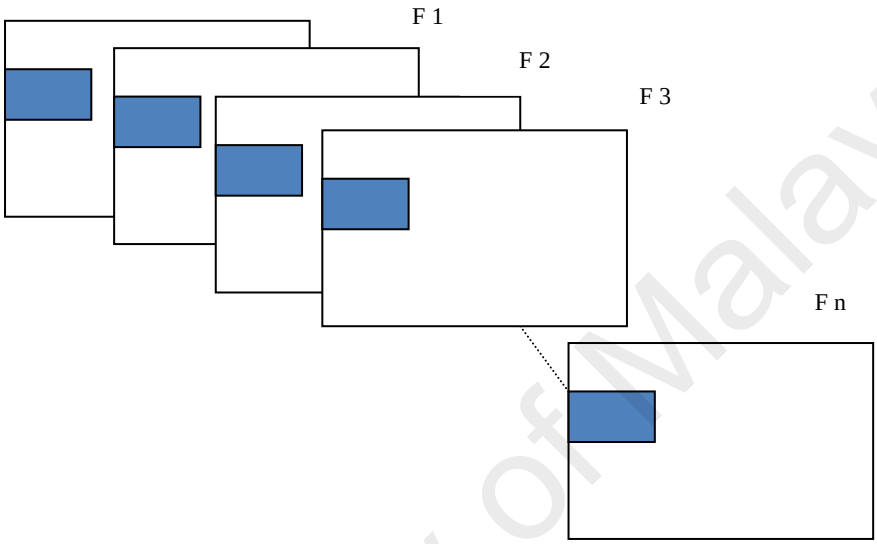

Figure 3.3: Video Frame Partitioned into Pixel Blocks

3.3 Feature Extraction Stage

As discussed earlier, the aim of feature extraction is to extract and isolate the important salient characteristics from a video signal that are unique for a non-forged video. Thus any attempt to alter the video will disturb the uniformity of the video features. Block based feature extraction method is considered as one of the standard method that is used for feature extraction in image and video processing because of its wide popularity interms of extraction accuracy as compared to other feature extraction methods. Thus, by using the proposed video inpainting and chroma key forgery detection techniques, each video is divided into image frames; each frame is further

divided into smaller pixel blocks. The desired features are then extracted from independent blocks for further analysis.

3.4 Statistical Correlation of Extracted Video Features

Once the features are extracted successfully from video frame blocks, the statistical correlation R between features from blocks that are neighbours to each other is computed as shown in Figure 3.4.

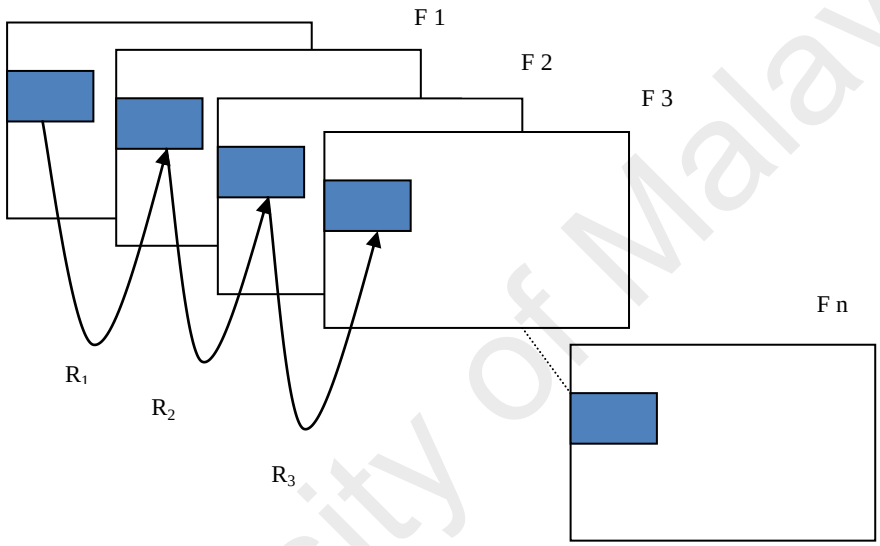

Figure 3.4: Correlation computation of extracted features

Finally, tampered regions are located by the analysis of block level feature correlation which is achieved using a classification or heuristic mechanism.

3.5 Chapter Summary

In this chapter, the general methodology is presented which is used in the design and implementation of the proposed system for video inpainting and chroma key forgery detection. However, a more specific detail for each contribution and the framework models are explained in detail in chapter 4 and 5 respectively.

CHAPTER 4 : VIDEO INPAINTING DETECTION

In this chapter, the contribution which is a framework and experimental results of an inventive technique and system for video inpainting forgery detection is presented. This technique utilizes the statistical correlation of Hessian matrix features for the detection of inpainting forgery in a digital video that is recorded using a static camera. This key contribution is the introduction of a Hessian matrix as a feature in a technique for the detection of video inpainting forgery. The advantage of the Hessian matrix feature is its unique ability to establish a better and faster mechanism from which key points in a video frame can be calculated across pixel blocks, thus making this techniques robust, simple and efficient compared to other benchmark techniques proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014). Moreover, this technique can also detect inpainting forgery in both compressed and non-compressed videos; this is because compression has no effect on the Hessian matrix features. This technique also has a reduced execution time as compared to the techniques proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014) because of the relative speed of Hessian matrix generation from a video and the limited number of processing steps proposed in this technique.The chapter is divided into three main parts: the first section (section 4.1) highlight a brief introduction. The second section (section 4.2) present our proposed framework for video inpainting forgery detection based on the correlation of Hessian matrix features while the experimental results, analysis and discussion are presented in the third section (section 4.3).

4.1 Introduction

The digital world is overwhelmed with digital videos. This is because digital videos are everywhere especially in areas such as banks, train stations, airports and other sensitive places mostly for the purpose of security. Some of the videos acquired in these

areas in one way or the other may be used as evidence during a court case in order to relate a suspect to a crime. However, because of the availability of freely available user friendly video editing software, it is now easy to illegally manipulate a video for malicious reasons. One example of illegal video manipulation is the removal of an object from a video scene using one of many video inpainting methods. This happen especially when the video accidentally falls into the wrong hands, thus makes the authenticity of such a video extremely difficult to establish using the human naked eye. For this reason, a novel technique is proposed based on the correlation of Hessian matrix feature for the detection of video inpainting forgery for object removal in static video scenes.

4.2 Video Inpainting Detection Framework

This research focuses on addressing the detection problem of digital video inpainting forgery for the illegal removal of an object from a real world scene. These problems include decreased detection accuracy, increased false positive detection rate and high computational complexity of existing detection algorithms. In order to address these problems, the following video inpainting detection framework, shown in Figure 4.1, is proposed, using the statistical correlation of Hessian matrix (SCHM).

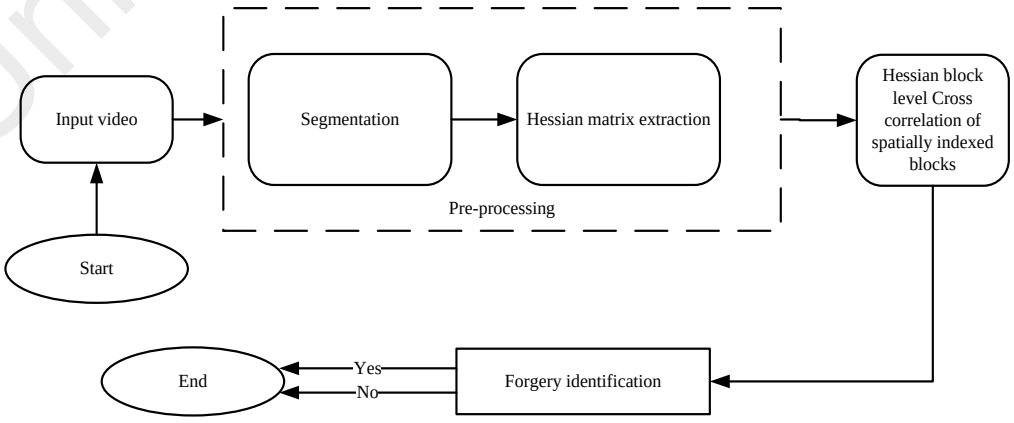

Figure 4.1: Proposed Video Inpainting Detection Model

The architectural process of this proposed video inpainting detection framework is divided into three sequential stages involving the pre-processing stage, Hessian block level cross correlation computation and finally inpainted region forgery identification.

However, prior to the pre-processing stage, the input video is divided into smaller images called frames. Video frames are sequence of images which are extracted systematically from a video within small interval of time in order to preserve the video sequence continuity. The video frames are made up of small elements called pixels that describe their behaviour such as colour and intensity variations at some point within the video. Thus, a complete video is made up of a huge data describing its sequence and operations. However, in order to extract the useful features needed for the inpainting detection experiment a column wise frame decomposition is performed in which an extracted frame is further sub divided into partitions of ***NXN*** pixel blocks as depicted in Figure 4.2. This is to enable us use a block feature extraction approach.

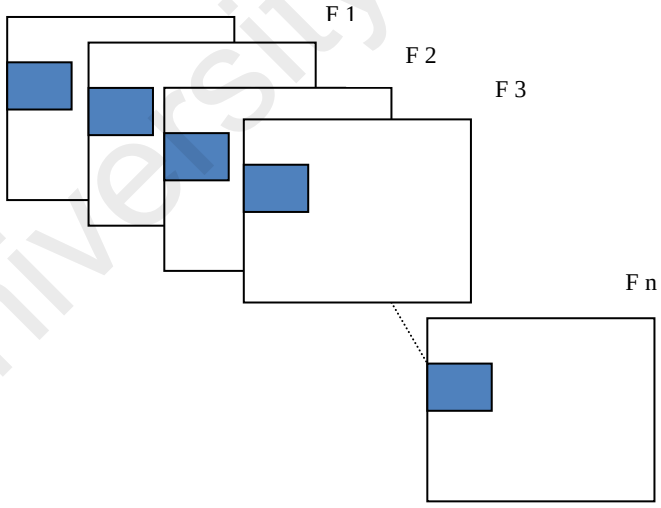

Figure 4.2: Video Frame Blocks

4.2.1 Pre-processing

Pre-processing refers to the use of algorithms for the enhancement of a video in preparation for analysis. This is to increase the efficacy of the video signal for ease of

analysis. This proposed video inpainting detection technique; segmentation and Hessian matrix feature extraction is performed during the pre-processing stage. Therefore, in this section different video segmentation techniques are discussed concerning how the Hessian matrix feature is extracted from a video.

4.2.1.1 Segmentation

The first step of this pre-processing stage is the segmentation process. Segmentation is the mechanism through which a video frame is divided into multi parts. This is to identify objects or other significant information in the digital video for ease of analysis. A variety of methods have been proposed for achieving segmentation which includes: the thresholding methods, color based methods, transform methods and texture methods. Different video segmentation methods are now discussed in order to determine the most preferable one, given the kind of problems needed to be addressed. Thisis because the best segmentation method is required, namely one that will minimally effect the original quality of the video.

4.2.1.1.1 Thresholding Methods

The method of thresholding is regarded as the simplest method of segmentation whereby pixels in a video are segmented based on the values of their intensities. Three different thresholding techniques can be found from the literature which includes the global, variable and multiple thresholding.

Global Thresholding

Global thresholding refers to the rate of the intensity variations between two image peaks (Lee, Chung, & Park, 1990; Sahoo, Soltani, & Wong, 1988). Global thresholding uses a selected global threshold *T* for the segmentation process as shown in equation 1.

$$g(x,y) = \begin{cases} 1, & if\ (x,y) > T \\ 0, & if\ (x,y) \leq T \end{cases} \qquad (1)$$

This global threshold value is used to separate the pixels in a video frame into a binary classification based on the pixel intensity variation over a certain threshold value. The output is a segmented frame in a slice wise manner of a packed bit between the values of 0 to 1 (Lee et al., 1990). Pixels with intensity values less than or equal to the threshold T are set to 0 while others above the threshold T are set to 1.

Variable Thresholding

Variable thresholding refers to the rate of the intensity variations between two image peaks in which the threshold values do change with respect to time. This type of thresholding performs well when the region of interest and its corresponding background are almost of comparable sizes otherwise the performance is degraded.

Multiple Thresholding

Global and variable thresholding classify pixels as a binary classification, in which pixels may have an intensity values either lower or greater than that of a given threshold. However, the multiple thresholds allow pixels in a video to be classified into more than two different classes of intensities. An example is a segmentation of a video into 3 classes namely: bright pixels, background pixels and intermediate pixels. This type of segmentation is useful when the desired content to be segmented has very many pixel variations.

4.2.1.1.2 Colour Based Method

This is a segmentation method that is used to divide an image or video into different colour clusters. A given cluster is randomly chosen as a centre or based on some heuristic (Barghout & Sheynin, 2013). Each pixel in the video is assigned to a cluster that reduces the distance from the pixel to the cluster centres. In this case, the distance is the absolute difference that exist between a pixel and a given colour cluster.

The cluster centres are calculated by computing the mean of all pixels in a colour cluster in order to obtain a convergence point where no pixel changes a cluster. This segmentation method has a guarantee of convergence. However, the segmentation process does not always return an optimal solution. This is because the optimal solution depends on the initial colour cluster selection.

4.2.1.1.3 Transform Method

The transform method of segmentation partitions an image or video pixels into three dimensions, which involve two spatial coordinates and then gradient intensity. Pixels in a video with very high intensity magnitudes that corresponds to lines of a transform are used to represent region boundaries. However, this method is only proposed in theory. The actualization of this method is still pending further research.

4.2.1.1.4 Texture Methods

A texture in an image or video refers to the values that are obtained from the quantification of the image or video perceive textures. These values allows the extraction and understanding of colour intensity arrangements in a spatial domain of an entire image, video frame or an interested region within the image or video frame (Shapiro & Stockman, 2001). The importance of textures in image and video segmentation is its usefulness as descriptive information about larger image regions as smaller segments. Two common types of texture segmentations are the region based texture segmentation and the boundary based texture segmentation.

Region Based Texture Segmentation

The aim of this type of texture segmentation is to cluster video pixels together on the basis of their texture characteristics. These texture characteristics may be classified into two namely; natural texture characteristics and artificial texture characteristics. Natural

texture characteristics are found naturally embedded in an image or video scene while artificial texture characteristics are created in the image or video scene.

Boundary Based Texture Segmentation

The aim of this type of texture segmentation is to cluster image or video pixels on the basis of the object edges extracted from the pixels coming from different texture characteristics. This type of segmentation has proved to be an excellent segmentation method for videos. As such, in order to provide video frames that represent meaningful and convenient information for ease of analysis, the boundary based texture method is applied for video frame segmentation in this research experiment. This allows easy and convenient identification of objects within a frame boundary such as lines and curves. Moreover, the result obtained from the segmentation process helps to apply a statistical approach that allows the video frame texture to be analysed as quantitative measures of intensity arrangement surrounding a given pixel block region.Figure 4.3 shows an example of an original video frame and a segmented frame using the boundary based texture segmentation method.

a

b

c

Figure 4.3: (a) Original Video Frames, (b) Inpainted Video Frames, (c) Result of Segmentation of the Inpainted Video Frame

4.2.2 Hessian Feature Extraction

Having discussed the segmentation phase of the pre-processing stage of this proposed video inpainting detection framework, the second phase of the pre-processing stage is discussed which is the Hessian matrix feature and the extraction of the feature from a video for the purpose of this experiment.

4.2.2.1 Hessian Matrix

The idea of Hessian matrix started from the concept of mathematical theory. The study of Hessian matrix started in the 19th century by a mathematician from a German origin by the name Ludwig Otto Hesse. The Hessian matrix developed was named after

its founder. However, the original term used by the founder for describing a Hessian matrix is the "functional determinant".

In mathematical concept, a Hessian matrix is a square matrix of second-order partial derivatives of a scalar-valued function that is used in describing the local curvature of a function of many variables as in the definition below.

Definition

Suppose f is a real valued function over $\mathbb{R}^n \rightarrow \mathbb{R}$ where the function f takes a vector $x \in \mathbb{R}^n$ and producing a scalar output $f(x) \in \mathbb{R}$. Now if the second order partial derivative of f exist and is continuous over the functions domain, then the Hessian matrix H of that function is a square matrix of NxN dimension generally denoted in equation 2 as follows:

$$H=\begin{bmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} & \dots\dots & \frac{\partial^2 f}{\partial x_1 \partial x_n} \\ \frac{\partial^2 f}{\partial x_1 \partial x_2} & \frac{\partial^2 f}{\partial x_2^2} & \dots\dots & \frac{\partial^2 f}{\partial x_2 \partial x_n} \\ \frac{\partial^2 x}{\partial x_1 \partial x_1} & \frac{\partial^2 x}{\partial x_n \partial x_2} & \dots\dots & \frac{\partial^2 x}{\partial x_n^2} \end{bmatrix} \quad (2)$$

In image processing and vision computing, a Hessian matrix provides the second order partial derivative of an image which involves the image gradients and intensities at different points. An example of Hessian matrix in image processing can be seen in feature detection algorithms such as SIFT. SIFT uses Hessian matrix for the selection of adequate localized features that are later used to determine whether the feature positions found from the difference of Gaussian extrema are the same found on the edges or corners in an image. These features have been reported to be successfully used for copy move forgery detection in digital images, measurement of curvature at a point when the image is treated as an intensity surface and the description of the local structure in a neighbourhood around a point. In this research, the use of Hessian matrix feature is

proposed for the detection and localization of inpainted region in a video. This is because of the ability of the Hessian matrix features to identify characteristic interest points in a video irrespective of intensity changes as compared to other proposed features from the literature (Sato et al., 1997).

4.2.2.2 Hessian Matrix Feature Extraction

To extract the Hessian matrix features from a video, a block based approach is employed for feature extraction in which the entire video is divided into multiple independent frames and each frame is further divided into pixel blocks of ***NXN*** partitions. The Hessian matrix of a given pixel block is then obtained by calculating the second order of the partial derivative of the frame pixel block. Thus, a Hessian matrix provides a description of a 2nd order intensity variations surrounding a chosen pixel region (Sato et al., 1997).

Once the Hessian matrix feature vector is obtained, the eigenvalues and eigenvectors can be easily obtained to extract the orthonormal coordinates aligning the second order structure of each pixel block within the video frame (Frangi et al., 1998). The extracted Hessian matrix $H(i,j)$ from the video frame pixel blocks in our proposed video inpainting detection framework is used to identify tampered and non tampered regions within the video. The advantage of using the Hessian matrix features is mainly because of its reliability in identifying characteristics interest points and intensity changes for image analysis.

4.2.3 Statistical Correlation of Hessian Matrix Feature

Once a suspected video is pre-processed and the Hessian matrix features are successfully extracted from frame pixel blocks, the relationship between the pixel blocks Hessian data is computed and the histogram of correlation analysed.

Correlation is a factual statistical method that is used to demonstrate whether and how two sets of data are related. The use of correlation is important for predictive relationship that is to be exploited in a practical scenario over a set of data. Thus, in this stage, a statistical correlation technique is applied on the extracted Hessian data set from different frame pixel blocks in the video in order to establish the relationship that exists between them.

The Hessian matrix is denoted as pixel values from the 2nd order intensity variations surrounding a chosen pixel regionas $H(i,j)$. Then the correlation existing between neighboured frame pixel blocks are modelled using equation 3.

$$R_i = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\left(H_{i,j}^{t}-\bar{H}\right)\left(H_{i,j}^{t-1}-\bar{H}\right)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}\left(H_{i,j}^{t}-\bar{H}\right)^{2}\left(H_{i,j}^{t}-\bar{H}\right)^{2}}} \qquad (3)$$

Where t represents the t^{th} frame and $\overline{H}$ is the average of the Hessian matrices for all frames t_i. The statistical correlation of the Hessian matrix in an inpainted region is usually changed in terms of increment or decrement depending on the kind of inpainting forgery that is done on the video.

4.3 Experimental Results and Analysis

In this section, the result of this experiment is presented. The data set used for the experimental testing was obtained (Hsu et al., 2008), (Zhang et al., 2009)and others created from video downloaded from Surrey University for Forensic Analysis (SULFA) (Qadir, Yahaya, & Ho, 2012), for the initial simulation of these experiments. These datasets were processed and analyzed in order to address the problem of video inpainting forgery detection as mentioned in chapter one of this thesis. There are two objectives behind the use of datasets from different sources. The first reason is to use the different dataset for the initial simulation of our experiments in order to determine how the use of Hessian matrix features can effectively determine inpainting forgery in a

digital video. The second reason is for performance evaluation of our proposed technique. These goals were achieved successfully. The results shown in this section prove the success of the use of statistical correlation of Hessian matrix features for video inpainting forgery detection.

4.3.1 Data Set

To provide a justification of the efficacy for this proposed video inpainting detection technique, a series of experiments were performed on a total of 4802 frames from 20 different test videos that were obtained from the (Hsu et al., 2008; Qadir et al., 2012; Zhang et al., 2009). Two different inpainting schemes namely texture and structure inpainting was performed on each video separately. Table 4.1 shows a summary of the test videos with respect to the number of frames for independent video and the video frame resolution. The varying number of frame is used as to test how robust the proposed technique is interms of different video length while the varying frame resolution is to test the robustness of the proposed technique with respect to different video quality.

Table 4.1: Summary of Test Videos

Test Video	No of Frames	Frame Resolution
Video Sequence 1	330	320 × 240
Video Sequence 2	190	720 × 480
Video Sequence 3	200	720 × 480
Video Sequence 4	162	320 × 240
Video Sequence 5	200	480 × 720
Video Sequence 6	200	240 × 320
Video Sequence 7	200	240 × 320
Video Sequence 8	200	240 × 320
Video Sequence 9	340	240 × 320
Video Sequence 10	528	240 × 320
Video Sequence 11	200	240 × 320
Video Sequence 12	200	240 × 320
Video Sequence 13	200	240 × 320
Video Sequence 14	512	240 × 320
Video Sequence 15	320	240 × 320
Video Sequence 16	180	240 × 320
Video Sequence 17	120	240 × 320
Video Sequence 18	120	240 × 320
Video Sequence 19	200	240 × 320
Video Sequence 20	200	240 × 320

4.3.2 Results of Experiments on Video Inpainting Detection

In this section, the result of this experiment is discussed for the detection of texture and structure video inpainting forgery in the form of histograms of correlation for the Hessian matrix features that are extracted from the test videos. These histograms of correlation are computed and analysed for variation of the Hessian correlation across video frame pixel blocks at a threshold of 0.9956. Furthermore, the correct inpainting detection precision and false positive detection rates for each video sequence are also reported. Finally, the regions of inpainting are identified.

4.3.2.1 Result of Hessian Correlation for Texture Synthesis Inpainting Detection

The Figures 4.4 to 4.23 shows the result of histograms of Hessian correlation between successive frame blocks for the 20 test videos that are tampered using texture based inpainting at a threshold of 0.9956. The diamond slopes in the histogram of

correlations represent the non-tampered Hessian blocks and the circled slopes represent the tampered Hessian blocks.

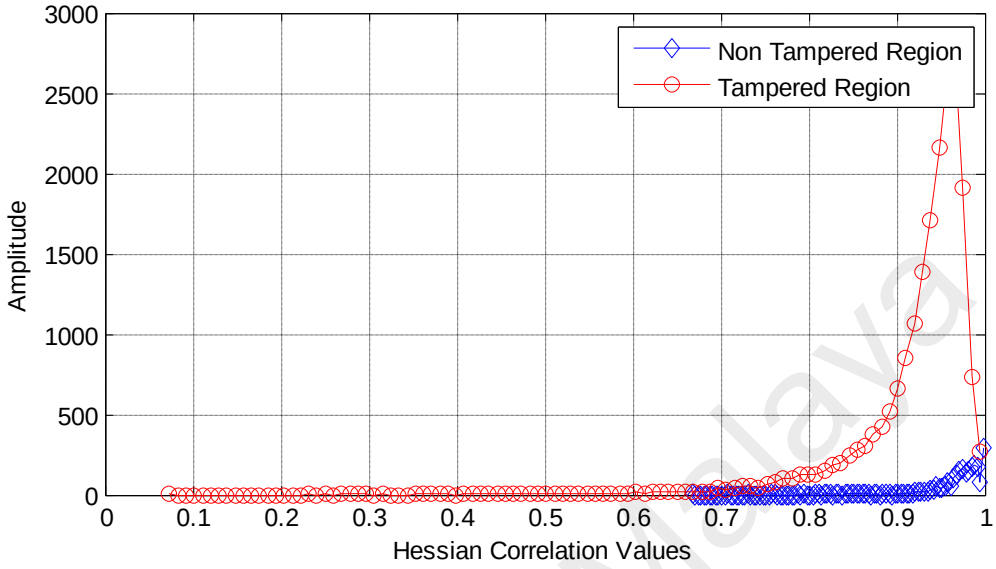

Figure 4.4: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 1

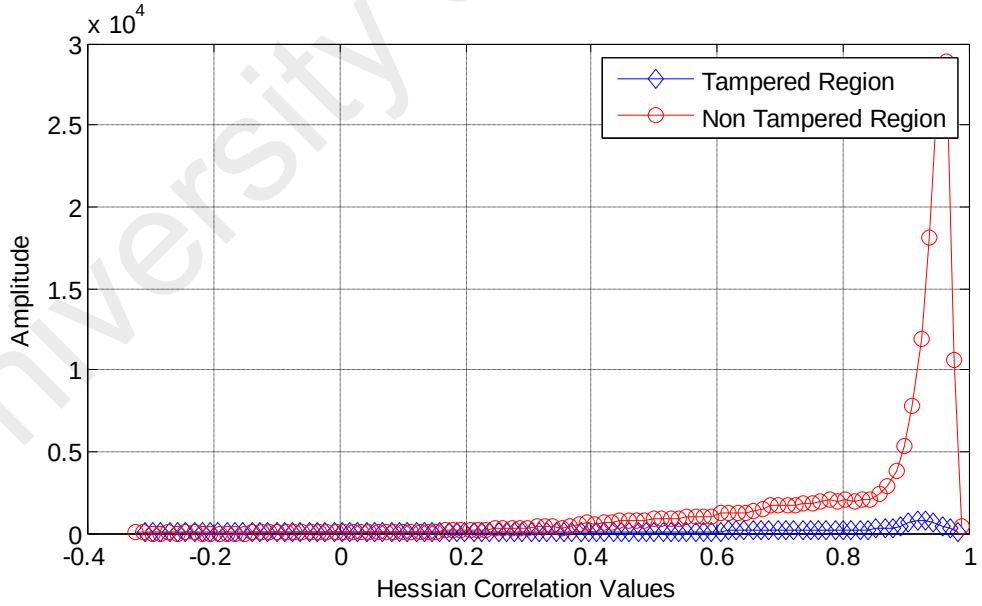

Figure 4.5: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 2

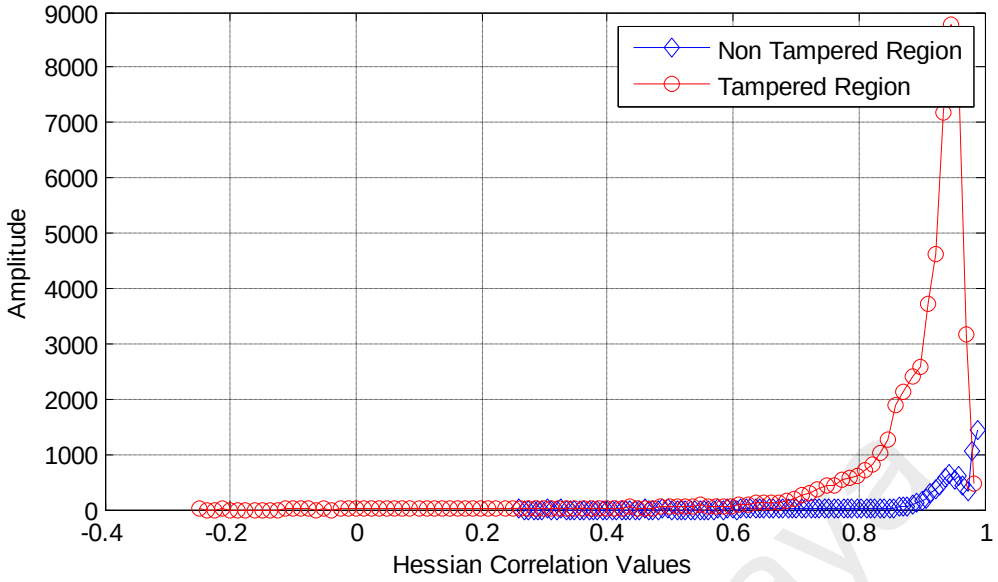

Figure 4.6: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 3

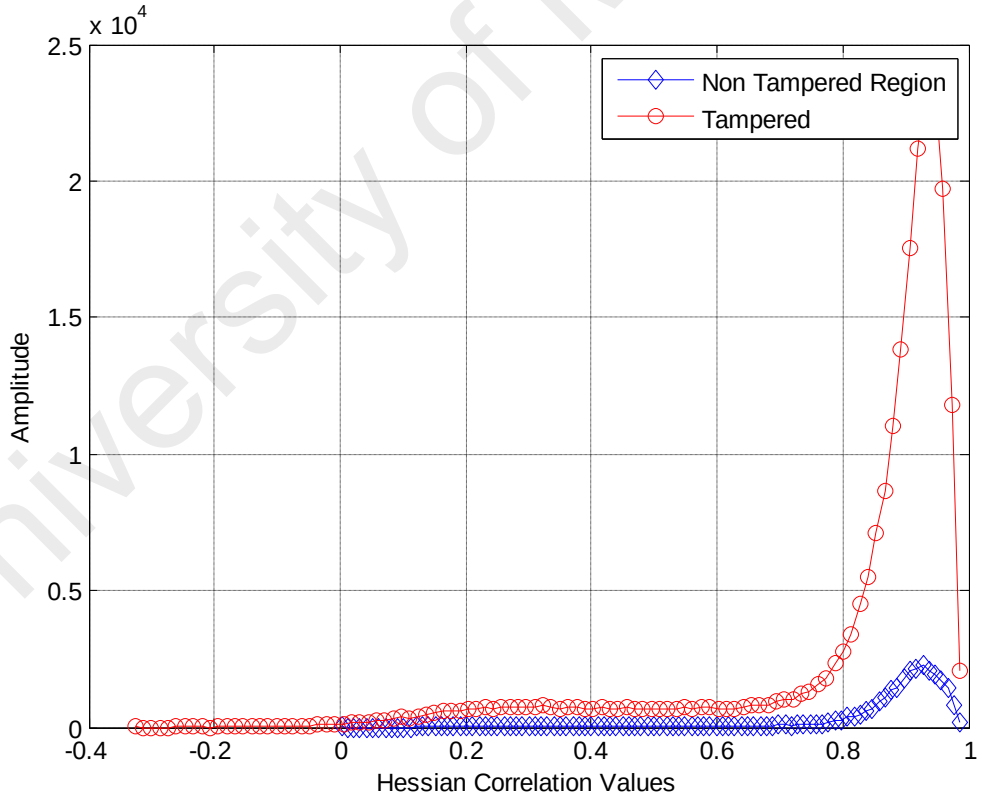

Figure 4.7: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 4

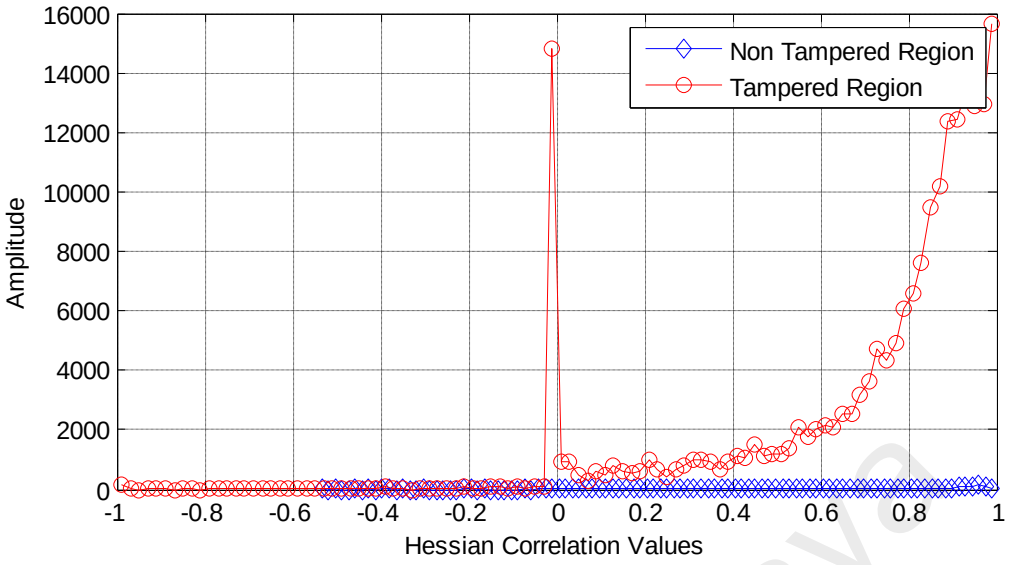

Figure 4.8: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 5

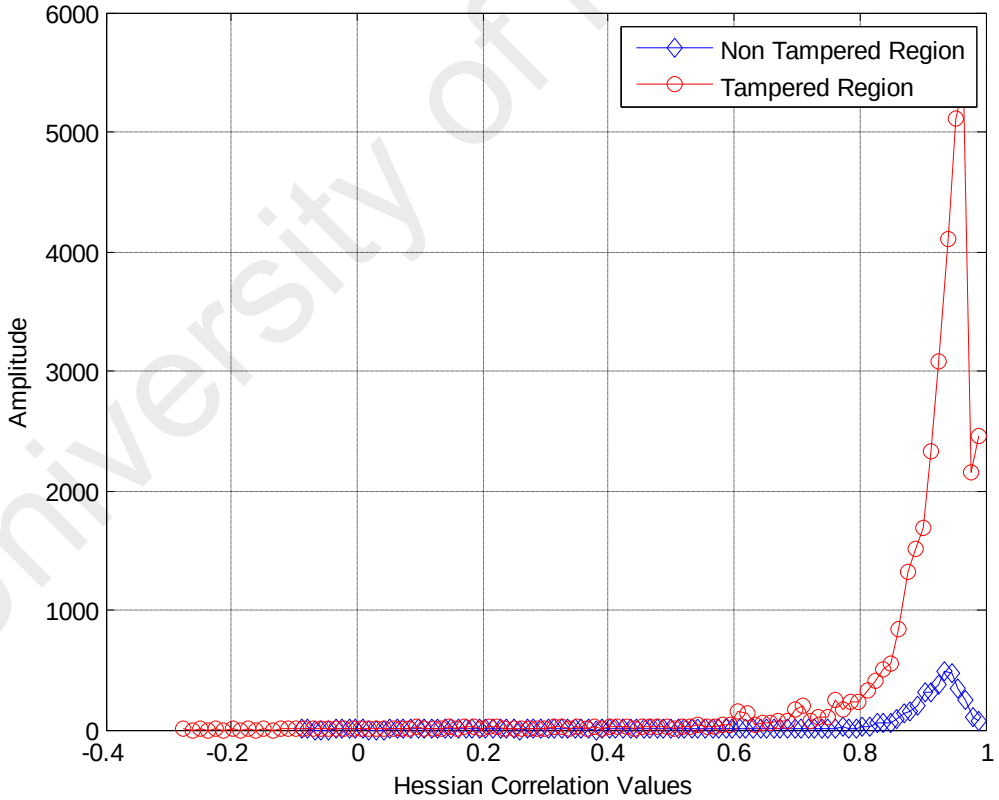

Figure 4.9: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 6

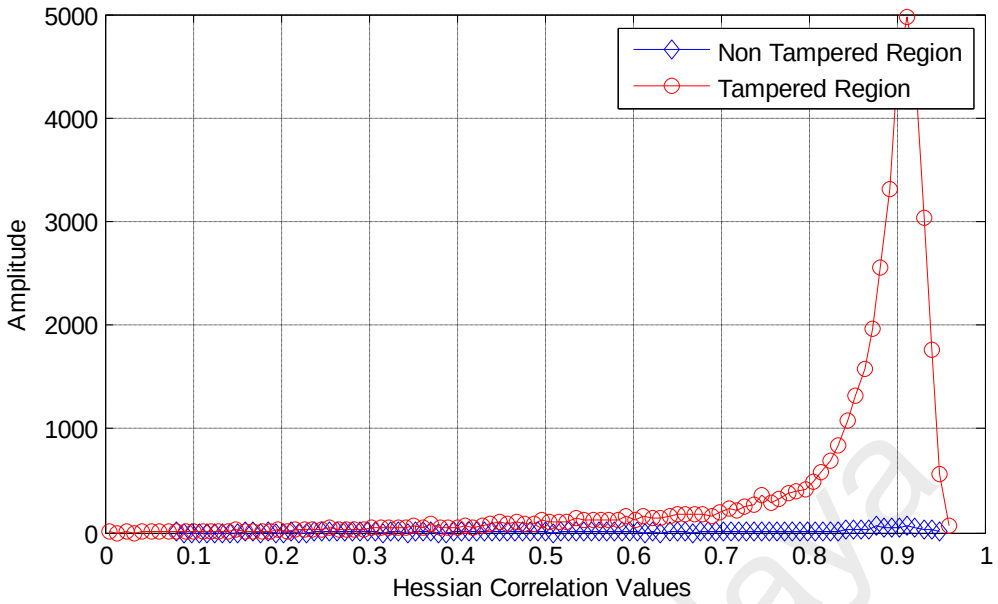

Figure 4.10: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 7

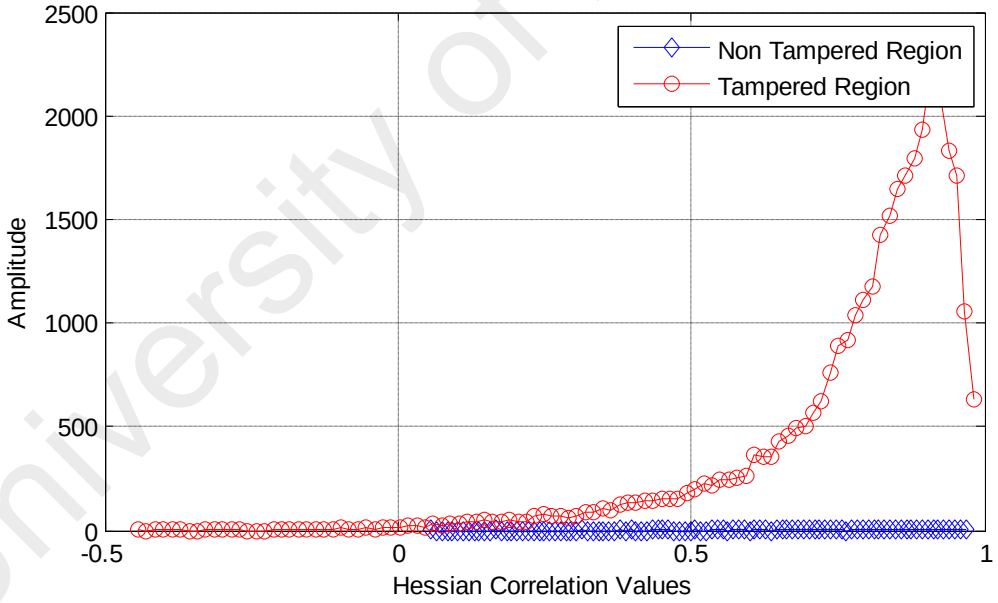

Figure 4.11: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 8

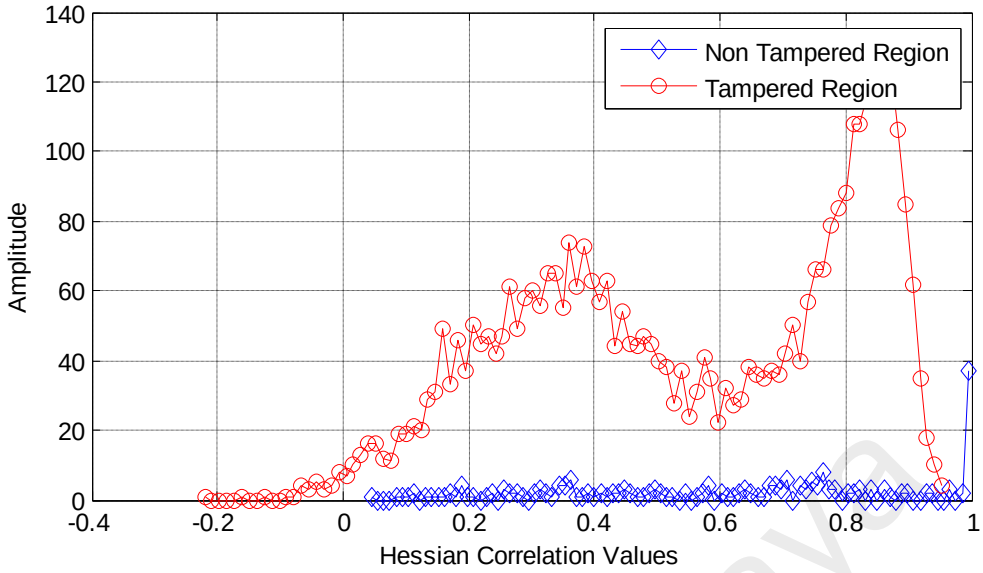

Figure 4.12: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 9

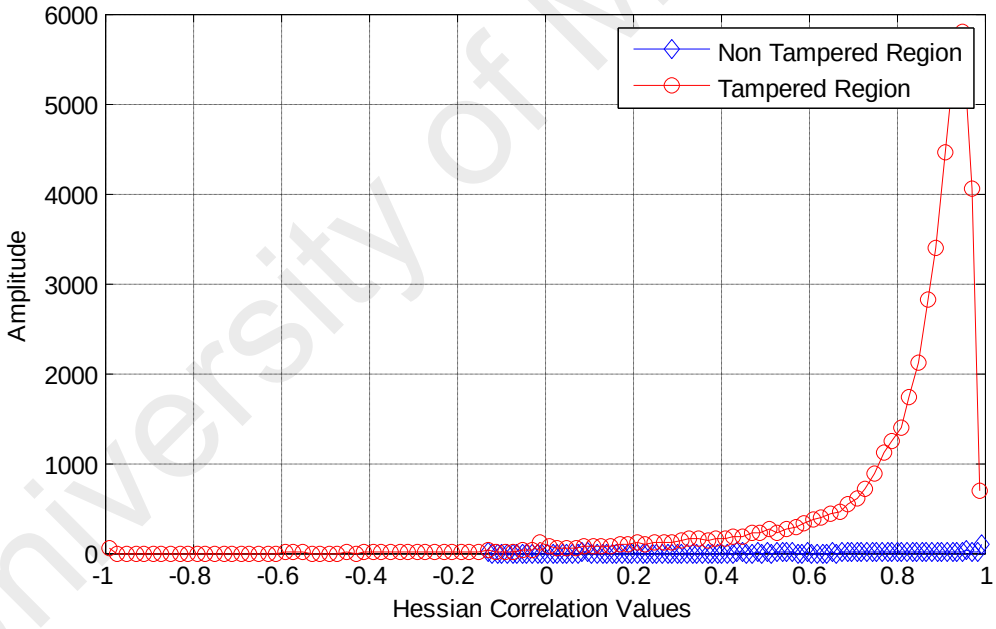

Figure 4.13: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 10

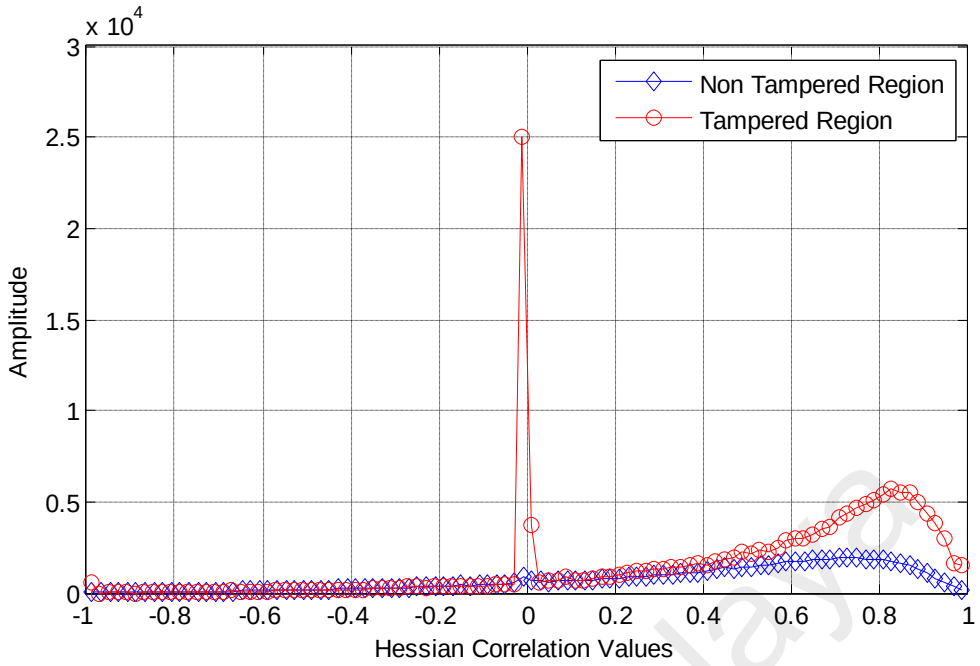

Figure 4.14: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 11

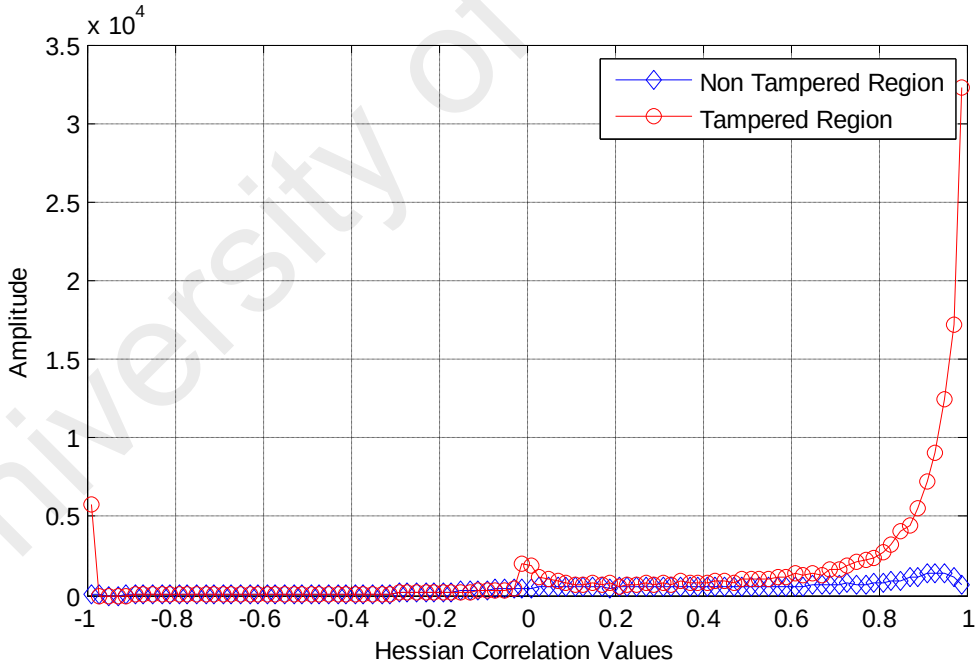

Figure 4.15: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 12

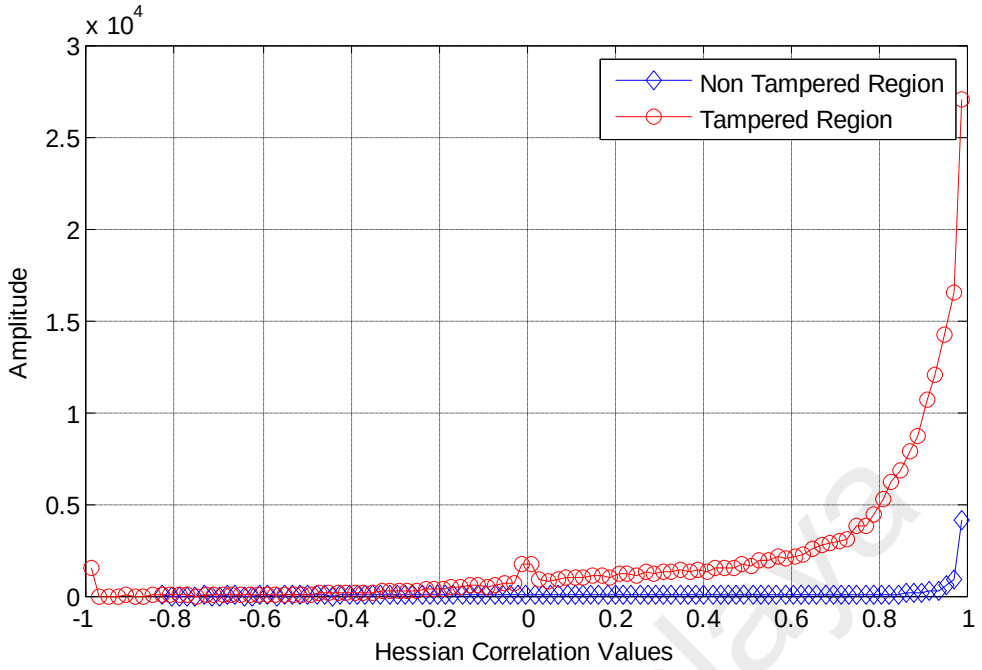

Figure 4.16: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 13

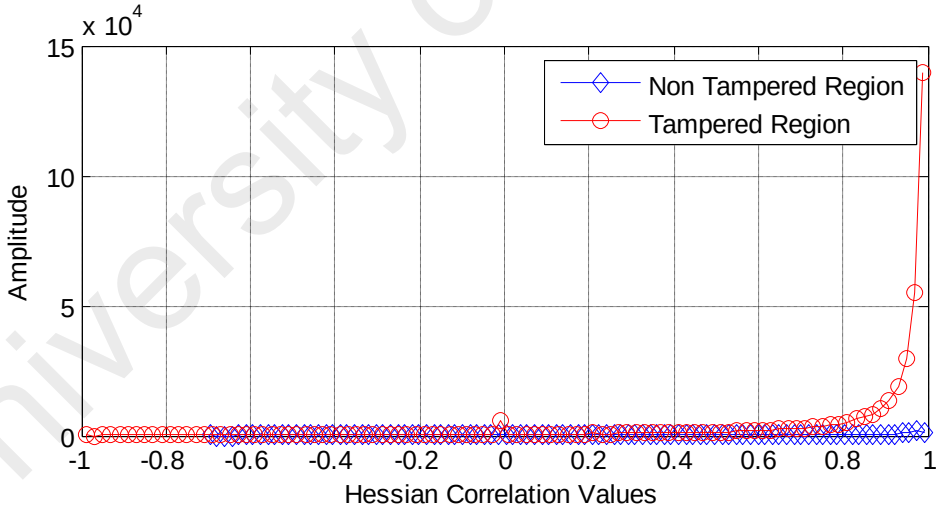

Figure 4.17: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 14

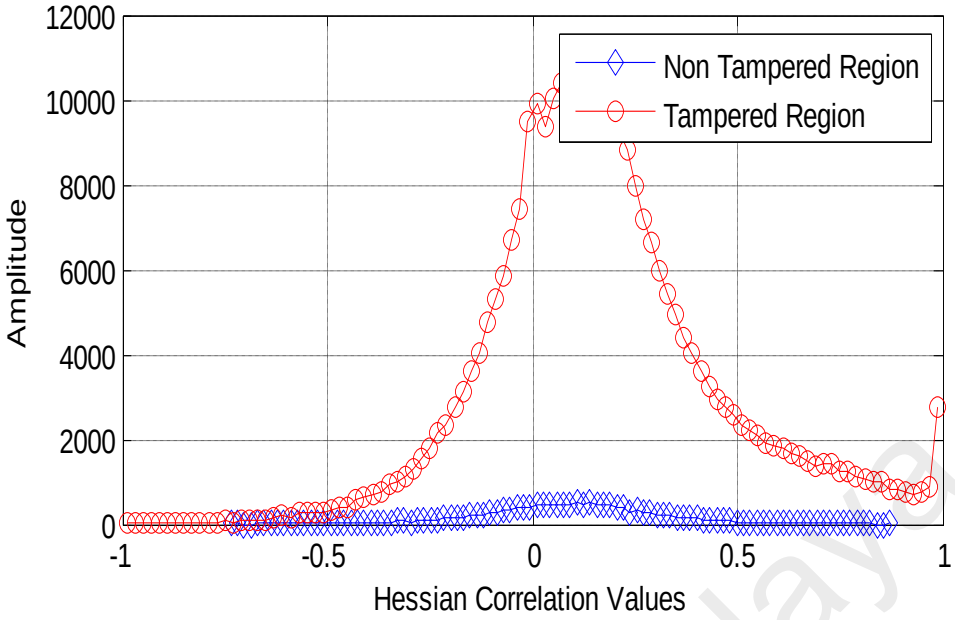

Figure 4.18: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 15

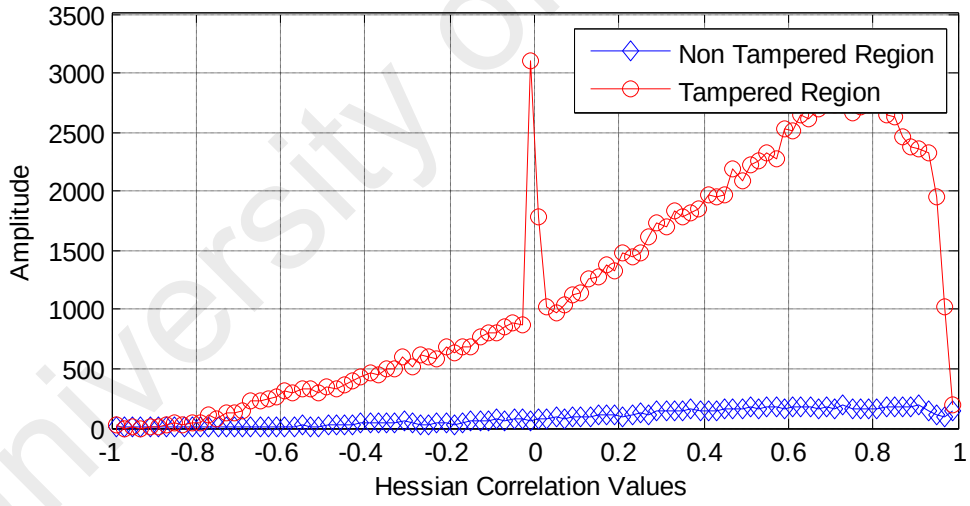

Figure 4.19: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 16

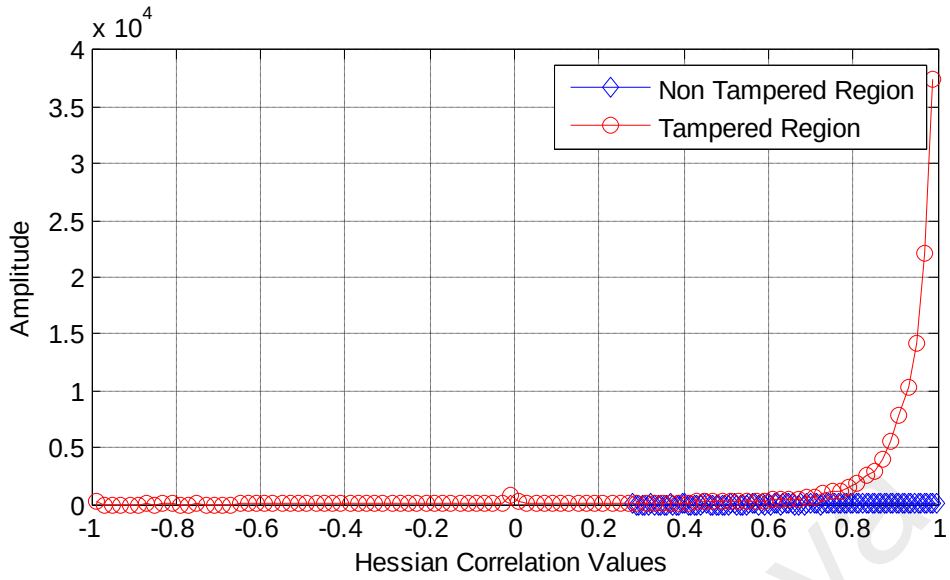

Figure 4.20: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 17

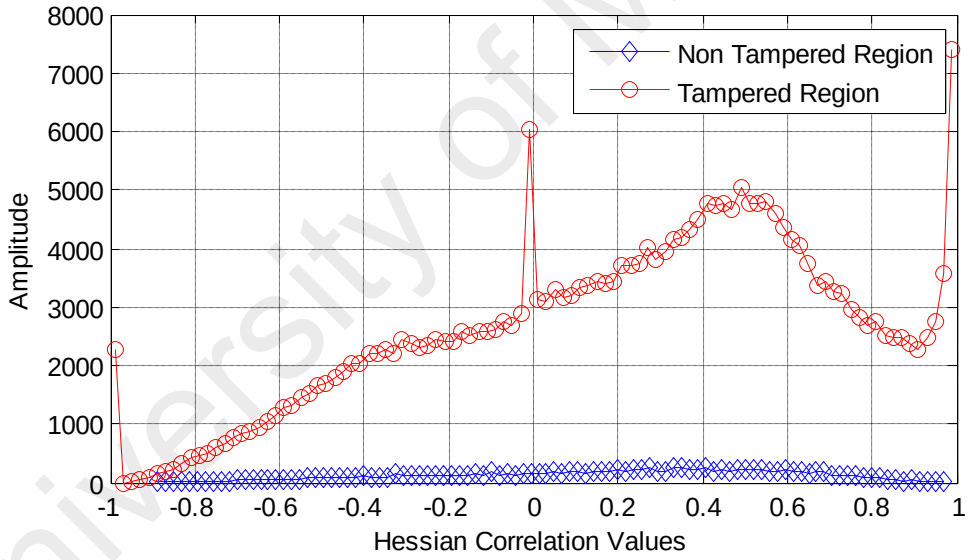

Figure 4.21: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 18

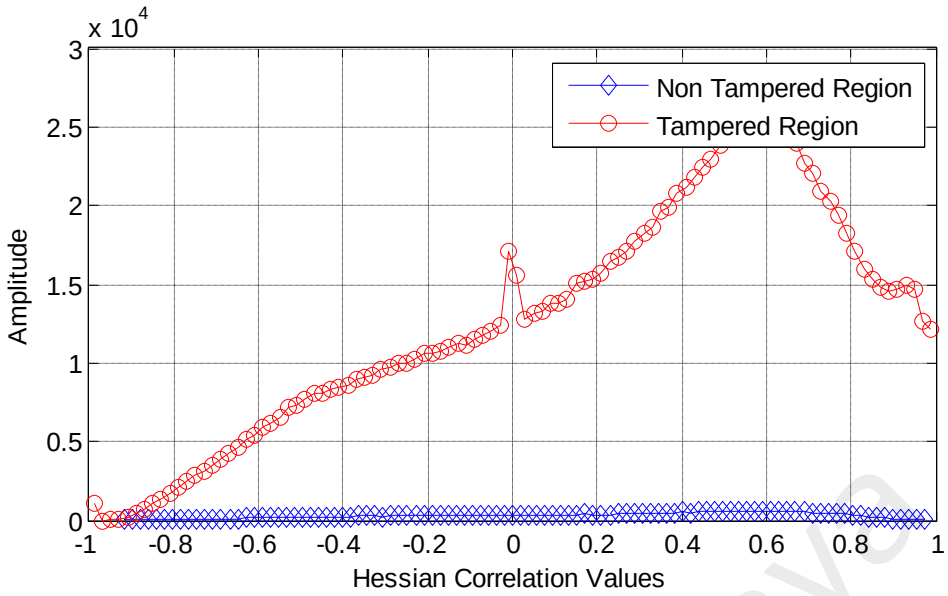

Figure 4.22: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 19

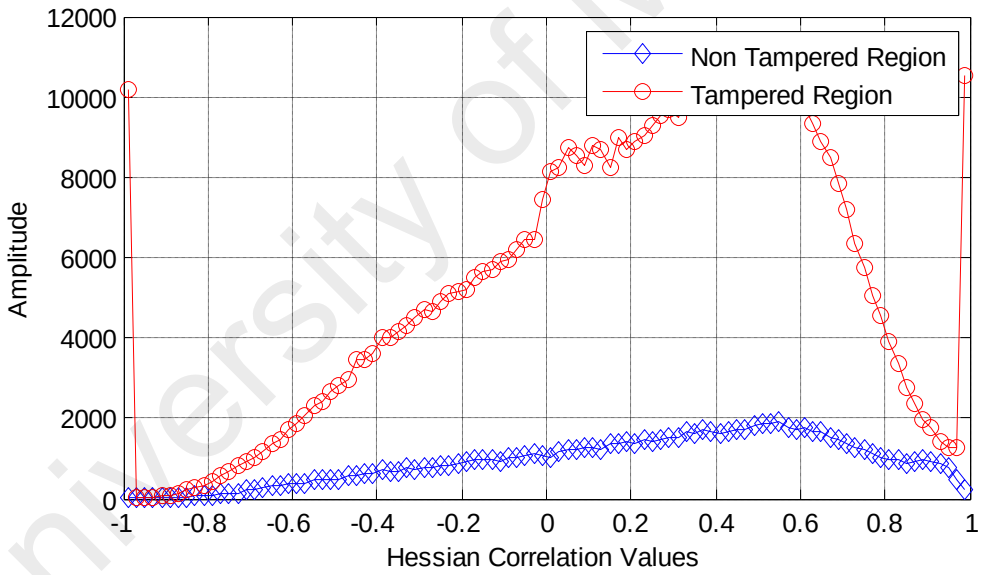

Figure 4.23: Hessian Correlation between Successive Video Frame Blocks for Texture Based Inpainting for Test Video 20

It will be observed from Figures 4.4 to 4.23 for texture based inpainting that the Hessian matrix feature correlations of the two slopes between inpainted and non inpainted frame blocks are remarkably different in terms of the peak of their amplitude.This remarkable difference of texture based inpainting in amplitude variation between the Hessian correlations of inpainted and non inpainted regions is because of

the disagreement between the video homographic key points and the fundamental intensity matrix in the inpainted regions. This disagreement creates a very high alignment error that affects the intensity variation around an inpainted region, as such creating a significant difference in the slope of correlation between inpainted and non inpainted region. These techniques exploit the Hessian matrix variation between the video frame blocks for inpainting detection.

4.3.2.2 Result of Hessian Correlation for Structure Based Inpainting Detection

The Figures 4.24 to 4.43 shows the result of histograms of Hessian correlation between successive frame blocks for the 20 test videos that are tampered using structure based inpainting at a threshold of 0.9956. The diamond slopes in the histogram of correlations represent the non-tampered Hessian blocks and the circled slopes in the histogram of correlations represent the tampered Hessian blocks.

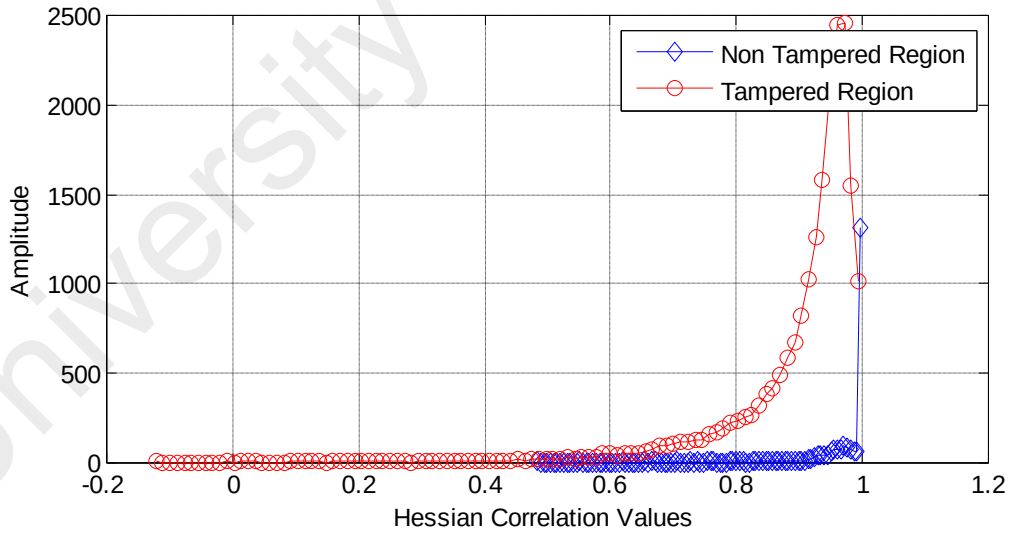

Figure 4.24: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 1

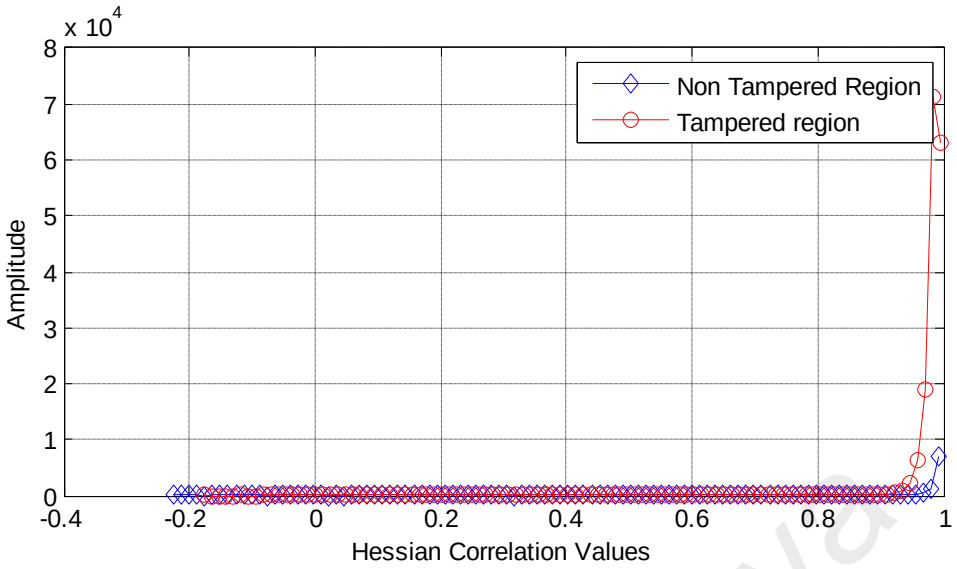

Figure 4.25: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 2

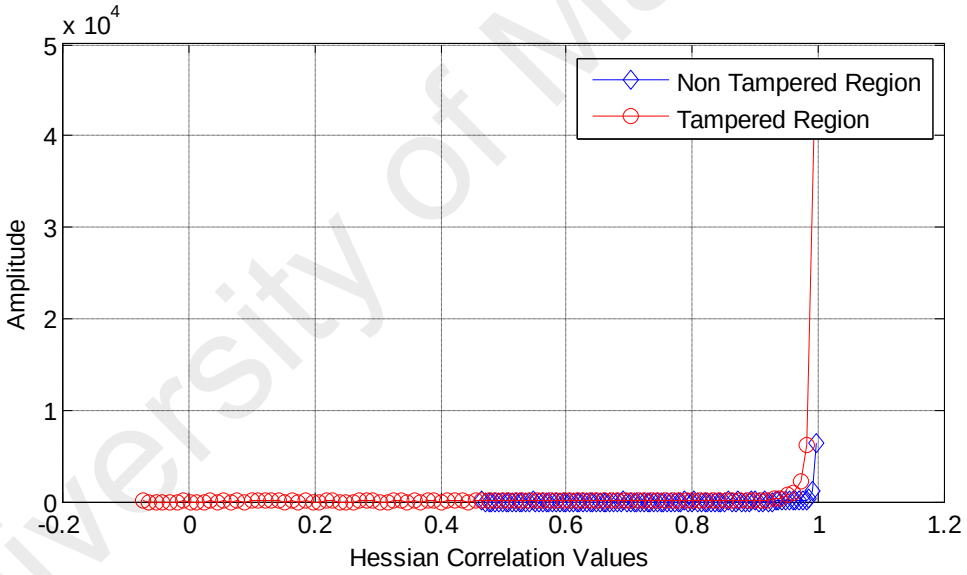

Figure 4.26: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 3

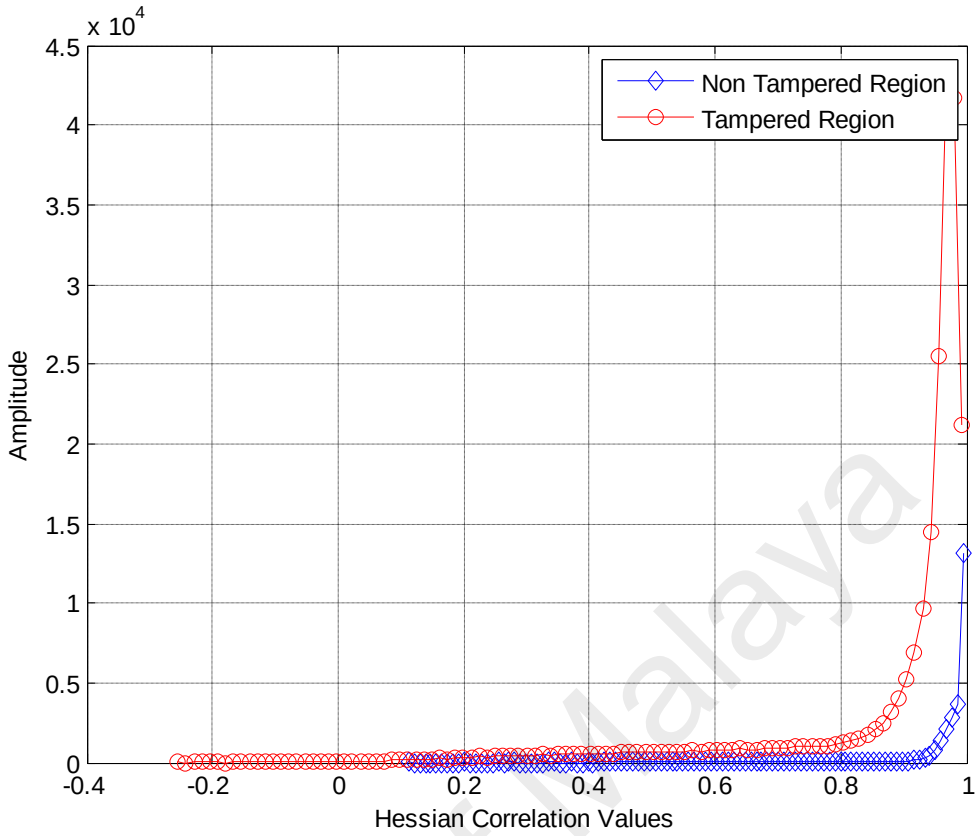

Figure 4.27: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 4

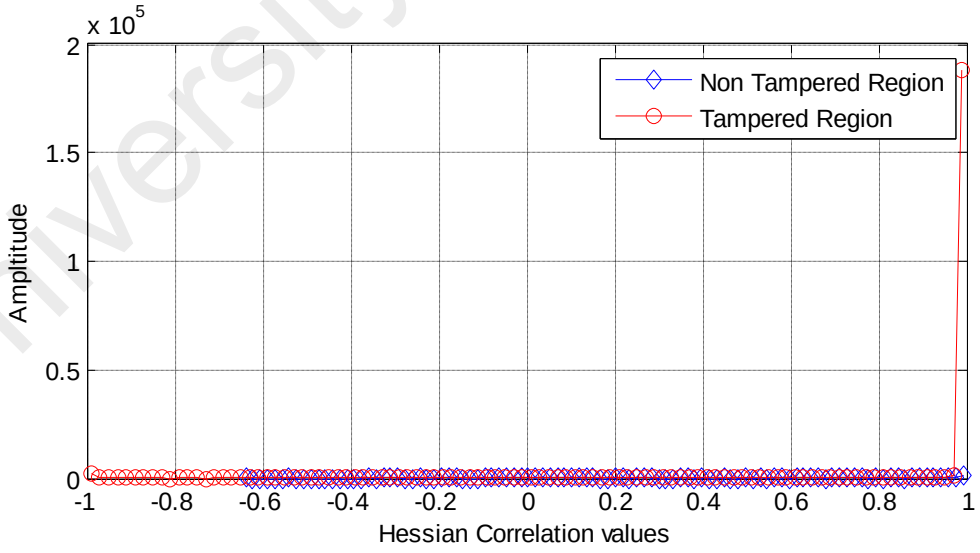

Figure 4.28: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 5

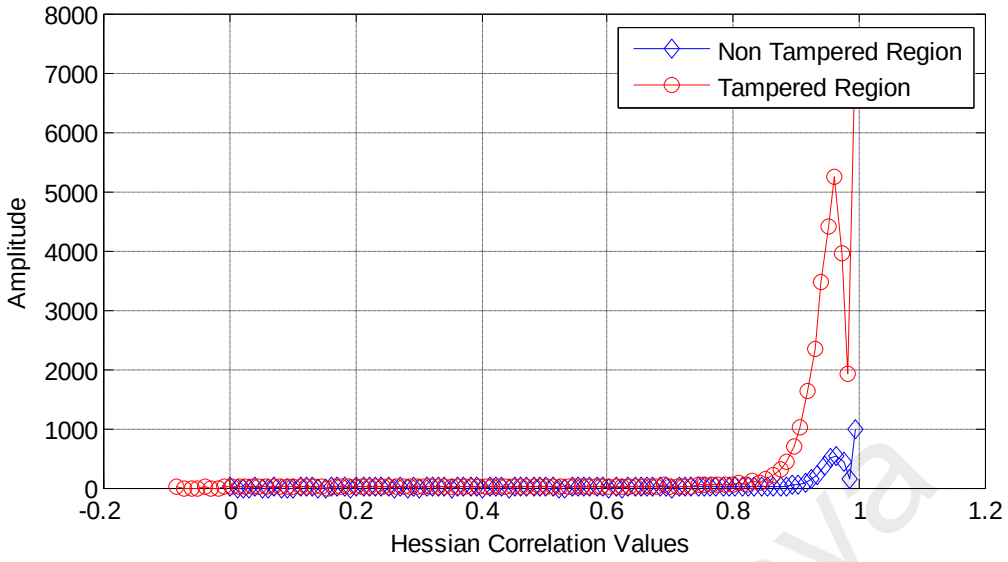

Figure 4.29: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 6

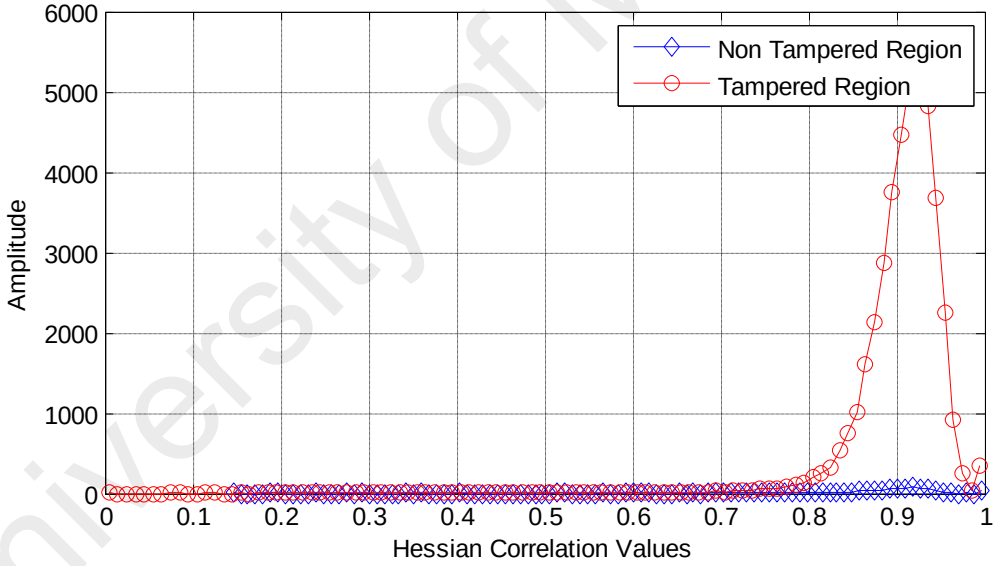

Figure 4.30: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 7

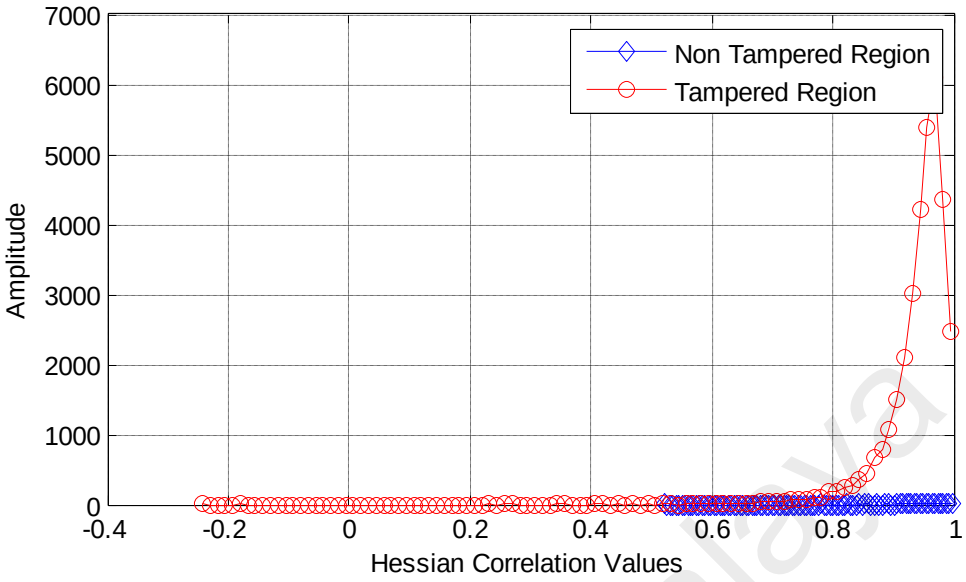

Figure 4.31: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 8

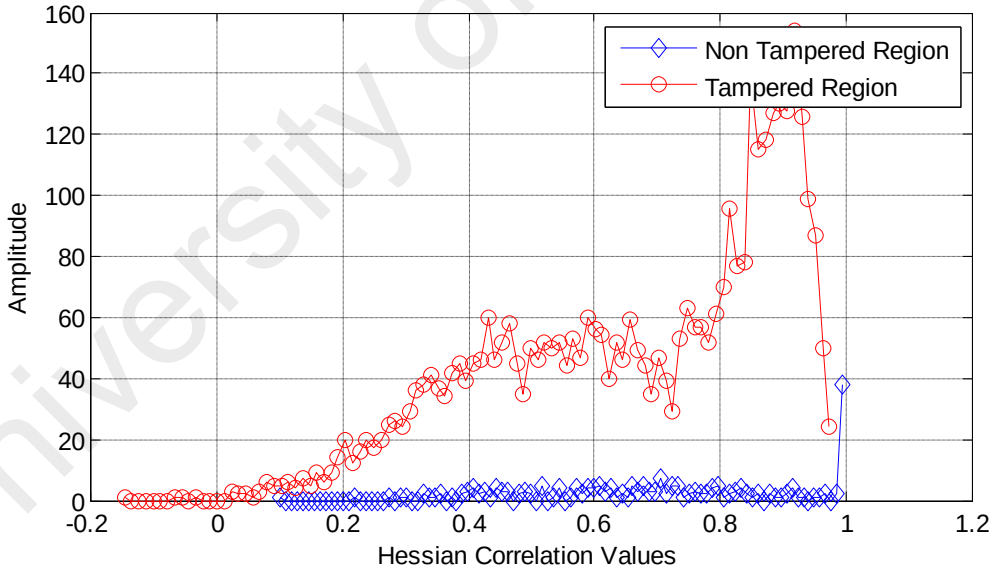

Figure 4.32: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 9

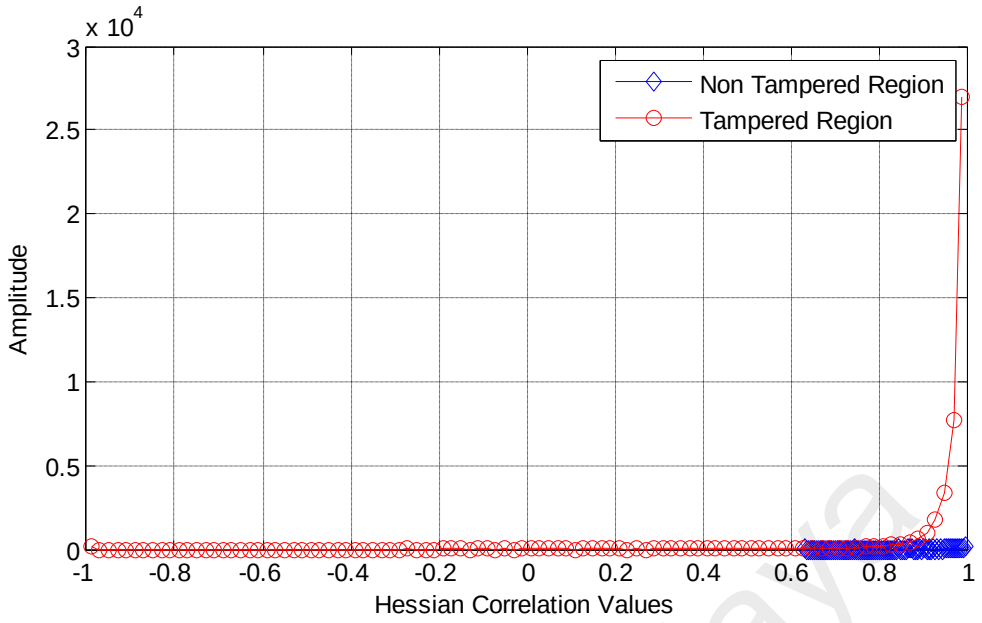

Figure 4.33: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 10

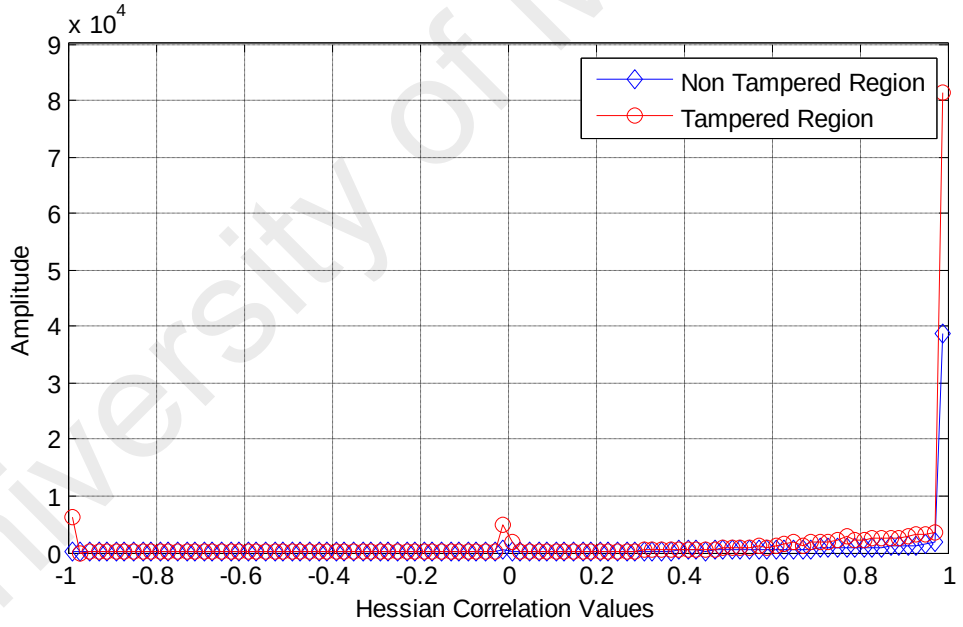

Figure 4.34: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 11

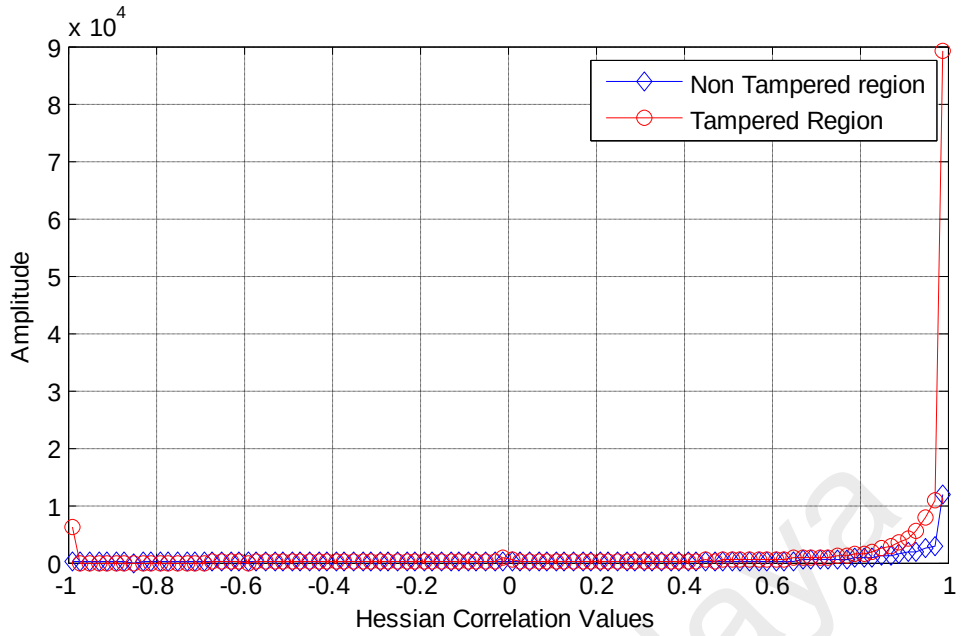

Figure 4.35: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 12

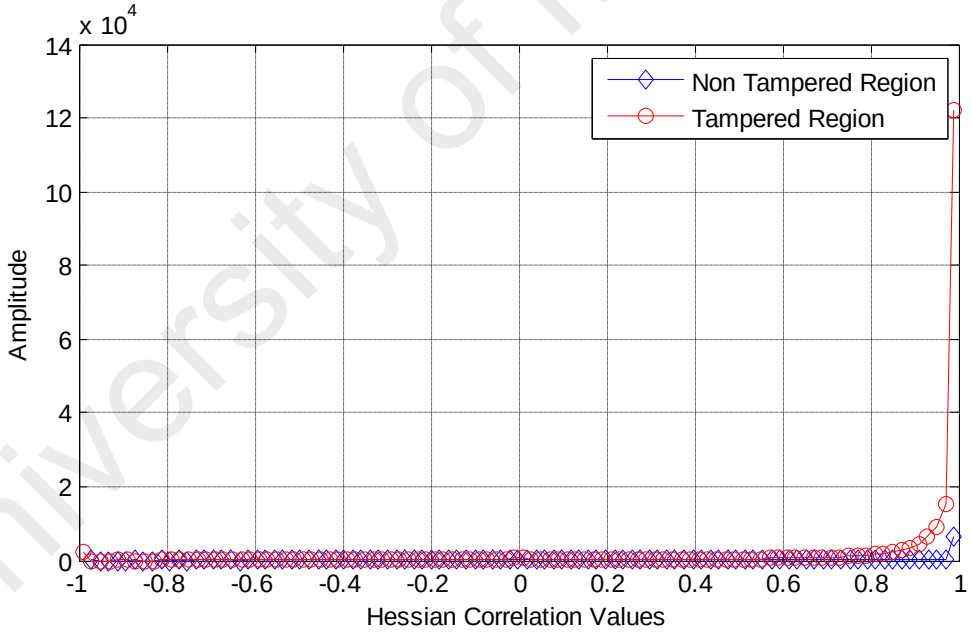

Figure 4.36: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 13

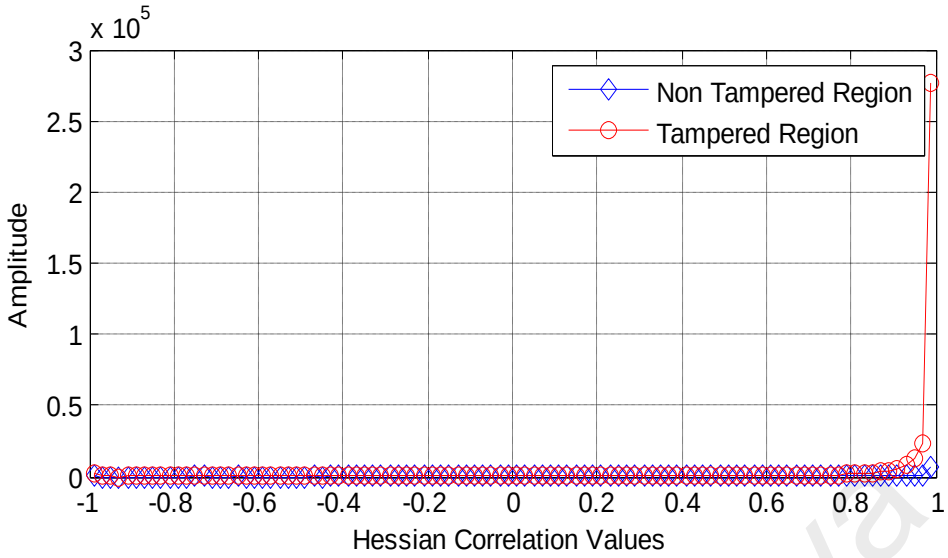

Figure 4.37: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 14

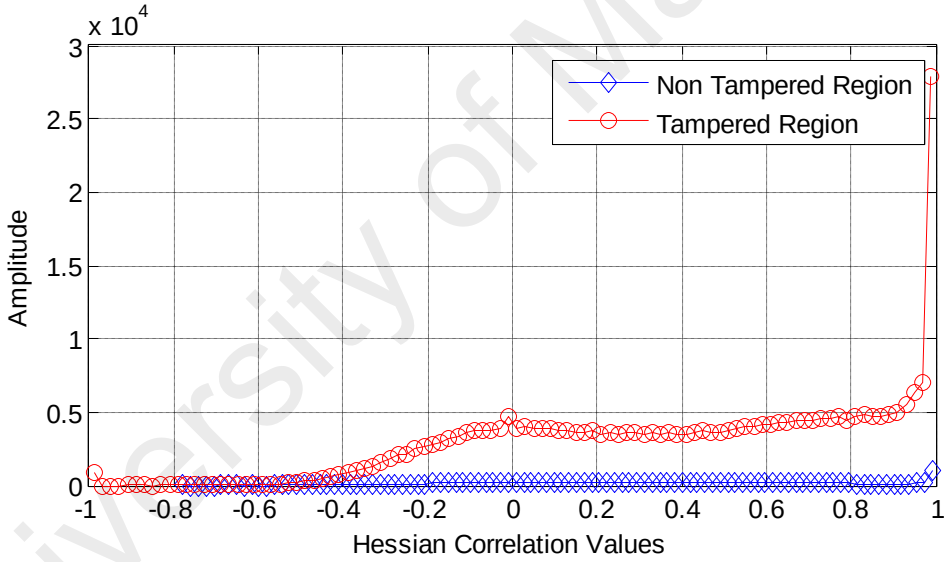

Figure 4.38: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 15

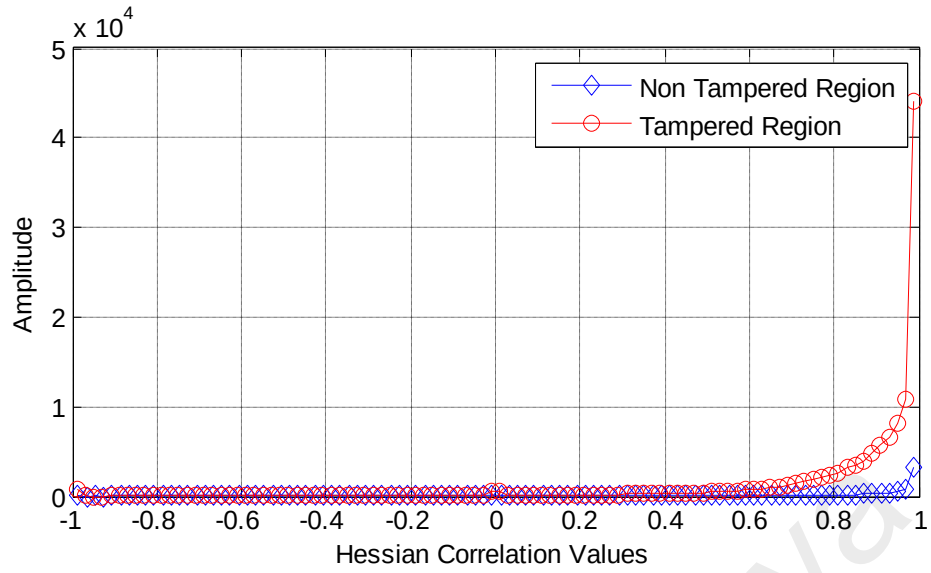

Figure 4.39: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 16

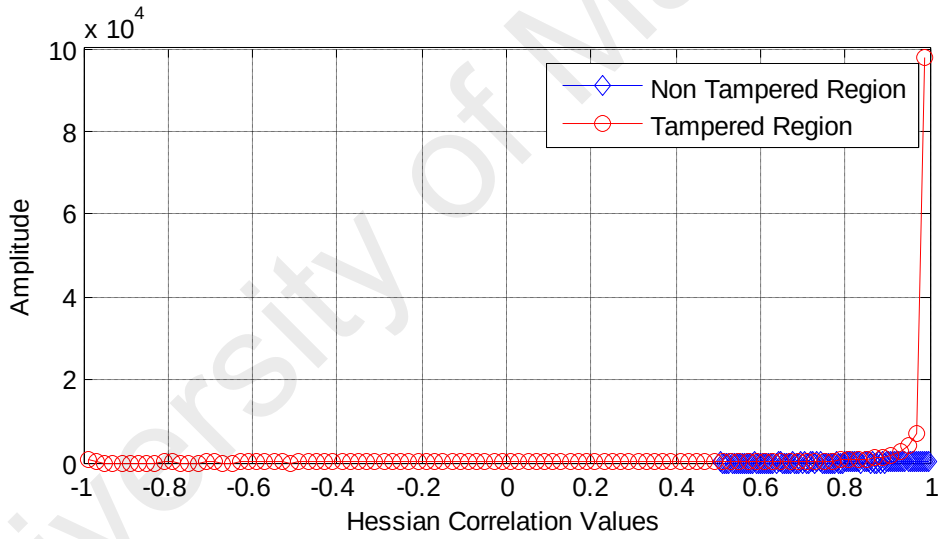

Figure 4.40: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 17

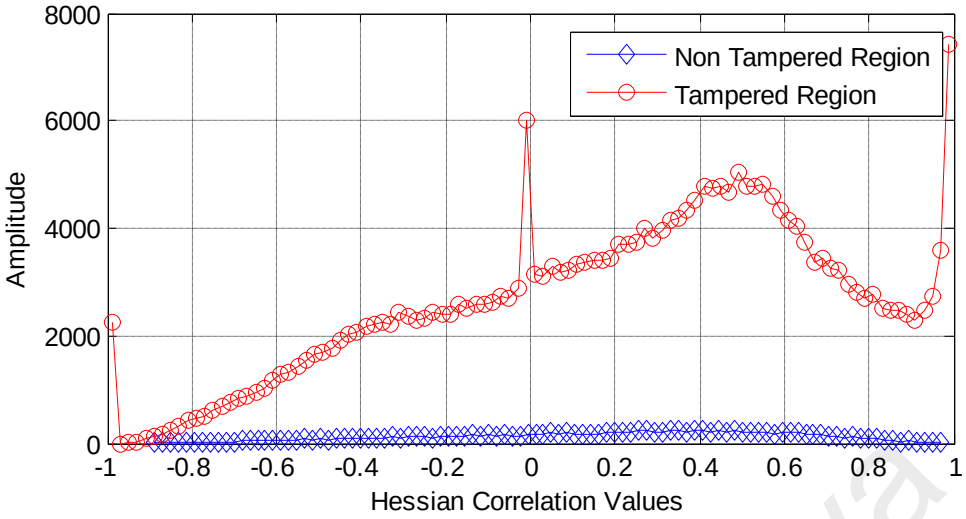

Figure 4.41: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 18

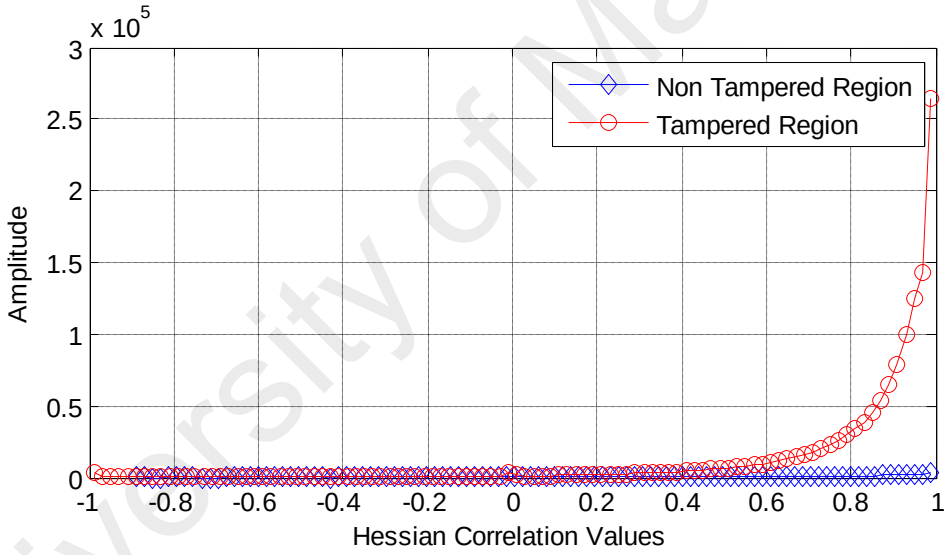

Figure 4.42: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 19

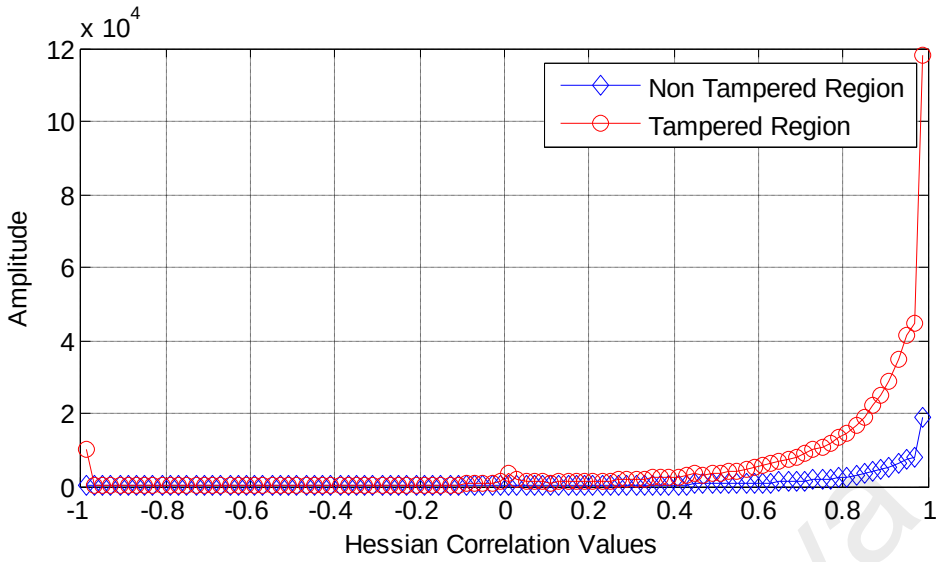

Figure 4.43: Hessian Correlation between Successive Video Frame Blocks for Structure Based Inpainting for Test Video 20

However, it will also be observed from Figures 4.24 to 4.43 for thestructure inpainting, that the Hessian matrix feature correlations of the two slopes between inpainted and non inpainted frame blocks are slightly different in terms of the peak of their amplitude unlike the texture based inpainting. This slight difference of structure based inpainting in amplitude variation between the Hessian correlations of inpainted and non inpainted regions is because of the high agreement between the video homographic key points and the fundamental intensity matrix in the inpainted regions. This agreement reduces the alignment error that affects the intensity variation around an inpainted region, as such creating only a slightest difference in the slope of correlation between inpainted and non inpainted region. This variation is a good clue for tamper detection using our proposed technique.

4.3.3 Inpaint Region Identification

Inpainted regions in the video are located by isolating the inpainted region from the non inpainted ones through the analysis of the video frame block level Hessian correlations. In order to accomplish this isolation, a classification scheme is defined to determine whether a block within a video frame has been inpainted or not based on the

correlation values R obtained fromtemporally neighboring blocks using an Otsu threshold mechanism. The classification is defined as follows in equation 4:

$$Class_n = \begin{cases} Inpainted\ Block & |R > predefined\ Threshold| \\ Non\ Inpainted\ Block & Otherwise \end{cases} \quad (4)$$

If the correlation R is greater than the predefined threshold, the pixel block is considered to be inpainted. However, if the correlation R is less than the predefined threshold, the pixel block is not considered as inpainted. The process is repeated for all remaining pixel blocks in the video frames. The classification results for different video sequence from the dataset used for our experiments are shown in Figures 4.44 to 4.54.The white region in the detection row of each Figure indicates regions for which an object has been removed.

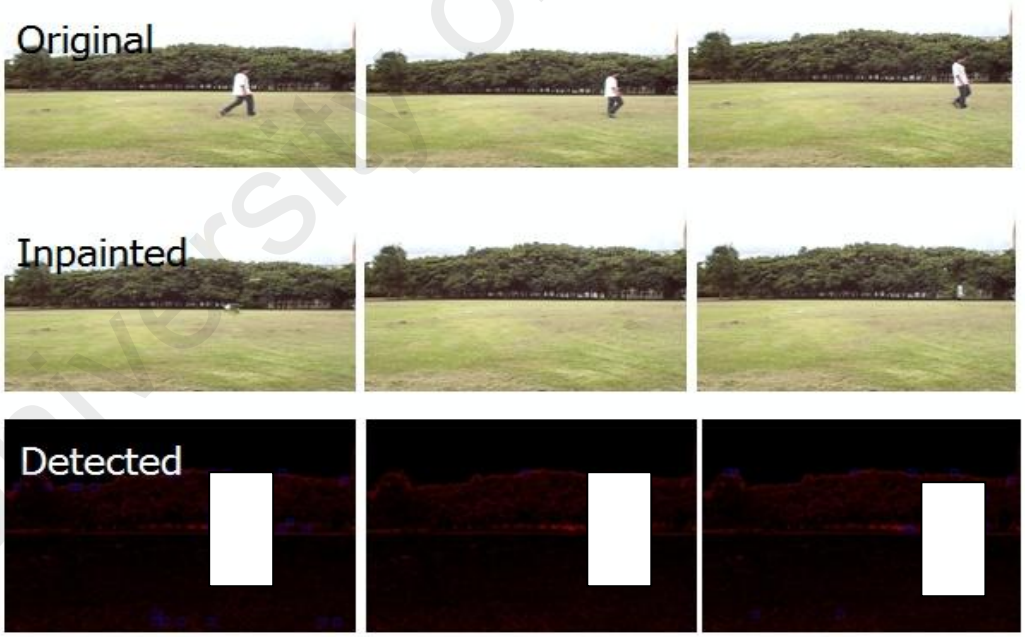

Figure 4.44: Region Inpaint Localization for Test Video 1

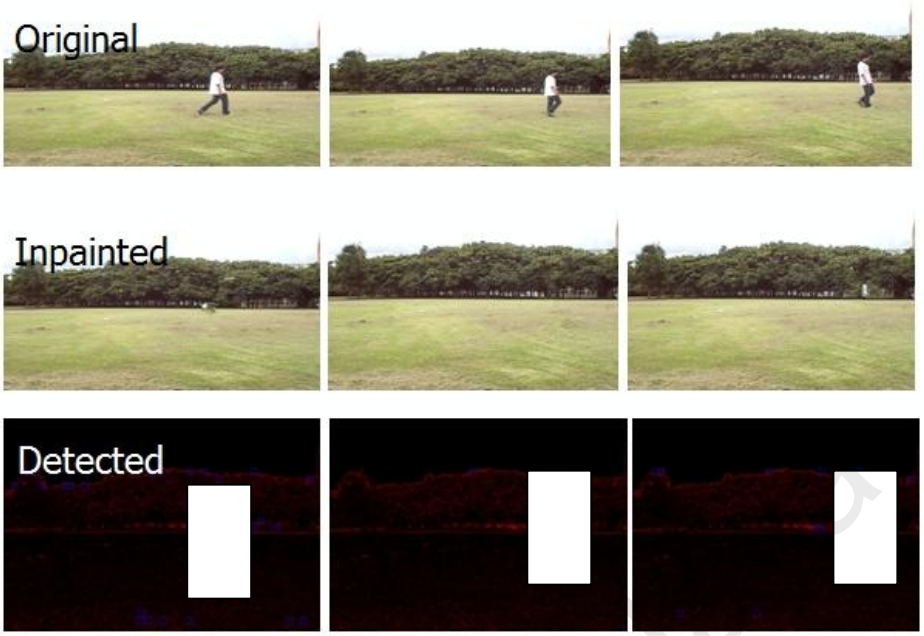

Figure 4.45: Region Inpaint Localization for Test Video 2

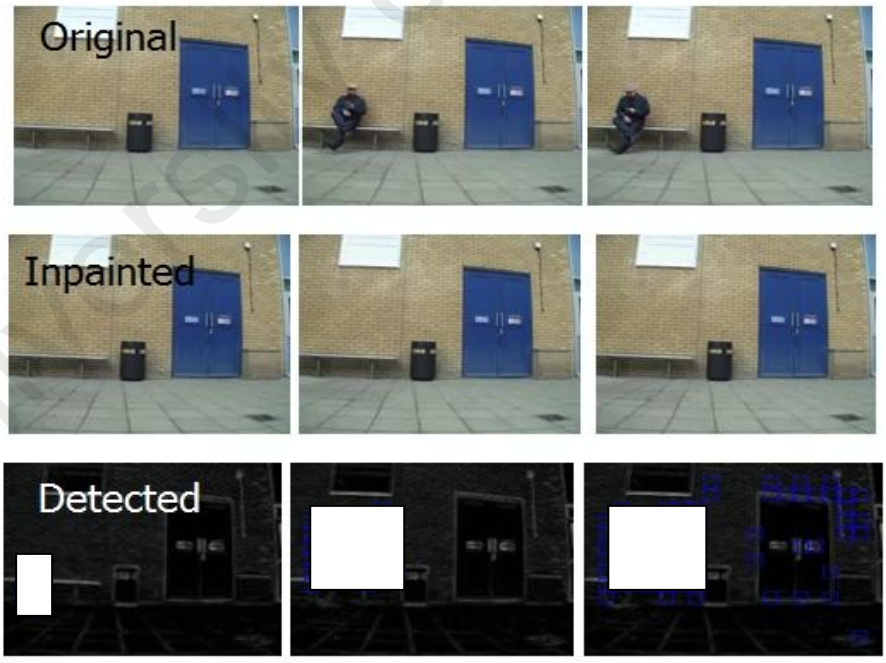

Figure 4.46: Region Inpaint Localization for Test Video 3

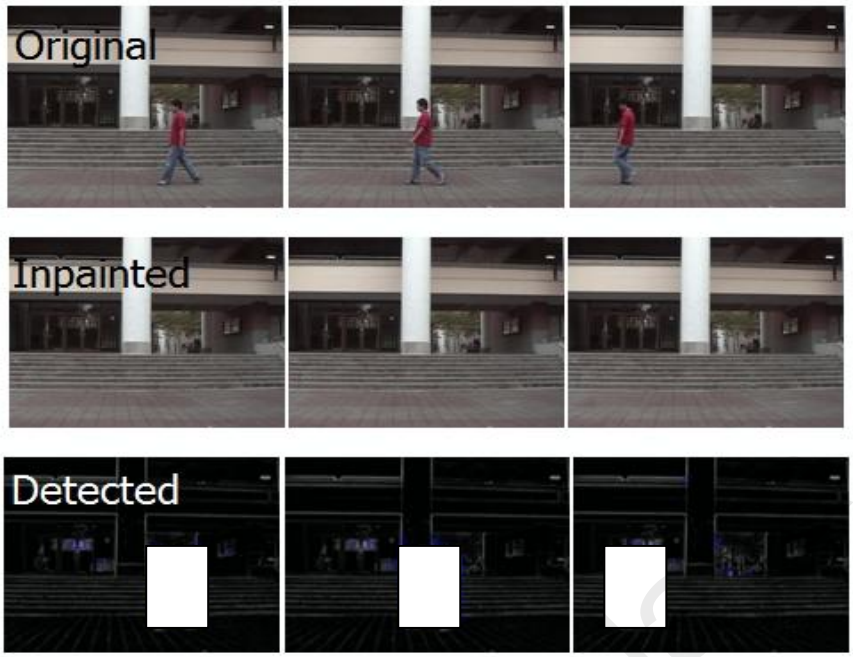

Figure 4.47: Region Inpaint Localization for Test Video 4

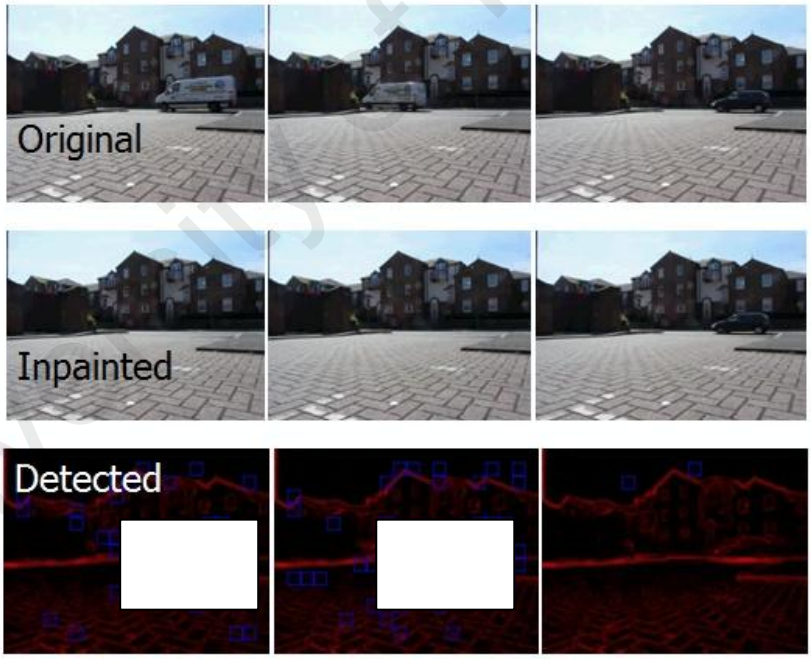

Figure 4.48: Region Inpaint Localization for Test Video 5

Figure 4.49: Region Inpaint Localization for Test Video 6

Figure 4.50: Region Inpaint Localization for Test Video 7

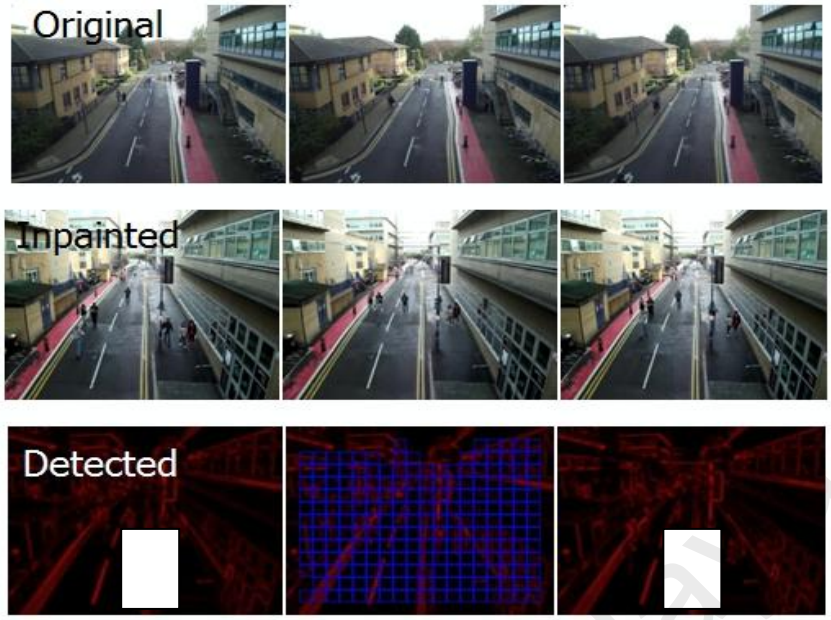

Figure 4.51: Region Inpaint Localization for Test Video 8

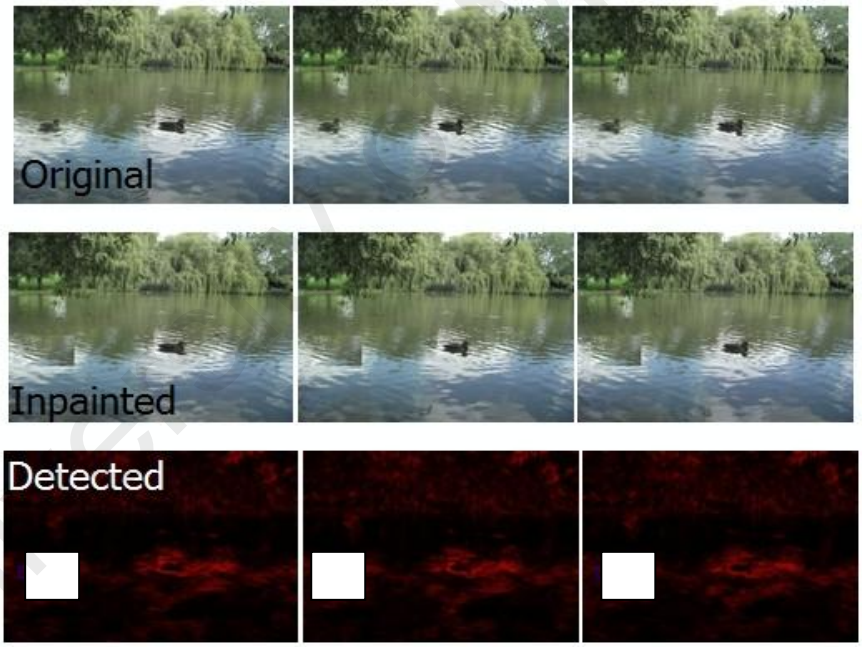

Figure 4.52: Region Inpaint Localization for Test Video 9

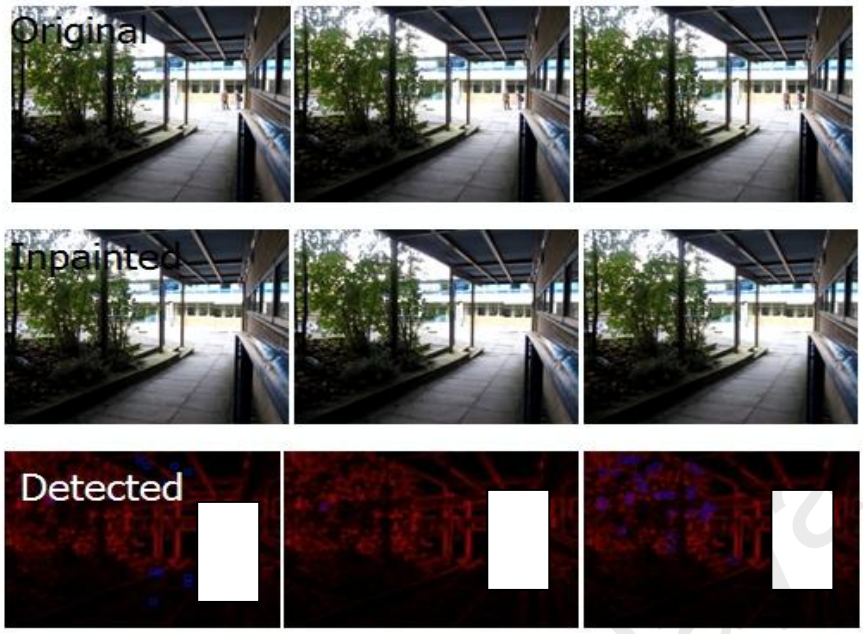

Figure 4.53: Region Inpaint Localization for Test Video 10

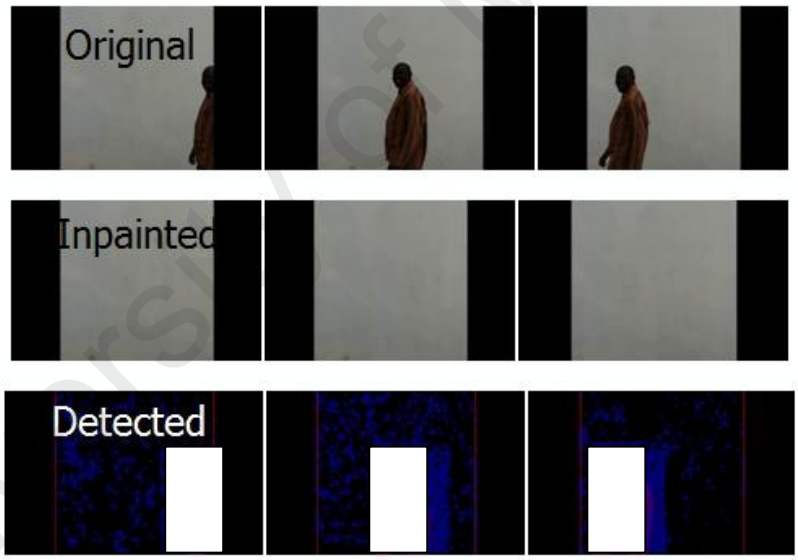

Figure 4.54: Region Inpaint Localization for Test Video 11

4.3.4 Performance Evaluation Metrics

In this section, a discussion is provided on the performance metrics used in most of the work from the literature that is related to this domain. The performance metrics includes: detection precision rate and false positive rate of the proposed detection techniques. In this work, the aforementioned metrics are considered as the measure of performance for our video inpainting detection technique.

Precision is one of the basic performance measures that are used for the evaluation of a search and identification problem. In a general definition, precision which is also referred to as a prediction of possible true values is the ratio of true relevant retrieved instances with respect to a total number of relevant and irrelevant data recorded during an experiment. However, in the context of this study, precision is used as the as ration of true correct inpainting detection with respect to the total data set. The percentage (%) sign is usually its quantity of precision measurement. In this study the precision measure is defined as follows using equation 5.

$$Precision = \frac{N_D}{N_D + N_{ID}} \quad (5)$$

Whereby N_D is the number of correct detection and N_{ID} is the number of incorrect detection.

False positive rate refers to the error that is obtained in an evaluation scenario in which certain conditions are observed and tested positive for which it is mistakenly false. In the context of this study, the false positive metric is used as the percentage of the ration of incorrect detection with respect to the total number of observed and experimentally tested data. False positive performance metric is represented as follows in equation 6.

$$false\ positive = \frac{N_D}{N_D + N_m} \quad (6)$$

Where N_D is the number of correct detection and N_m is the number of miss rates.

The results of the performance of this proposed video inpainting detection technique is summarized in Table 4.2. It can be seen from the results in Table 4.2 that this

proposed technique achieves high percentage detection precision rate and less false positive detection rates.

Table 4.2:Performance Evaluation of the Proposed Video Inpainting Detection Technique

Video	Detection Precision (%)	False Positive (%)
Test Video 1	99.54	0.78
Test Video 2	99.86	0.07
Test Video 3	99.97	0.02
Test Video 4	95.98	0.11
Test Video 5	99.56	0.04
Test Video 6	73.95	0.50
Test Video 7	98.20	0.13
Test Video 8	96.38	0.97
Test Video 9	98.58	1.78
Test Video 10	95.76	0.01
Test Video 11	98.63	0.03
Test Video 12	99.46	0.14
Test Video 13	95.32	0.43
Test Video 14	97.86	0.13
Test Video 15	99.12	0.02
Test Video 16	98.49	0.15
Test Video 17	99.03	0.01
Test Video 18	98.35	0.03
Test Video 19	93.47	0.03
Test Video 20	99.20	0.23

4.3.5 Comparison with Other Detection Techniques

In this section, the performance of this technique is demonstrated and examined with respect to other different video inpainting detection techniques proposed in the work of (Hsu et al., 2008)(Zhang et al., 2009) and (Lin & Tsay, 2014). These techniques are handpicked as benchmark techniques because of their prominence and great performance rate of 96.61%, 93.40% and 97.52% individually for video inpainting identification throughout the years. The performance of our technique is measured in light of three measurements metrics including detection precision, false positive rates, and execution time.

All techniques were evaluated based on the same benchmark dataset designed by (Hsu et al., 2008), (Zhang et al., 2009) and (Qadir et al., 2012) for video inpainting forgery detection. Table 4.3 shows the comparison result of the precision and false positive rates for the different video inpainting detection techniques.

Table 4.3: Comparison with Other Detection Techniques

Reference	**Average Precision Rate (%)**	**False Positive rate (%)**
(Hsu et al., 2008)	96.61	1.18
(Zhang et al., 2009)	93.4	6.60
(Lin & Tsay, 2014)	97.52	3.22
Proposed Technique	99.79	0.29

This proposed technique demonstrates a higher rate of inpainting detection precision compared with the technique proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014). Essentially, the relative comparison of false positive rate among the four techniques demonstrates that this proposed inpainting detection technique based on the correlation of Hessian matrix features records a low false positive rate contrasted with the techniques proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014).

In addition, the execution time contrasted with other video inpainting detection techniques proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014) is presented in Table 4.4 for the twenty test video. The execution time was measured by running the benchmark techniques and the proposed techniques on the same dataset. Thus, the four video inpainting detection techniques were run utilizing Matlab on an Intel Celeron PC having a 1.83 GHz processor speed, 64 bit operating system, and 4GB RAM.

Table 4.4:Execution Time for Different Detection Approaches

	Execution Time(seconds)			
Test Videos	**(Hsu et al., 2008)**	**(Zhang et al., 2009)**	**(Lin & Tsay, 2014)**	**Proposed**
1	794.00	712.34	612.34	683.20
2	1417.92	1335.54	1432.65	1329.64
3	2228.54	1329.64	1276.78	1165.98
4	201.56	175.66	177.48	141.09
5	428.97	711.02	596.71	537.39
6	537.39	813.76	463.39	337.12
7	244.21	534.54	346.87	237.29
8	240.08	320.34	474.13	239.62
9	223.91	354.37	387.65	250.20
10	1562.44	1894.76	2341.91	1436.10
11	302.34	436.65	513.59	232.14
12	298.32	341.21	259.13	239.54
13	267.66	336.88	265.15	239.63
14	1578.21	1753.90	1965.57	1265.32
15	934.23	974.86	1007.27	832.15
16	289.38	369.34	349.32	226.34
17	204.22	385.23	338.54	198.67
18	286.29	303.41	297.85	187.43
19	316.71	493.43	457.4	234.67
20	269.58	324.75	397.19	254.43
Average	**631.298**	**695.0815**	**698.046**	**513.3975**

The comparison of execution time for the different video inpainting detection techniques as shown in Table 4.4 demonstrates that this proposed technique has the most limited execution time. This is a direct result of the relative speed in Hessian matrix extraction from a video and the minimal number of steps for the detection algorithm that is proposed in this technique making it both productive and less complex. In addition, the technique proposed in the work of (Hsu et al., 2008) demonstrates a moderately more execution time than this proposed technique. This difference in execution time is due to the sensible time spent for extraction of noise residue in (Hsu et al., 2008). Furthermore, the technique proposed in the work of (Zhang et al., 2009) likewise demonstrates a more drawn out execution time compared to this proposed technique. The difference in execution time is due to the intricate preparing stages included in the extraction of ghost shadow artifacts from a video in (Zhang et al.,

2009). The technique in (Lin & Tsay, 2014) demonstrates a more extended execution time compared this proposed technique. This is as a result of its complex computational weight for spatio-transient examination.

4.3.6 Discussion

An inventive technique has been proposed in this thesis to detect texture and structure based inpainting forgery in a digital video that is robust to handle compressed and non-compressed videos, with a high detection precision, low false rate and shorter execution time. Thus, a new technique based on the analysis of the inconsistencies in the statistical correlation of Hessian matrix features is introduced. The goal is to extract the Hessian features from video frame blocks, compute the correlation of the Hessian values between neighbouring frame blocks and then analyze their correlation for inconsistencies based on predefined threshold values. The Hessian matrix features were selected from a video in view of its unwavering quality in distinguishing interest points from an image or video frame which will be suitable for forensic examination. The proposed video inpainting detection technique was evaluated using a combination of distinctive datasets from (Hsu et al., 2008)(Zhang et al., 2009)and (Qadir et al., 2012). These datasets were picked on account of their wide utilization as benchmark data for video forensic examination.Based on the selected datasets, the performance of this proposed video inpainting detection technique was evaluated in order to ascertain its robustness based on three different metrics namely: precision rate, false positive rate, and execution time. The precision rate is defined as when an inpainted region in the video is accurately recognized as inpainted, false positive is defined as when an inpainted region in the video is wrongly distinguished as not inpainted.

The result of this analysis clearly demonstrates that this proposed technique for video inpainting identification which utilizes the Hessian features extracted from a video

significantly enhanced video inpainting detection precision rate by around 3% contrasted with the technique proposed in (Hsu et al., 2008), 6% contrasted with the technique proposed in (Zhang et al., 2009) and 2% contrasted with the technique proposed in (Lin & Tsay, 2014). The improvement in precision rate is a direct result of the capacity of Hessian features to extract the local structure of the pixel data in a given area regardless of size and intensity value of the area.

A reduction in the rate of false positive detection is additionally recorded when this proposed technique is contrasted with other techniques proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014).

Finally, this proposed technique has likewise demonstrated a shorter execution time when contrasted with the three different techniques proposed in (Hsu et al., 2008), (Zhang et al., 2009) and (Lin & Tsay, 2014) as appeared in Table 4.4.

4.4 Chapter Summary

This chapter discusses a contribution that presents a system for recognizing video inpainting forgery by utilizing the correlation of Hessian Matrix, extracted from a digital video. Tests performed in this study have demonstrated that the utilization of a Hessian matrix has altogether enhanced the accuracy of video inpainting forgery detection. In light of the outcomes of this study, the utilization of Hessian matrix has been determined to be a valuable procedure in distinguishing inpainting falsification in a digital video.

CHAPTER 5 : CHROMA KEY DETECTION

This chapter involves the innovative methodology and experimental results of an invented technique and system for chroma key forgery detection in digital videos. This technique utilizes the statistical correlation of blurring features for the detection of chroma key forgery in a digital video that is performed either using a green or blue screen as a background. The key contribution is the introduction of blurring artifact as a feature in a technique for the detection of video chroma key forgery. The advantage of the use of blurring features in this technique is to provide a solution to the limitations associated with existing chroma key detection techniques presented in (Xu et al., 2012) and (Wang & Farid, 2009) . The limitation of these existing techniques is their dependence for chroma key detection on source video encoding. However, the accuracy of these techniques diminish rapidly when the two source videos used for the chroma key composition have the same encoding. Thus, the use of blurring features is proposed to detect chroma key forgery involving videos that have different or the same quality of encoding. The chapter is divided into three main sections: the first section (section 5.1) highlights a brief introduction. The second section (section 5.2) present the proposed framework for chroma key forgery detection based on the correlation of blurring features while the experimental results, analysis and discussion are presented in the third section (section 5.3).

5.1 Introduction

Digital videos have become easy to acquire and disperse, mostly due to the implanted camera in hand held gadgets such as cellular telephones, PDA's and tablets (Su, Zhang, & Liu, 2009; Zhang & Su, 2009). Additionally, the visual quality of a video can be upgraded and their contents can also be extracted using a variety of video manipulation softwares. On the other hand, the advancement of these video

manipulation softwares has impacted the use and control of digital video manipulation for noxious reason (Rigoni, Freitas, & Farias, 2016). Digital video forgers use video manipulation softwares to tamper the original content of a digital video. The target of these digital video forgers is to misdirect the view of the audience watching the video.

There are different illegal fabrications that can be performed on a video. This illegal digital video fabrication includes splicing, inpainting, copy move, duplication and chroma key forgery.

Chroma key forgery which is also known as green screen, blue screen or color separation overlay uses the innovation of video editing software such as Adobe Photoshop, VSDC software to compose two video streams together based on colour hues.Chroma key forgery is achieved by first recording a video using a constant background colour such as green, the background colour of the video is then made transparent, replacing it with any other video clip, graphic or still image. Therefore, when such a video is presented as admissible digital evidence in a court, it will lead to a wrong conviction, or when the video is shared over social media, it will tarnish the social status of the person involved in the video.

For this reason, a novel technique based on the correlation of blurring artefact is proposed for the detection of chroma key forgery in digital videos. The motivation driving the utilization of the blurring artefact, extracted from a video for chroma key forgery detection in this proposed technique, is to establish a more reliable feature in contrast to other features used for chroma key forgery detection from the literature.

5.2 Chroma Key Detection Framework

This section portrays the proposed technique based on blurring artefact as a feature for the detection of chroma key forgery in digital videos. It is worth noting that the

target of digital manipulators is to create a forged video with no hint of forgery to the human naked eye. As such, to that effect, these digital forgers make use of video editing softwares that will conceal all the visible hint of forgery in the tampered video. Most video editing softwares for chroma key forgery apply a significant amount of blurring on the resulting forged video so as to make the video troublesome for the human naked eye to figure out if it is an original video or forged. However, because the videos used for the chroma key composition are from different sources, the blurring quality associated with each pixel data for the different videos will differ. This variation in the blurring feature is used in this proposed technique as an intrinsic fingerprint for chroma key forgery detection.

The point of this research study is to extricate the blurring variations from the different videos and use them for chroma key forgery detection purpose. This proposed detection technique is discussed in three fundamental stages of pre-processing, feature extraction and post-processing as outlined in Figure 5.1.

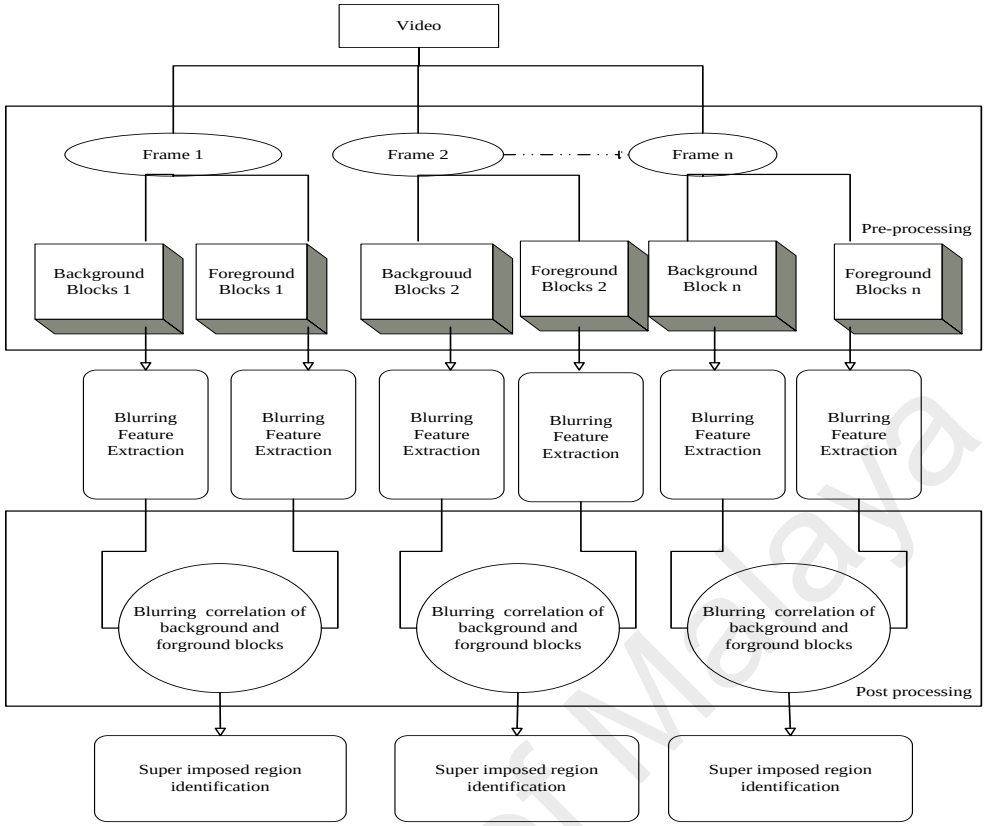

Figure 5.1:The Proposed Chroma Key Detection Framework

5.2.1 Pre processing

Video pre-processing refers to the use of algorithms for the enhancement of a video quality in preparation for analysis. This is to increase the efficacy of the video signal. In this proposed technique, the efficacy of our video is increased by removing spurious noise that affects the quality of the video using noise filtering algorithm. Unfortunately, choosing the appropriate filter for this purpose is not an easy task to achieve. Therefore, in this section different video pre-processing techniques are discussed for noise removal from digital videos in order to determine the most preferable one given the intended problemto address.This is because we want the best noise filtering algorithm that will have minimal effect to the video data, so as not to affect the original quality of the video. Research studies on image and video noise removal have been in progress for

decades. However, our study will be focusing on the most commonly used de-noising algorithms.

5.2.1.1 Noise in Digital Videos

Research on video quality enhancement by using the concept of noise removal has been ongoing for a long time. This is mainly as a result of low end acquisition devices used for video recordings. Example of video acquisition devices includes camcorders, cameras and mobile phones. However, because of the imperfection of these devices, the resulting videos they generate have variable quality. This is because of certain disturbances called noise that affect the pixels in the video.

Noise is referred to as the presence of pixels in a video frame whose colour and brightness has no relation to the subject. Noise is more noticeable in recorded video when there is very little illumination reaching the camera's sensor during the video acquisition process (Mairal, Sapiro, & Elad, 2007; Olshausen, 1996; Yang et al., 2008), thereby degrading the quality of the video and affecting the useful features that may be extracted for the video analysis process.

Since the aim is to extract reliable features from a video for chroma key forgery detection, various video denoising algorithms are studied in order to choose the best algorithm that can successfully be used to remove noise from a video without affecting the relative quality of the video and the blurring features this study proposed to use for the chroma key forgery detection process. (Rieder & Scheffler, 2001).

In the last couple of years, a number of algorithms have emerged for video denoising. These algorithms have produced outstanding results as applied to different video formats, different noise distributions and variable denoising strength. The

evolution of these algorithms, though interesting but have created the problem of selecting the best algorithm with respect to performance and strength.

In this section three important algorithms are discussed from the literature that is effectively proposed for video de-noising. A detailed description is given of each algorithm highlighting the advantages and limitations of each algorithm. This is to provide a justification for the algorithm that is chosen for this work. Moreover, this discussion also provides answers and highlights on some open challenges for future research.

The de-noising algorithm are new concepts on de-noising and sharpening of video signals (Rieder & Scheffler, 2001), adaptive spatio-temporal filtering for video de-noising (Cheong et al., 2004), wavelet-domain video de-noising based on reliability measures (Wexler, Shechtman, & Irani, 2004).

New concepts on denoising and sharpening of video signals

The algorithm proposed in this work presents a novel method for enhancing the signal quality of a video by removing noise from the video. Two fundamental issues were addressed in this algorithm. The first is noise removal from a video in conjunction with quality enhancement whilst the second is a combination of luminance transition improvement (LTI) with peaking, which is done in order to provide the best video outcome for human visual system. All these issues were successfully achieved by processing the video signals in distinctive ways. The de-noising part of this algorithm takes into account noise and sharpness simultaneously.As a result presenting an orthogonal wavelet filters as an optimal solution for video denoising (Rieder et al., 1998) and an orthogonal Haar filter for sharpness peak.Thealgorithm has the advantage of improving the video signal quality by successfully removing noise from it with a minimal computational complexity. However, the algorithm has the limitation of

conflicting influence between the signal quality improvement of the video and human visualization system as such cannot be effectively used as a de-noising system for this proposed chroma key video forgery detection solution. This is because the conflicting influence of the video will affect the blurring quality of the video around pixel boundaries.

Adaptive spatio-temporal filtering for video denoising

The algorithm proposed in this method for video denoising is based on spatio temporal filtering. The spatio temporal filtering approach is based on adaptive selection with a combination of wavelet based transform (Antonini et al., 1992) and wiener filter (Goldstein, Reed, & Scharf, 1998). The temporal filtering is based on bi-directional block based motion estimation compensation that uses an enhanced predictive zonal search (EPZS) algorithm. The flow chart of the algorithm is shown in Figure 5.2.

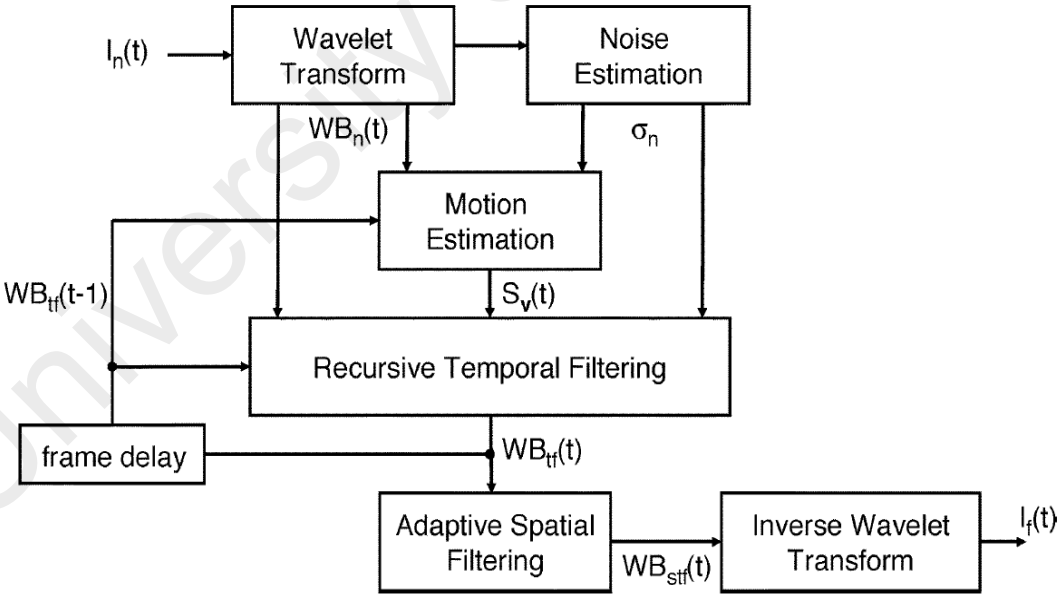

Figure 5.2: Adaptive Spatio-Temporal Filtering For Video Denoising

The experimental result for video de-noising using this method has shown an improvement in the quality of the video signal. However, the performance of the technique is more robust when considering video encoded with H.264 encoder.

Wavelet-Domain Video Denoising Based on Reliability Measures

The work of (Zlokolica, Pižurica, & Philips, 2006) proposes a video de-noising algorithm in view of non-decimated wavelet band separation. The de-noising algorithm is divided into three stages that involve motion vector refinement, temporal filtering, and adaptive spatial filtering. The motion vector refinement and temporal filtering are done in a close circle which is then accompanied by a frame by frame adaptive filtering in a wavelet domain. The motion estimation parameters are obtained based on the video motion trajectory per orientation. Temporal filtering is then applied to each motion trajectory in a wavelet domain to remove noise effect from the video. Finally, adaptive spatial filtering is used for smoothing the wavelet co efficient at locations where there is less effect of the temporal filter. The outcomes from the experimental results of this algorithm for noise removal on different videos show that it outperforms other algorithms usually with respect to peak of signal-to-noise ratio. For this reason, this algorithm is applied to a video to remove noise before analysis. This is because of the reliability of the algorithm in terms of signal to noise ratio and a minimal noise estimation error (Amer & Schroder, 1996).

Once the noise from the video is removed, the video is partitioned into individual frames as appeared in Figure 5.3. The individual frames are indicated by F while n is the number of frames in the video.

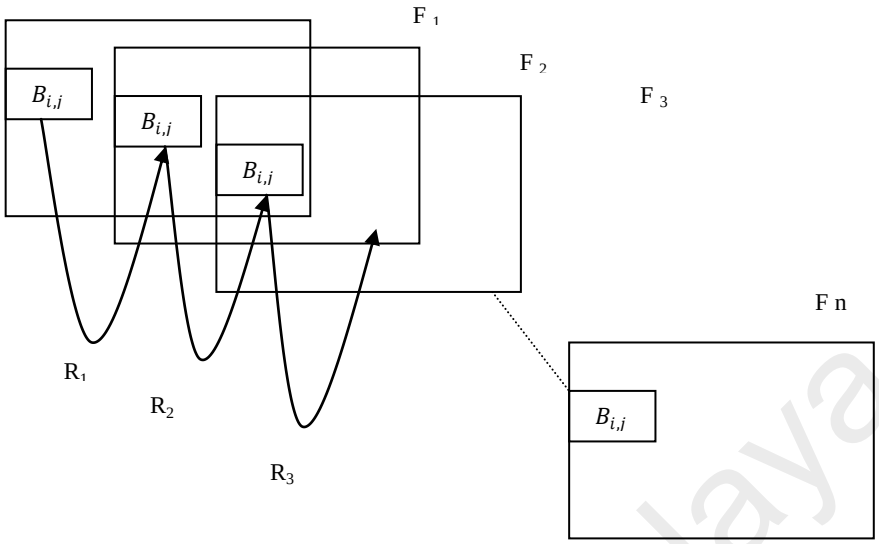

Figure 5.3: Correlation of Blurring Blocks

Each frame is further divided into $\boldsymbol{M} \times \boldsymbol{N}$blocks shown as $(B_{i,j})$, in Figure 5.3. In these blocks, $(B_{i,j})$ are identified by row (i) and column (j) index of the respective block. This is to enable the use a block feature extraction approach.

5.2.2 Feature Extraction

Feature extraction chooses components from a video that pass on valuable data that can be used for different video analysis purpose (Jain, 1987; Schindelin et al., 2012). The behaviour of these components is dictated by the relationship of their patterns. In this proposed chroma key video forgery detection technique, the blurring feature is utilizedwhich is extricated from a video foreground and background frame blocks, represented by $B_{i,j}$ in Figure 4.3.

5.2.2.1 Blurring Feature

Blurring in a video is the obvious streaking of quickly moving item or objects in a still picture or a succession of pictures, for example, a video. Once a video is blurred, it

will look hazy and indistinct to the sight or mind. There are three major causes of blurry videos which include; lens out of focus, subjective movement and camera shaking.

Lens out of Focus

This sort of blurring within a video is a result of concentrating unintentionally on a subject which may not be the photographic artist's proposed subject, thus making such a video blurry. However, because of the advent of the auto focus lens nowadays in most digital cameras and camcorders, it is very rare that the entire video will be out of focus. Usually, you will see one part of the video fresh and clear, however, other parts may be out of focus. Thus, different videos will have different blurring characteristics depending on the scene, camera or camcorder lens power and the photographic artist's expertise.

Subjective movement

Blurring in a video can come about because the subject in a video moves when the shutter is in action. This kind of subject motion may lead to the video or part of the video to be blurred. Although, this type of blurring can be avoided to some degree by setting the camera to a fast shutter speed, however, this requires extensive skilled digital knowledge, in conjunction with the availability of the necessary hardware.

Camera shaking

This is another regular issue that can cause a video to be blurry as a result of the slightest hand shake during video acquisition process. Thus it is best to make use of a tripod and a remote shutter during acquisition. However, even with the use of the tripod and remote shutter it is still impossible to achieve a blurred free video from handshake.

Considering chroma key forgery for video composition requires the use of two different videos that are likely to have variations in their blurring properties, because the

videos are from different sources, therefore it is proposed to use the blurring feature as a fingerprint for chroma key forgery detection in digital videos. Blurring features has been effectively utilized as a unique mark for different image and video forensic algorithms. For instance, it has shown to be a viable and trustworthy fingerprint in identifying logo removal forgery in images and video fabrication (Su et al., 2010; Zhang & Su, 2009) .

5.2.2.2 Blurring Feature Extraction

To obtain the blurring feature from the video frame blocks $B_{i,j}$ as shown in Figure 5.3, wiener deconvolution of low pass filter is used as modelled in equation 7.

$$W\left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right) = \frac{H * \left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right) S_{xx}\left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right)}{\left|H\left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right)\right|^2 S_{xx}\left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right) + S_{nn}\left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right)} \quad (7)$$

Where $B_{i,j}^{F_n}$ represents the block for the nth frame, $B_{i,j}^{F_n-1}$represents the previous block of nth frame.$S_{xx}\left(B_{i,j}^{F_n}{}_1, B_{i,j}^{F_n-1}\right), S_{nn}\left(B_{i,j}^{F_n}, B_{i,j}^{F_n-1}\right)$represents the power spectrum of original video frame with noise and $H\left(B_{i,j}^{F_n}{}_1, B_{i,j}^{F_n-1}\right)$represent the blurring filter. The rationale behind the use of this filter is its optimality of minimizing mean square estimation error and an accurate point estimation.

5.2.3 Post processing

In the post processing stage, the blurring features are extracted from the suspected video frame background and foreground pixel blocks represented as $B_{i,j}$ in Figure 5.3, then the technique of statistical correlation is applied to the blurring features extricated from the video for examination to generate the histogram of correlations. At that point, the histogram of correlations is investigated for chroma key forgery identification in the video.

5.2.3.1 Statistical Correlation of Blurring Features

Once the blurring features are successfully extracted from the background and foreground pixel blocks of the video under forensic examination, a cross correlation is computed between spatially indexed pixel blocks of the background and foreground. The modelled correlation existing between neighbourhood frame blocks are represented by equation 8.

$$R = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\left(B_{i,j}^{Fb} - \bar{B}\right)\left(B_{i,j}^{Ff} - \bar{B}\right)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n}\left(B_{i,j}^{Fb} - \bar{B}\right)\left(B_{i,j}^{Ff} - \bar{B}\right)^{2}}} \qquad (8)$$

Where B represents the blurring artefact for a particular video frame block,F_b represents the frame block background and F_f represents the frame block foreground and $\bar{B}$ is the mean of the blurring artifact across all frame blocks.

5.3 Experimental Results and Analysis

In this section, the results of these experiments are presented on chroma key forgery detection in digital videos. The data set used for the experiment is divided into three sets. There are three goals behind the use of three different datasets for the experimental process.The first reason is to use the designed dataset for the initial simulation of these experiments in order to determine how the use of blurring features can effectively detect chroma key forgery in a digital video.The second reason is to use the dataset from movies to evaluate the robustness of this proposed technique with professional chroma key effects in videos. The third reason is to test this proposed technique for chroma key forgery detection on compressed videos. These goals were achieved successfully. The results shown in this section prove the success of the use of statistical correlation of blurring features for chroma key forgery detection in digital videos.

5.3.1 Data Set

To provide a sound justification for this proposed chroma key forgery detection technique a series of experiments were performed on the video dataset created for the initial simulation of the experiment. The data set comprises of twenty test videos with a total of 3754 frames. The twenty test videos were created using VSDC software[3]. The videos created are approximately 3 minutes in length and a resolution of 800X480 with 16:9 display aspect ratio. The videos have a frame rate of 30 frames per second. These datasets were processed and analysed in order to address the problem of the detection chroma key forgery in digital videos.

5.3.1.1 Results of Experiments on Chroma key Forgery Detection

In this section, the results of this experiment is presented for the detection of chroma key forgery in the form of histograms of correlation for the extracted blurring features from frame blocks of the test videos. These histograms of correlation are computed and analyzed for variations in blurring correlations across video background and foreground frame blocks.

The performance metrics used to evaluate the robustness of this proposed technique for chroma key forgery detection includes: the true positive detection rate (TPR) and false positive detection rate (FPR). In the context of this study, TPR is used as the ration of true correct chroma key detection with respect to the total data set whereas FPR refers to the error that is obtained in an evaluation scenario in which certain conditions are observed and tested positive for which it is mistakenly false. The FPR metric is used as the percentage of the ration of incorrect detection with respect to the total number of

[3]http://www.videosoftdev.com/free-video-editor/download

observed and experimentally tested data. Equations 9 and 10 define the mathematical expressions used to obtain these performance metrics.

$$TPR = \frac{TP}{(TP + FN)} \qquad (9)$$

$$FPR = \frac{FP}{(FP + TN)} \qquad (10)$$

Where TP represents the number of true positive detections, FN represents the number of false negative detections, FPrepresents the number of false positive detections, TN represents the number of true negative detections. Table 5.1 reports the result obtained when this proposed technique was applied to the 20 videos from this data set.

Table 5.1: Result of Experiments on 20 Test Videos

Video	**TPR (%)**	**FPR (%)**
Test Video 1	95.26	1.70
Test Video 2	86.17	2.47
Test Video 3	96.31	2.40
Test Video 4	96.01	1.51
Test Video 5	96.05	2.54
Test Video 6	96.42	2.42
Test Video 7	96.18	1.53
Test Video 8	91.87	2.46
Test Video 9	96.55	2.46
Test Video 10	94.46	1.48
Test Video 11	87.72	2.36
Test Video 12	95.54	2.31
Test Video 13	64.39	1.93
Test Video 14	64.42	1.84
Test Video 15	94.79	1.90
Test Video 16	87.46	1.94
Test Video 17	94.82	1.41
Test Video 18	97.10	1.47
Test Video 19	94.96	1.49
Test Video 20	96.30	1.44
Average	**91.12**	**1.95**

Figures 5.4 to 5.23 demonstrate the histogram of correlations for the blurring features showing the relationships between background and foreground frame blocks and the chroma key composition detection result using this proposed technique for the 20 test videos that were used in these experiments. The white coloured region in the detected row showsa variation in terms of blurring correlation with other regions of the video, and therefore considered as superimposed on to an original background.

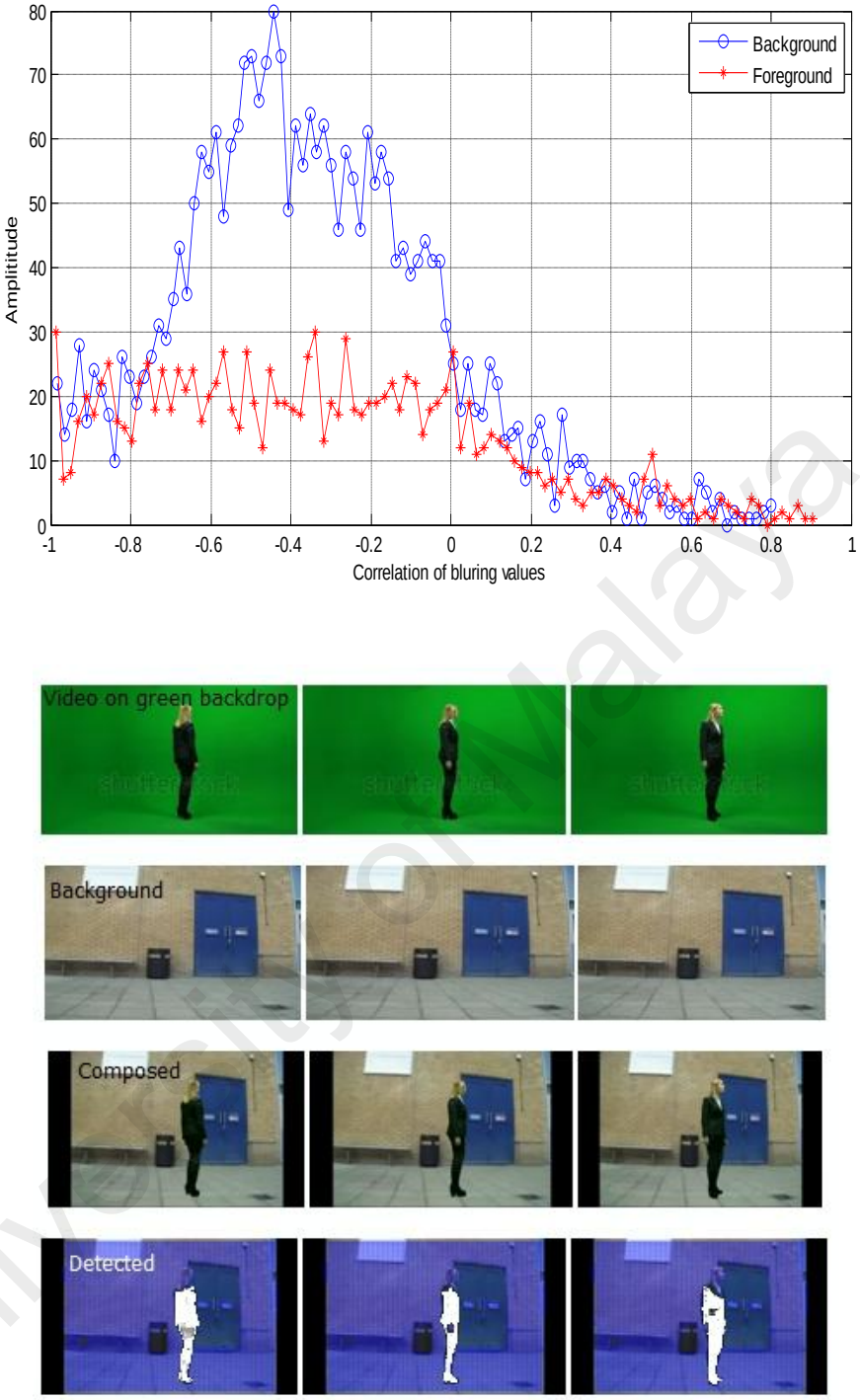

Figure 5.4: Histogram of Blurring Features Correlation and Forged Region Detection for Test Video 1

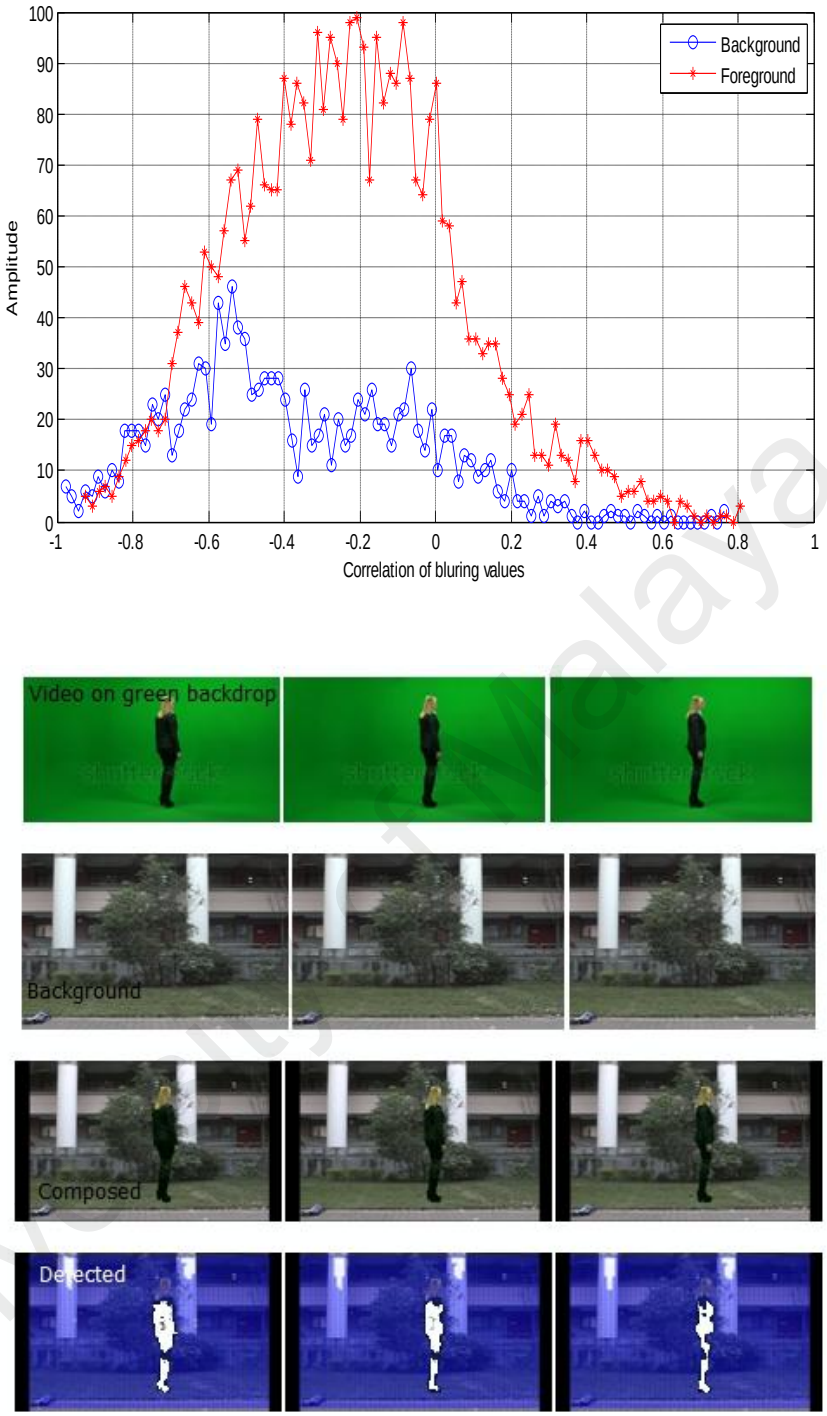

Figure 5.5: Histogram of Blurring Features Correlation and Forged Region Detection for Test Video 2

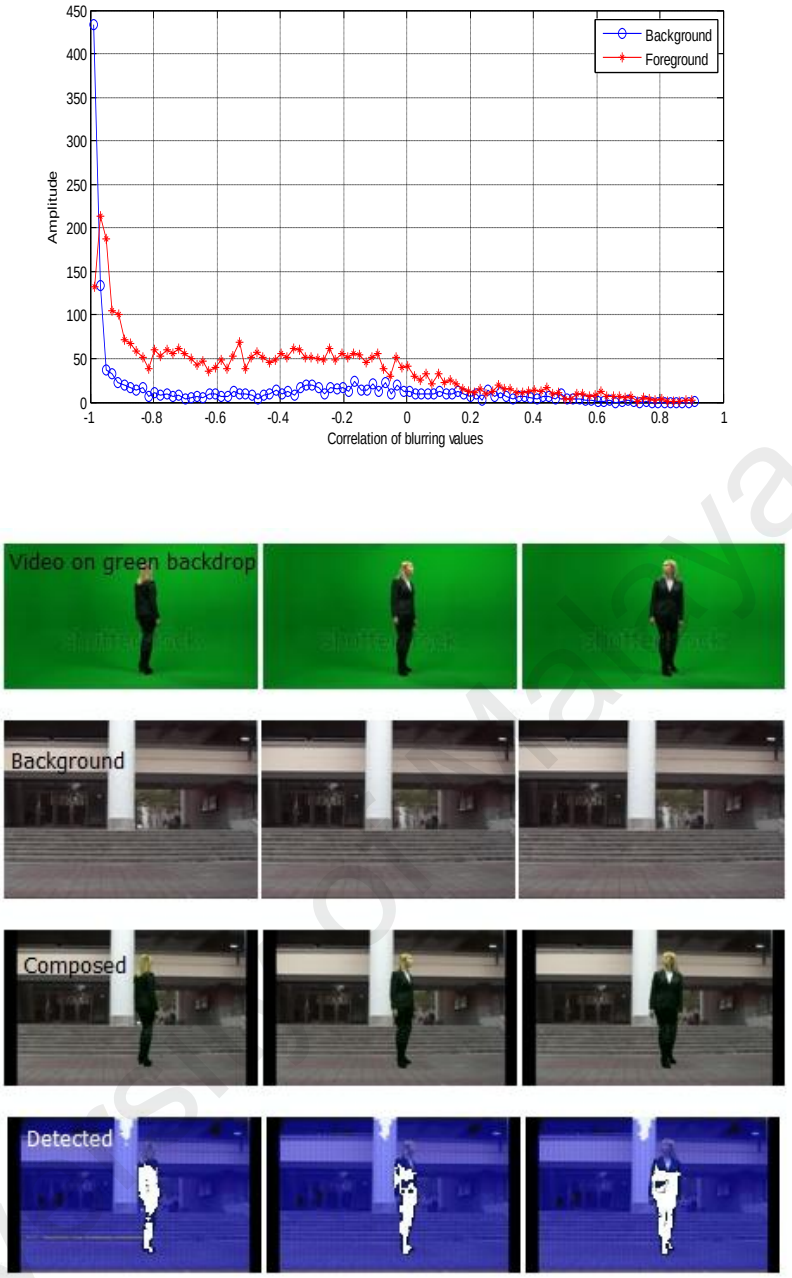

Figure 5.6: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 3

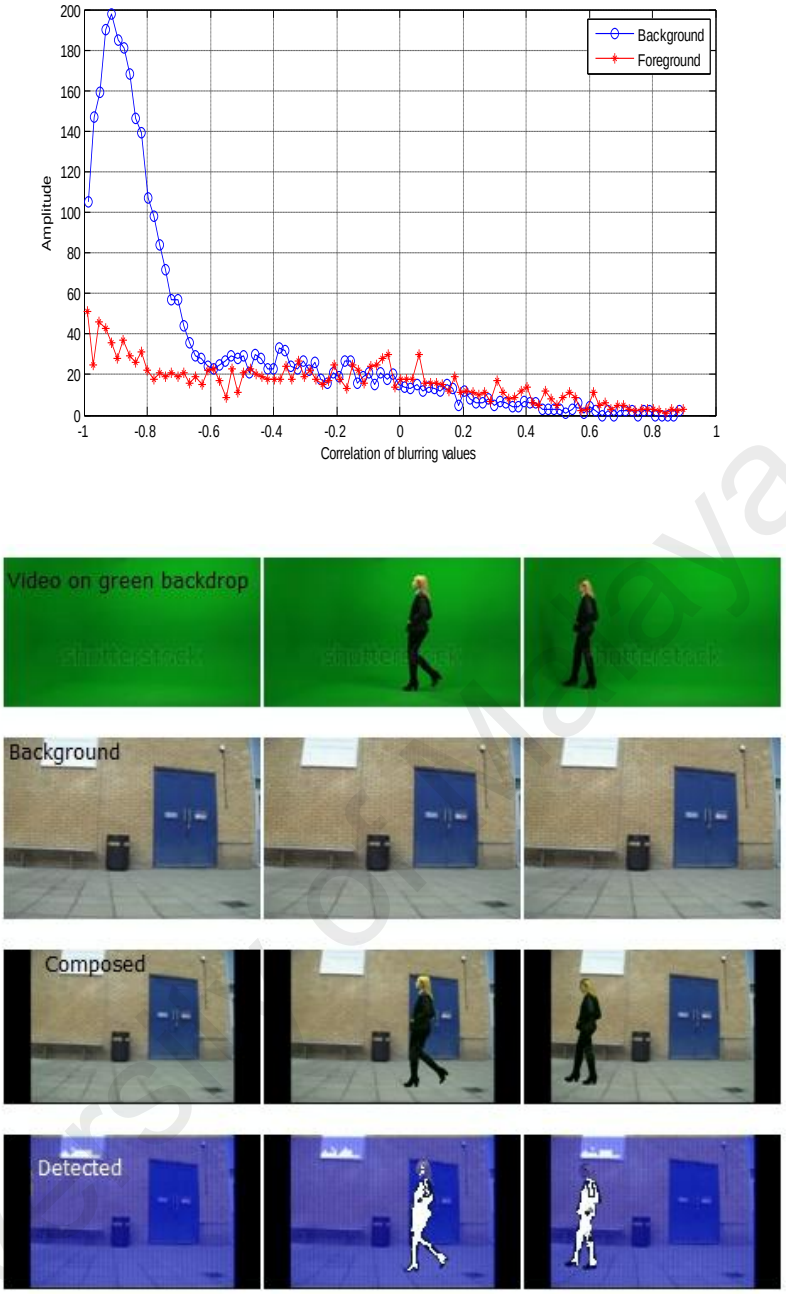

Figure 5.7: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 4

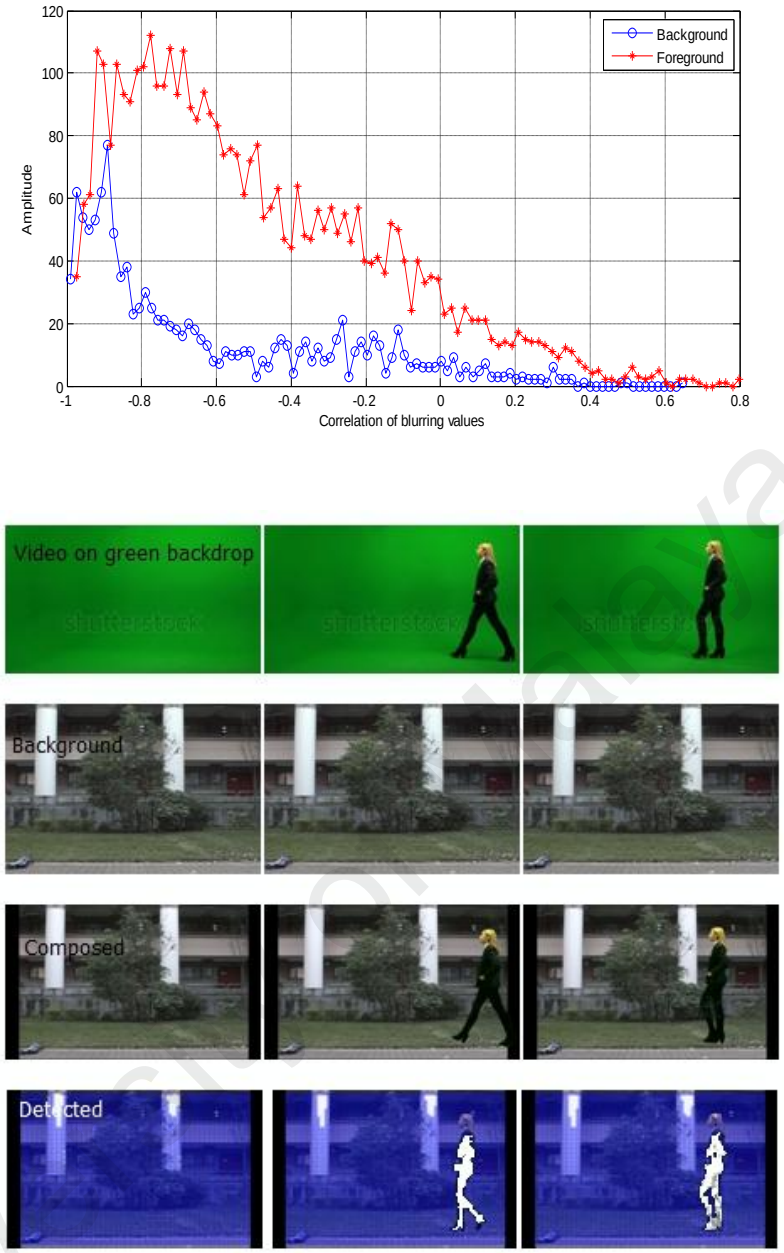

Figure 5.8: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 5

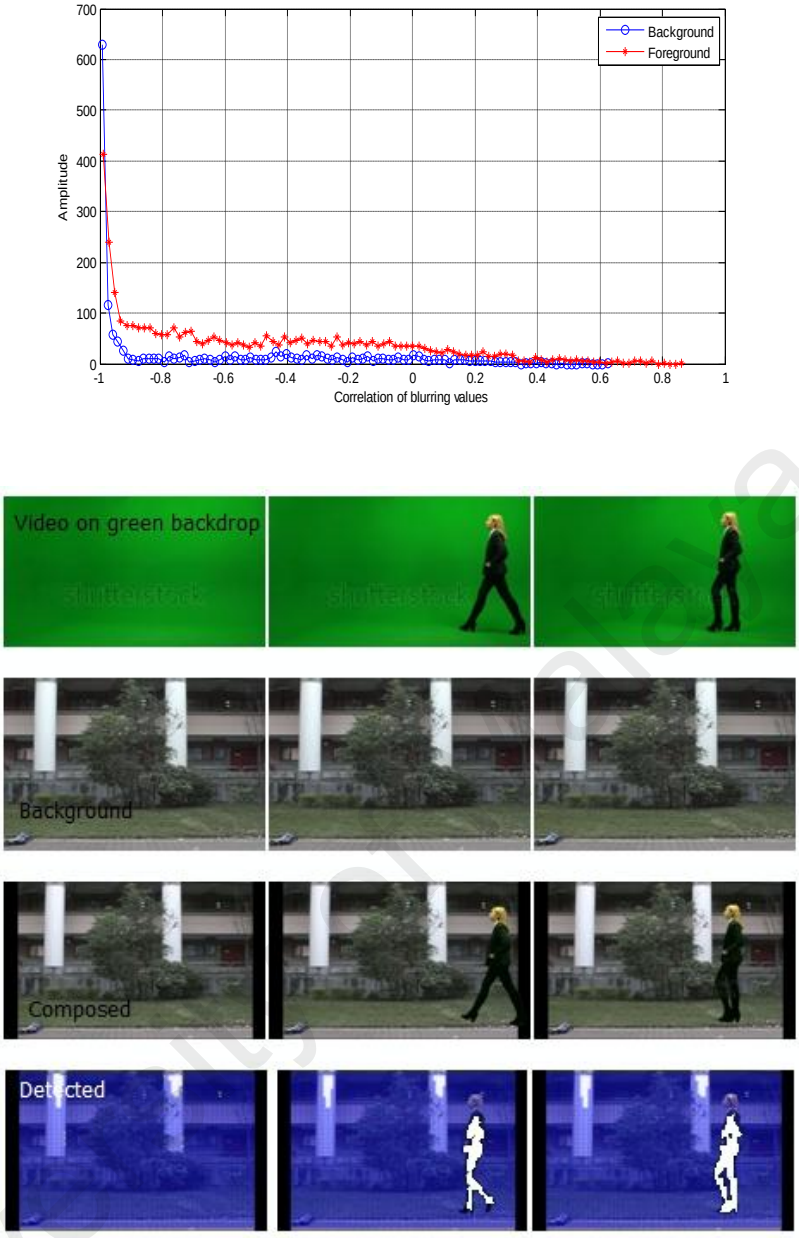

Figure 5.9: Histogram of Blurring Features Correlation and Forged Region Detection for Test Video 6

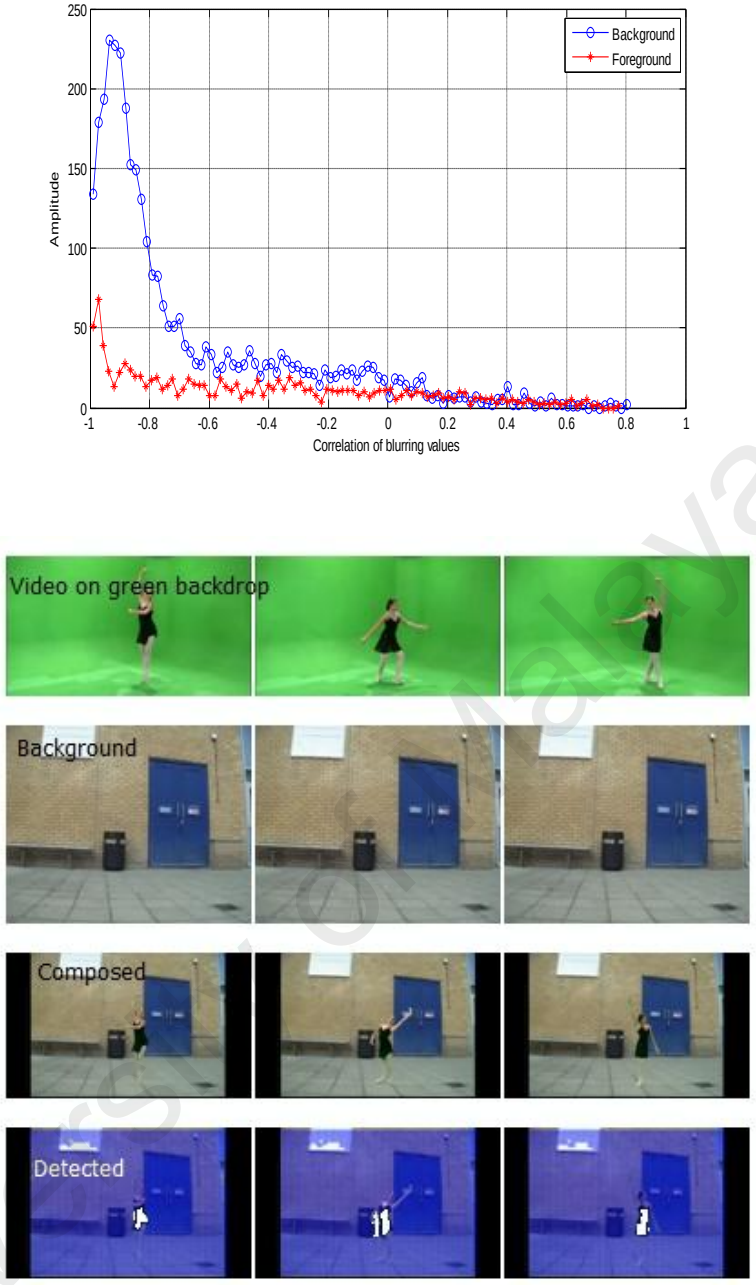

Figure 5.10: Histogram of Blurring Features Correlation and Forged Region Detection for Test Video 7

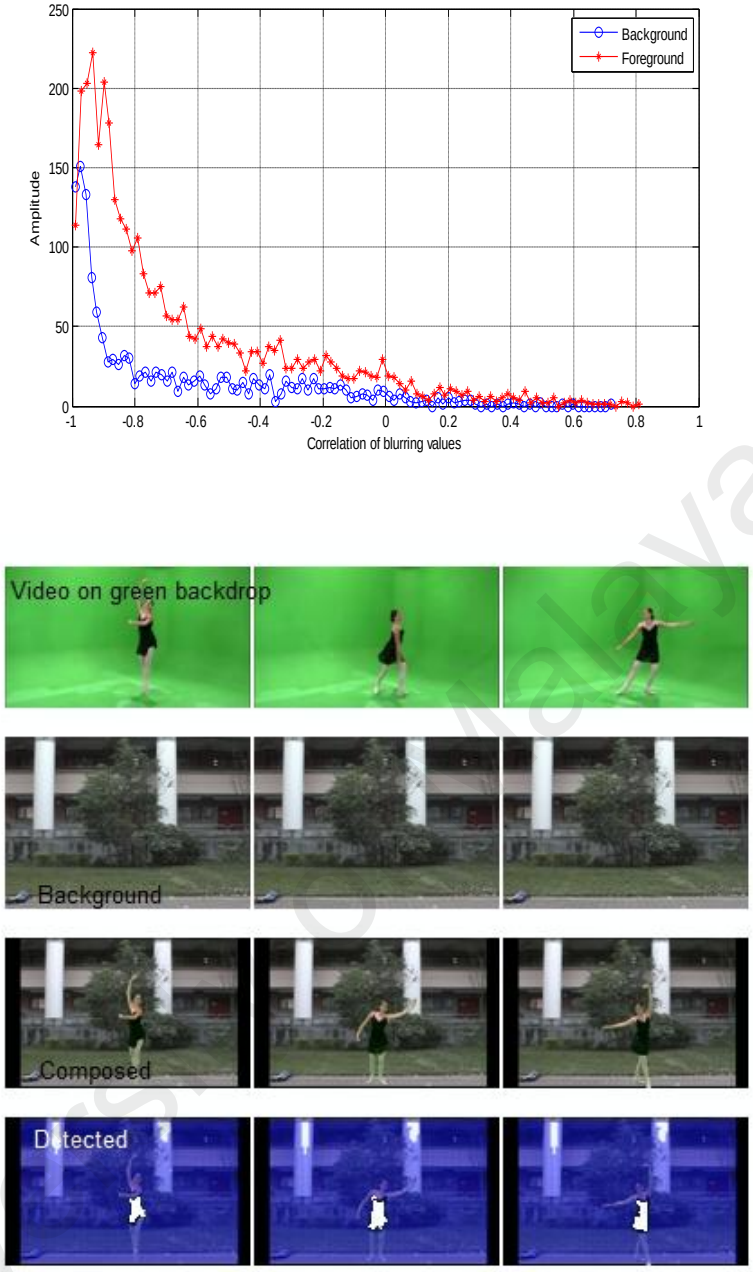

Figure 5.11: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 8

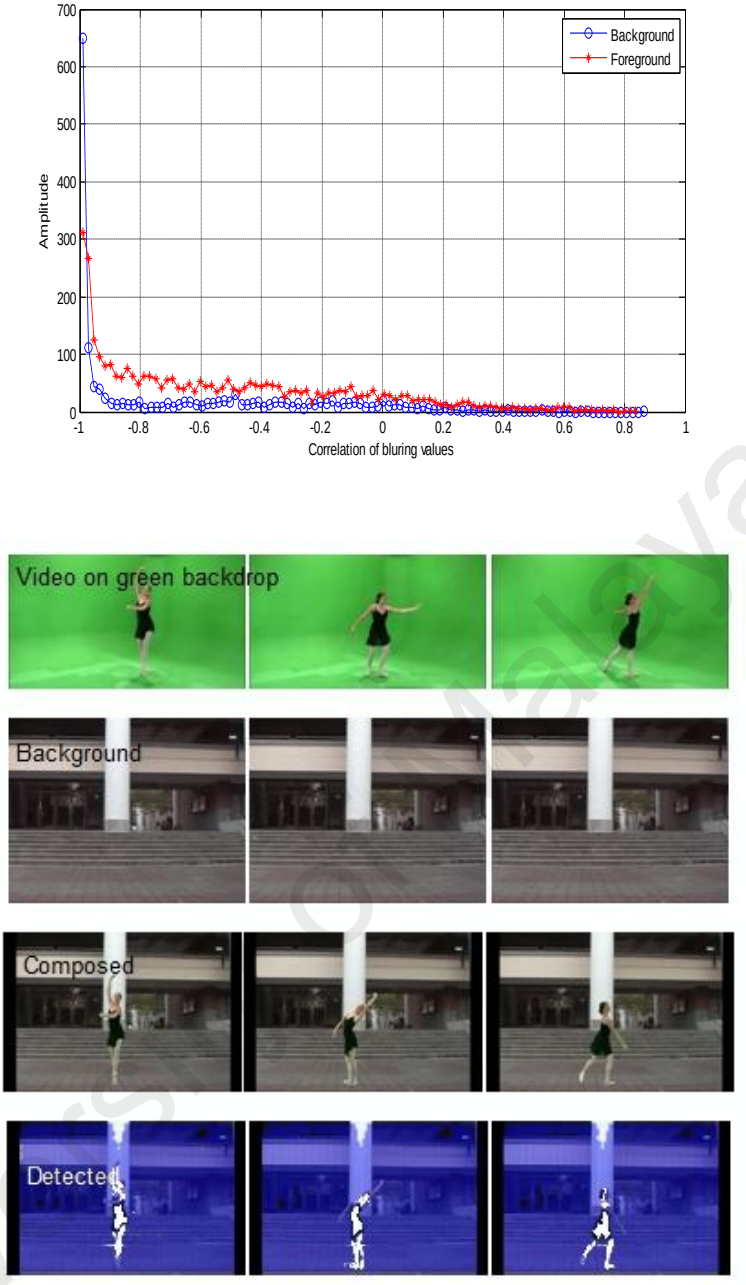

Figure 5.12: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 9

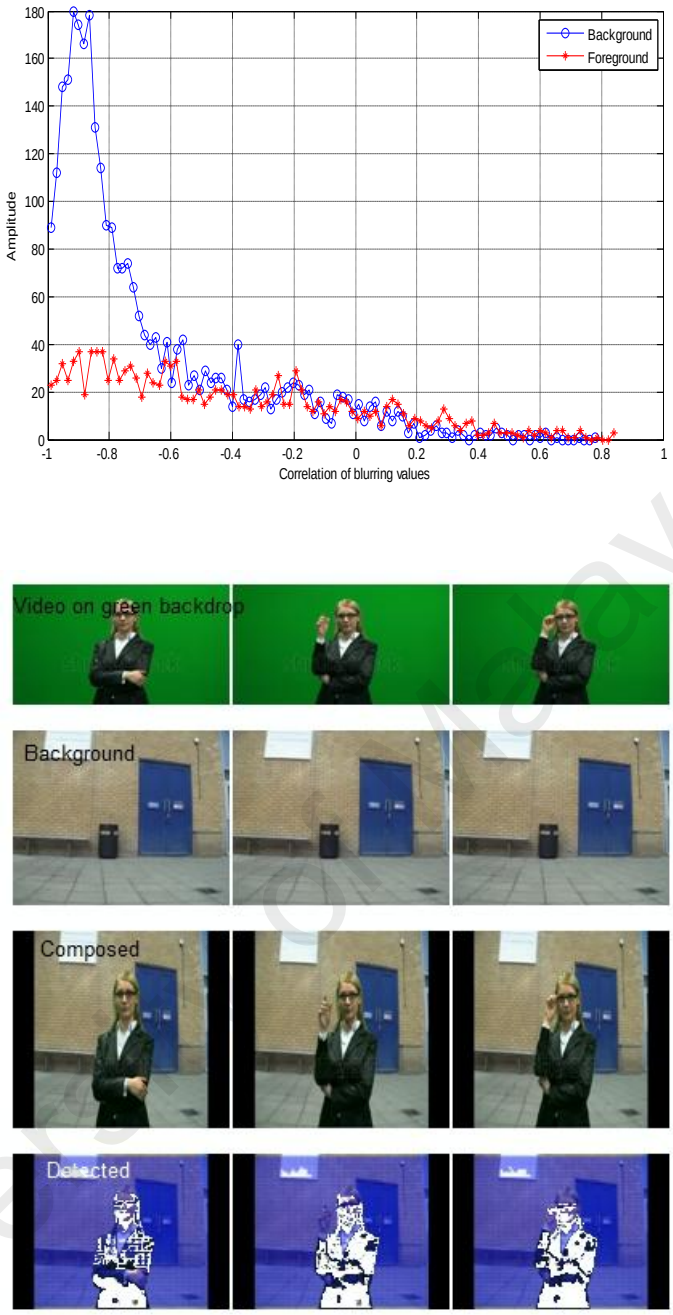

Figure 5.13: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 10

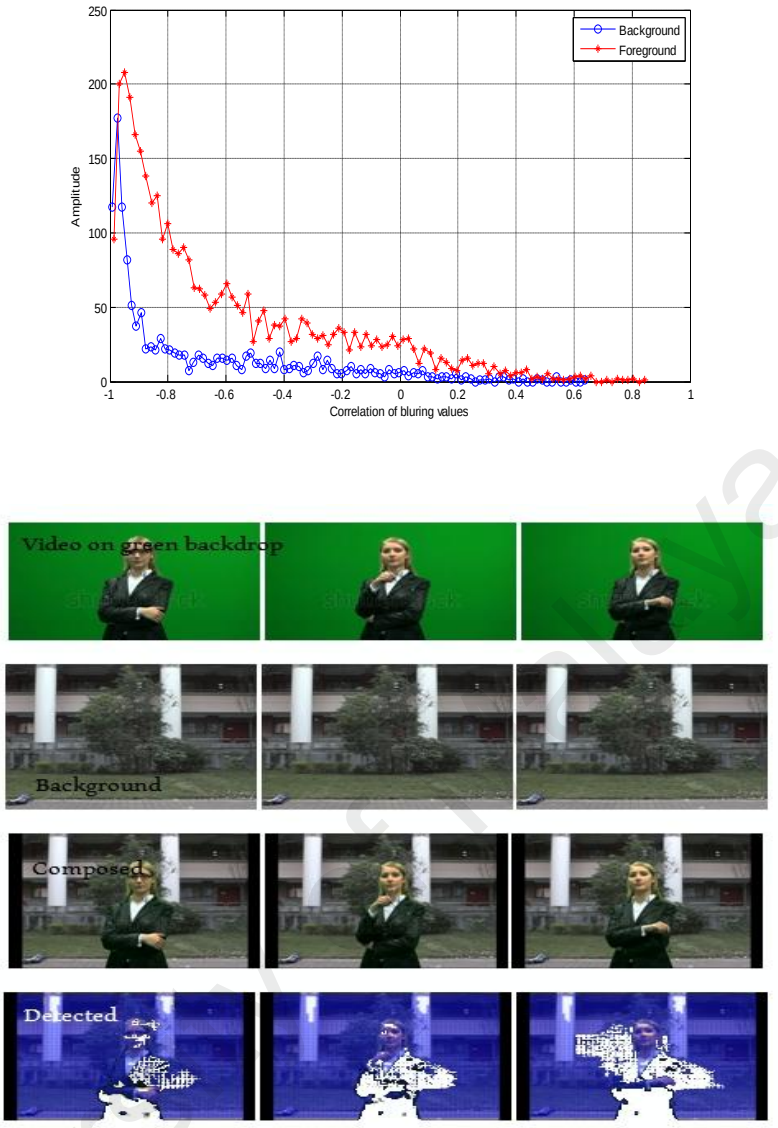

Figure 5.14: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 11

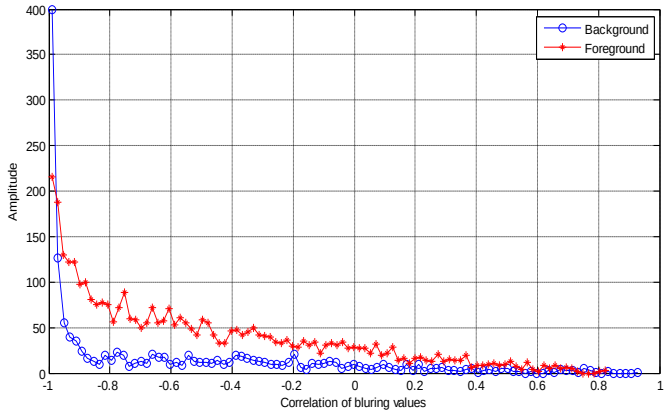

Figure 5.15: Histogram of Blurring Features Correlation and Forged Region Detection fortest Video 12

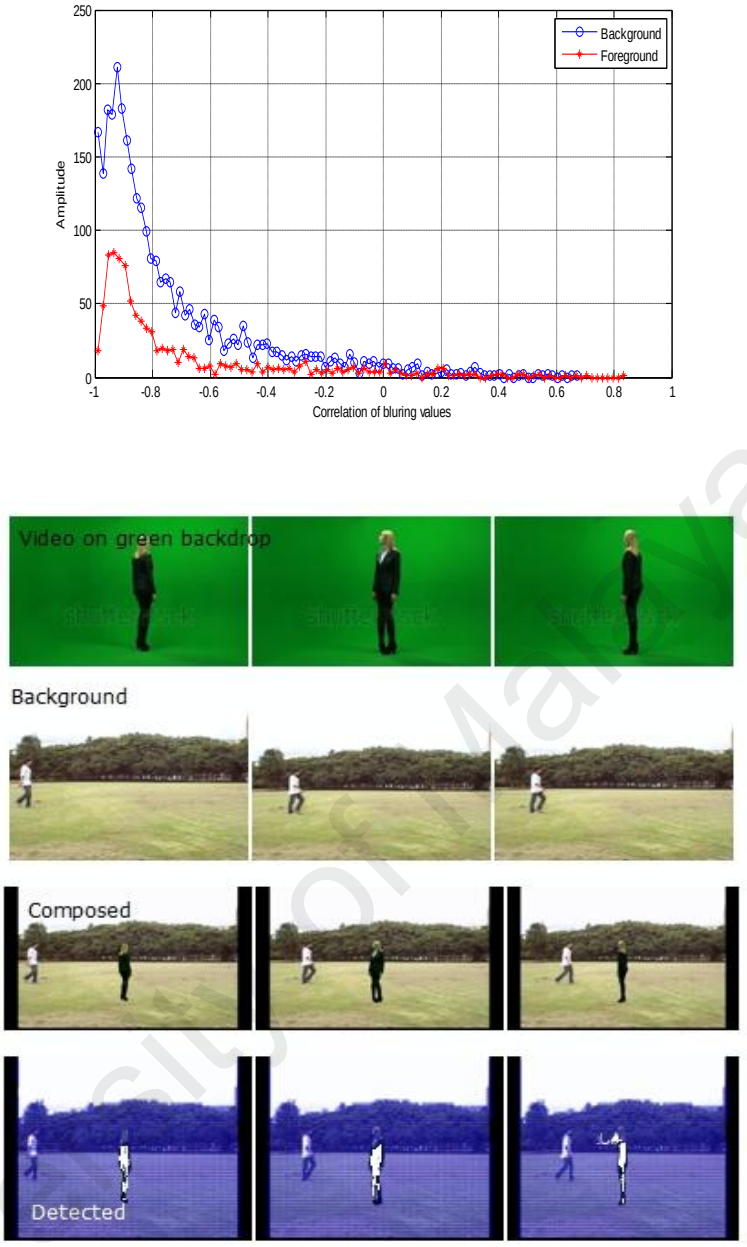

Figure 5.16: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 13

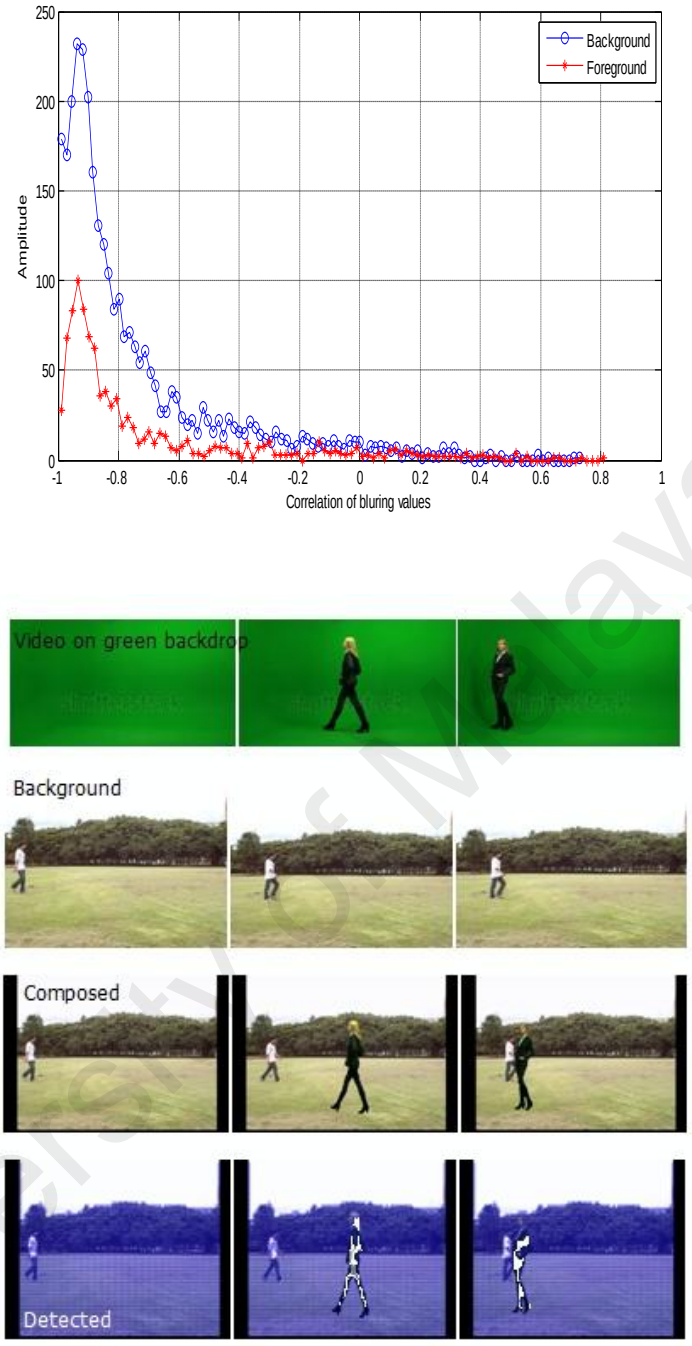

Figure 5.17: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 14

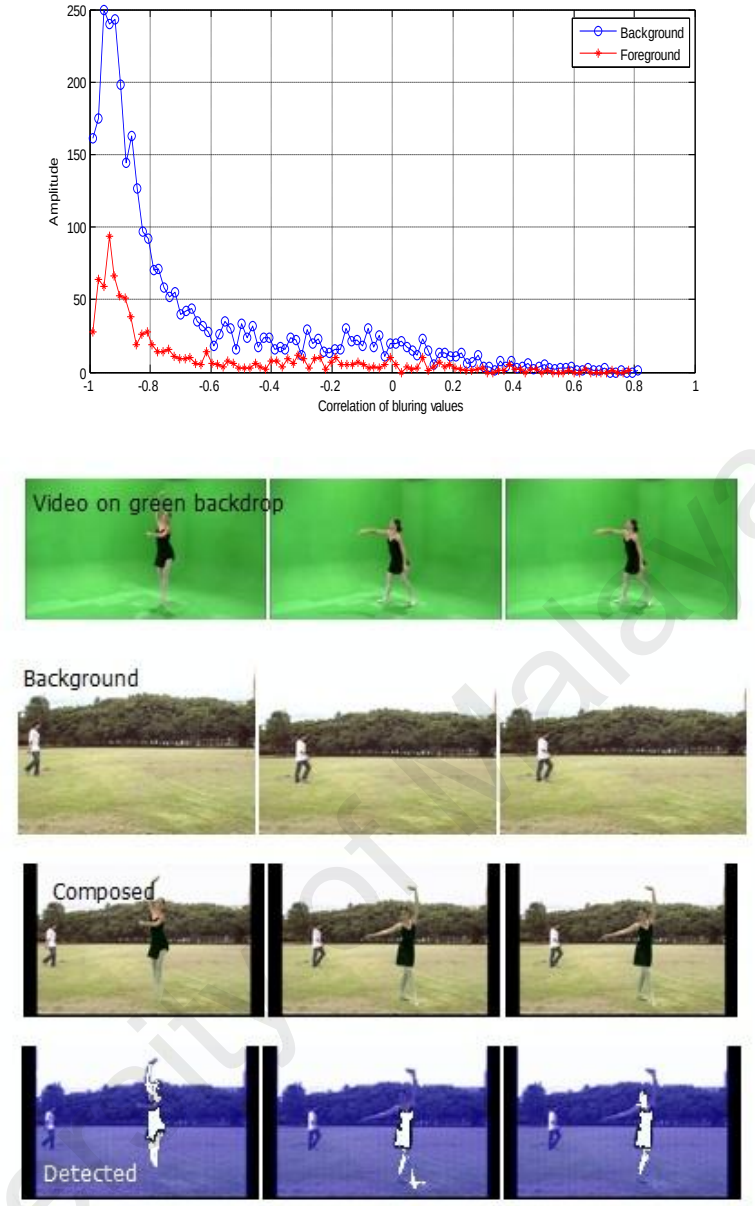

Figure 5.18: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 15

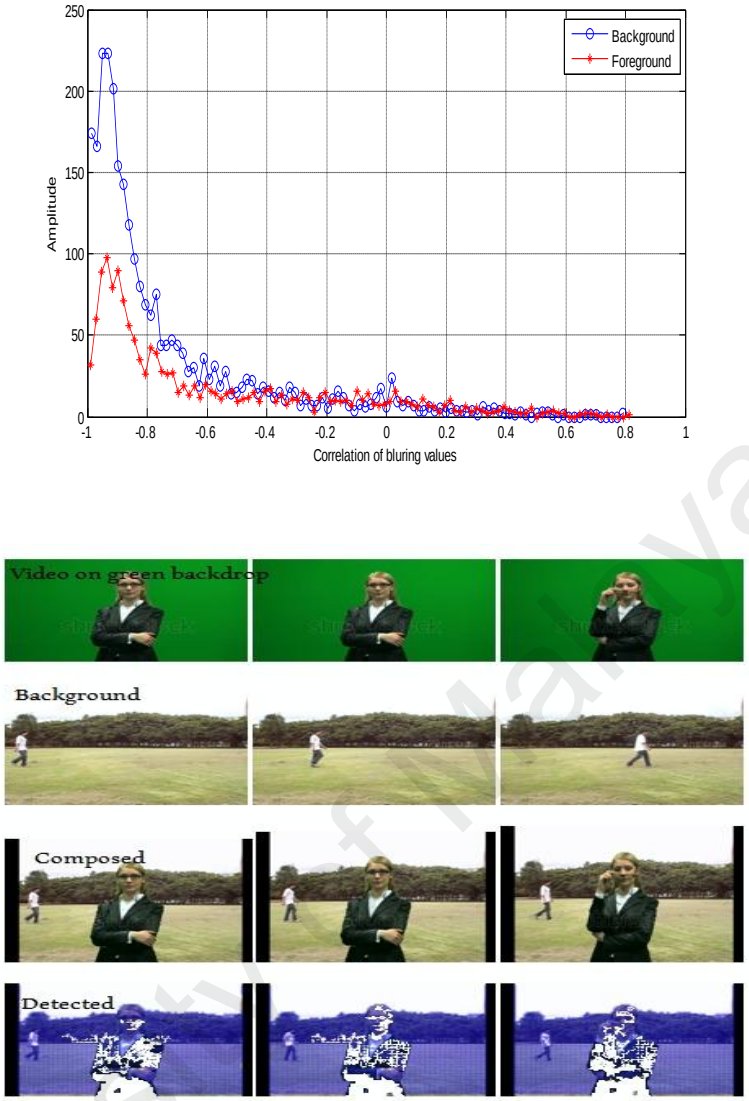

Figure 5.19: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 16

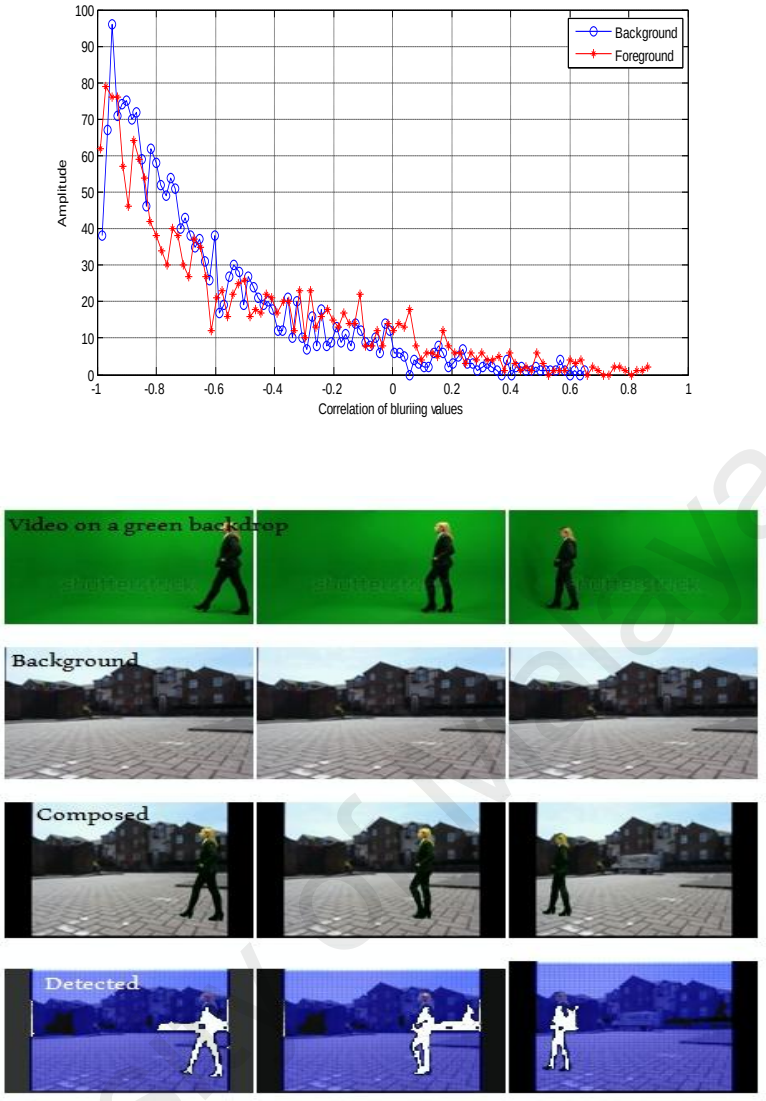

Figure 5.20: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 17

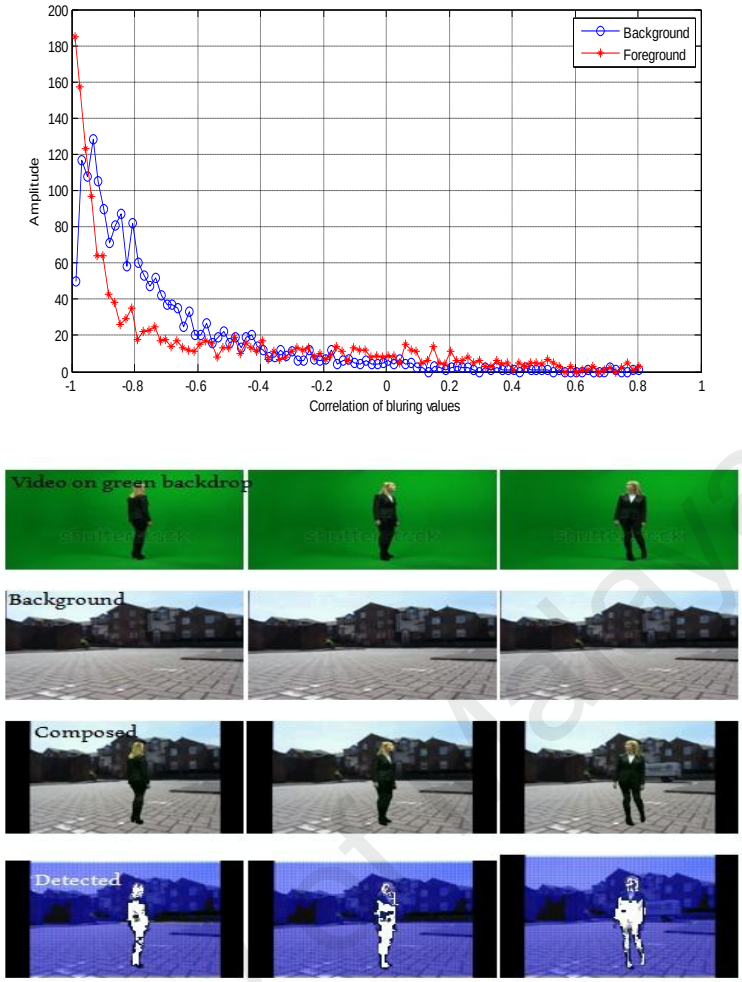

Figure 5.21: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 18

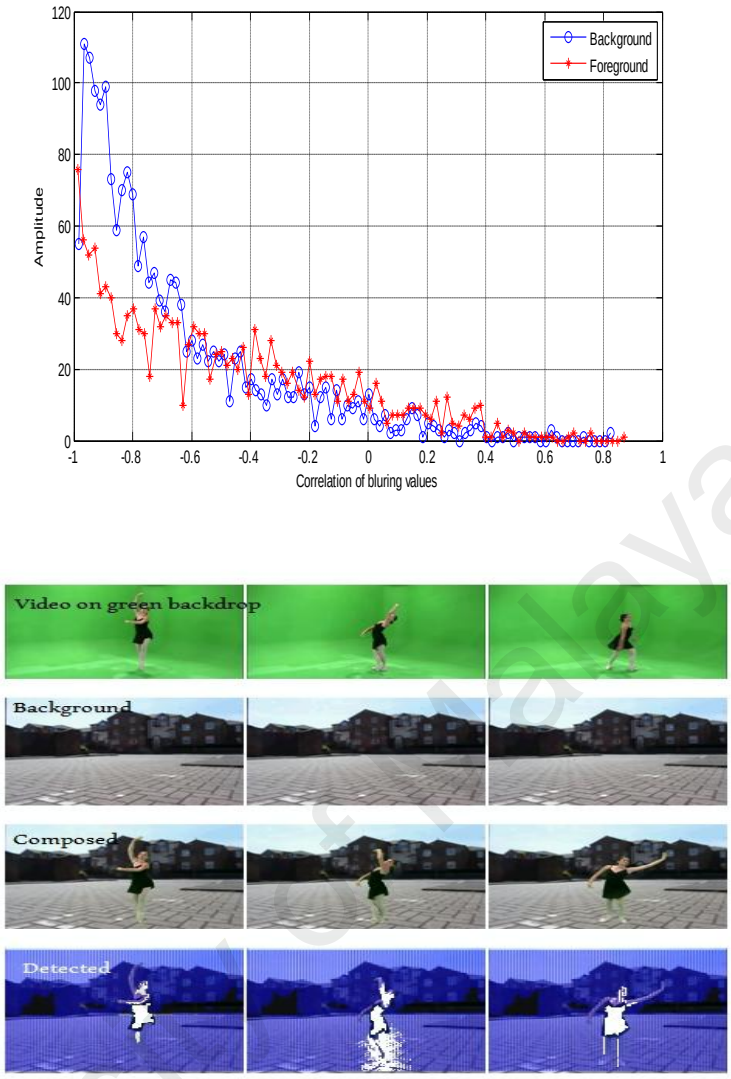

Figure 5.22: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 19

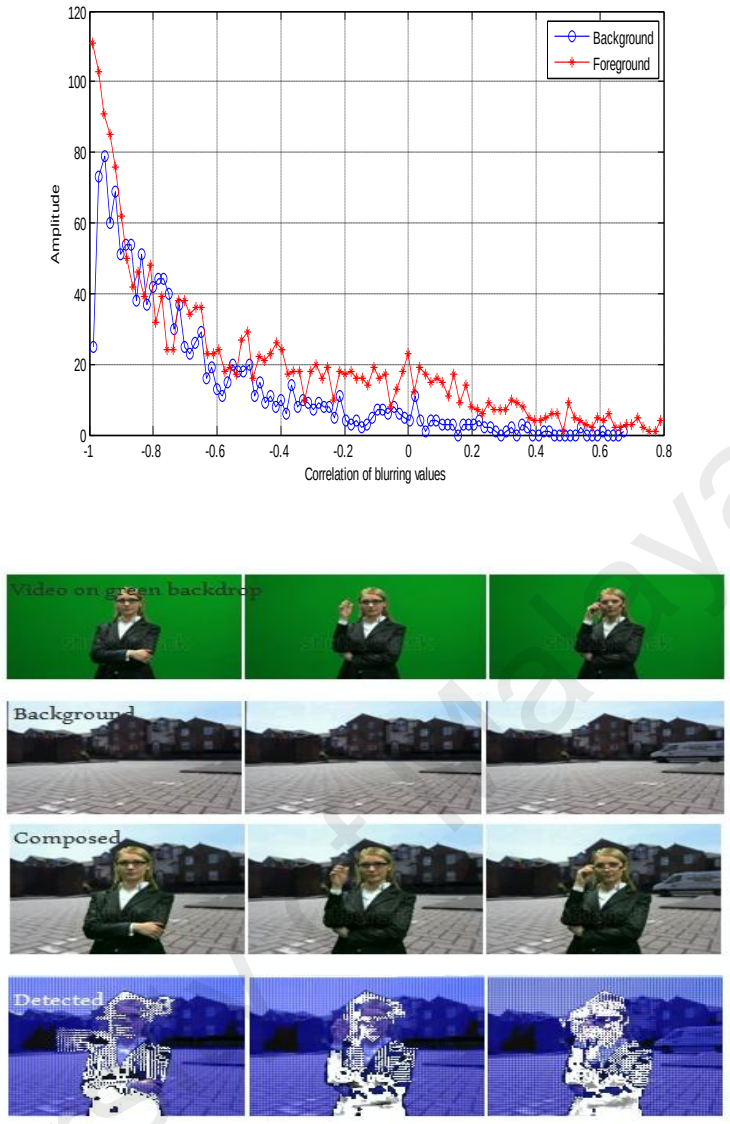

Figure 5.23: Histogram of Blurring Features Correlation and Forged Region Detection forTest Video 20

It will be observed from Figures 5.4 to 5.23 that the blurring features correlations of the two slopes between the background and foreground frame block exhibit a noticeable difference in terms of the peak of their amplitude when a video is composed. This is because when two videos from different sources are matted into a single video, they will normally exhibit difference in blurring quality with respect to their background and foreground pixels. This is as a result of the difference in the cause and degree of blurriness affecting each video as discussed in Section 5.2.2.1.Thus, making the blurring

variations between the videos used for composition a good clue for tamper detection using our proposed technique.

Additionally, to further test the strength of this proposed techniquefor chroma key forgery detection, it was applied, on real movies scenes as the second dataset. Scenes from two movies, in particular the Matrix and the Avengers were utilized for the test purpose and the obtained resultsare shown in Table 5.2.

Table 5.2: Detection Result on Scenes from Movie Extracts

Video	**TPR (%)**	**FPR (%)**
The Matrix Movie Scene	91.08	0.24
The Avengers Movie Scene	90.90	0.65
Average	**90.56**	**0.45**

Figures 5.44 and 5.45 demonstrate the result of the blurring feature correlation between the foreground and background frame blocks for the Matrix and the Avengers movie scenes respectively.

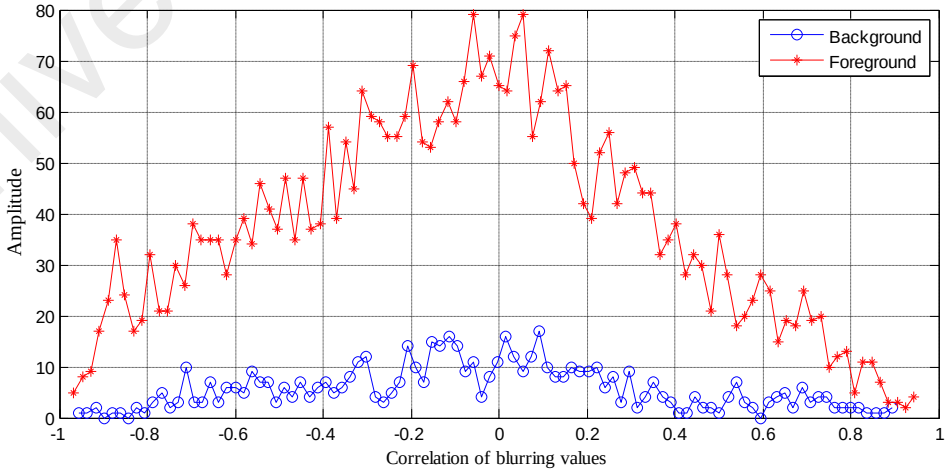

Figure 5.24: Histogram of Blurring Features Correlation for an Extract Scene from the Matrix Movie

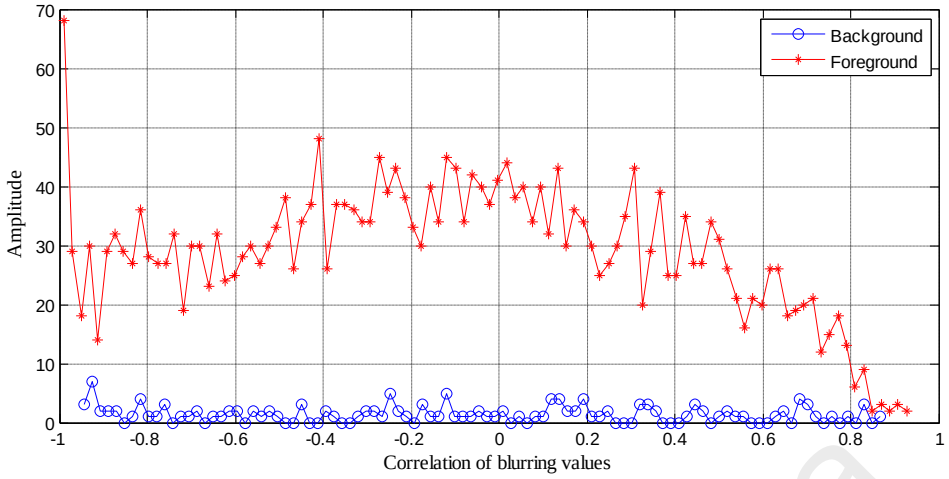

Figure 5.25: Histogram of Blurring Features Correlation for an Extract Scene from the Avengers Movie

The chroma key composition of the scenes from the two movies with the detection result using our proposed technique is shown in Figure 5.26. The white coloured region in the detection result row showsa variation in terms of blurring correlation with other regions of the video, and therefore considered as superimposed on to an original background.

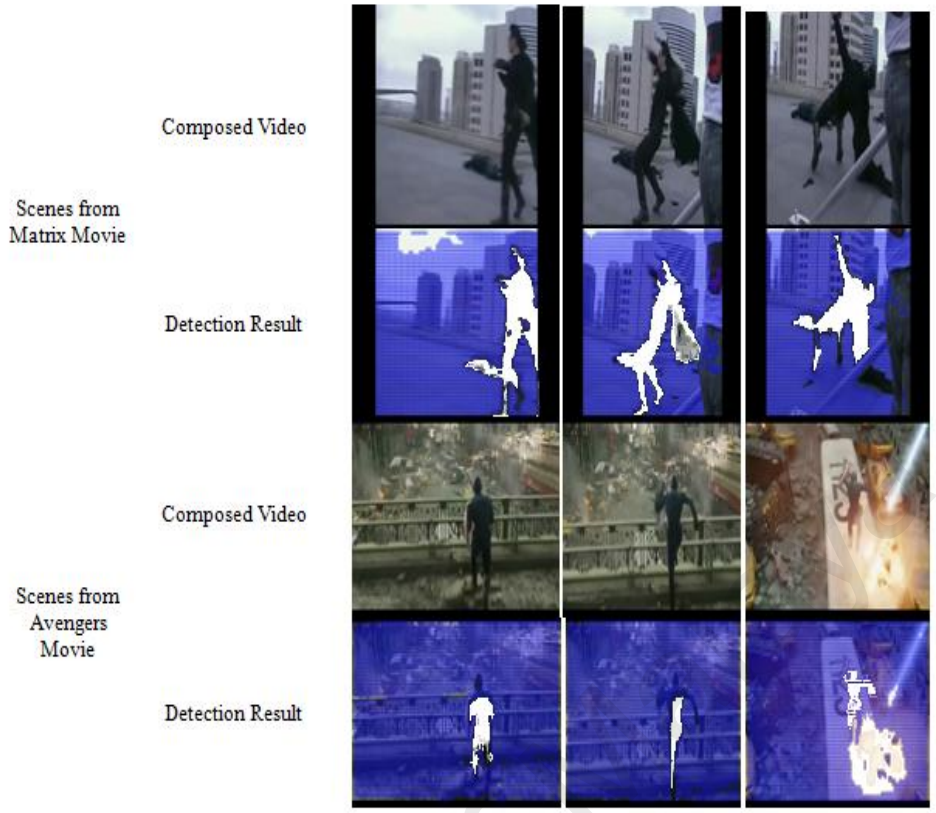

Figure 5.26: Extracts of Composed Movie Scenes and Their Detection Result

Furthermore, this technique was applied to an original video that has not undergone composition, and the detection result obtained is shown in Figure 5.27.

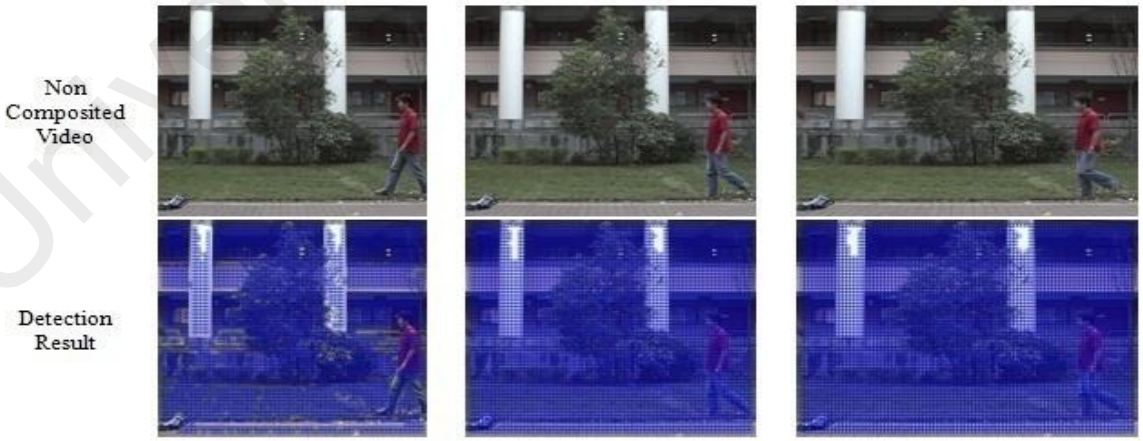

Figure 5.27:Original Video and Detection Result

It can be seen from Figure 5.27 that no significant region of the video foreground is isolated with a purely white background.This indicates that both the blurring

background and foreground have an almost equal correlation, as such signifying the video as not composed.

5.3.2 Comparison with other Detection Techniques

In this section, the performance of this technique is demonstrated by examination of the two existing chroma key detection technique proposed in the work of (Xu et al., 2012) and (Wang & Farid, 2009) using the same data set. To compare this proposed technique with the selected chroma key detection techniques, two metric performance measures were calculated; true positive detection rate (TPR) and false positive detection rate (FPR), which are the commonly used metrics for measuring the performance of forgery detection techniques.The result obtained from the comparison is summarized in Table 5.3.

Table 5.3: Comparison with Other Technique

Reference	Detection Approach	Average TPR (%)	Average FPR (%)
(Xu et al., 2012)	SCQDCT	88	3.24
(Wang & Farid, 2009)	ADQMBs	84.70	2.18
Proposed	SCBA	91.12	1.95

The result of the comparison between the three detection techniques for chroma key forgery had demonstrated that the proposed technique recorded a marginally higher true positive detection rate contrasted with the SCQDCT technique. This is a direct result of the benefit of blurring features as a set up metric that can without much of a stretch connect with the human visual experience.

5.3.3 Discussion

A new technique for the detection of chroma key forgery in a digital video has been presented, based on the statistical correlation of blurring features that are extracted from

a suspected video. The video is divided into multiple frames and each frame is divided into blocks of foreground and background. The blurring features are then extracted from each blocks and the blurring correlation between background and foreground frame blocks is computed. Foreground blocks with variations in blurring feature with the background is isolated as superimposed on to an original background. The technique records high performance in terms of TPR detection especially when the imposed object has a dark colour, for example blue, black and purple. Future work will concentrate on enhancing the reliability of the proposed technique when lighter colours such as white and grey are used for the forgery purpose.

5.4 Chapter Summary

This chapter discusses a contribution that presents a system for detecting chroma key forgery by utilizing the correlation of blurring features that is extracted from a digital video. These tests have demonstrated that the utilization of blurring features to detect chroma key forgery has enhanced the accuracy of chroma key forgery detection. In light of the outcomes in this study, the utilization of blurring feature can be trusted for chroma key forgery detection and this is a valuable artefact for digital video authentication.

CHAPTER 6 :CONCLUSION AND FUTURE WORK

This thesis is concluded by a reconsideration of the objectives set out in chapter one. The goal of this chapter is to provide an important summary of the contribution of this research and also provide a vector for the direction of future research.

6.1 Reappraisal of the Research Objective

The first objective of this study is to develop an efficient and robust technique that could detect inpainting forgery in digital video havingstatic and moving scenes on a stationary background. In order to achieve this objective, the use of the statistical correlation of Hessian matrix feature was proposed that can be extracted from a digital video. Firstly,the video is divided into frames; each frame is further divided into ***NXN*** blocks. The Hessian matrix features from independent frame blocks isextracted. The cross correlation of the Hessian matrix feature between blocks of neighbouring frames is computed thereby generating the histograms of Hessian matrix correlation between blocks of neighbouring frames. Inpainted regions are then identified using a thresholding mechanism.

The second objectiveis to develop an efficient and robust technique that could detect chroma key forgery in digital videos that is performed using either green or blue screen.In order to achieve this objective, the use of the statistical correlation of blurring feature is proposed that can be extracted from a digital video. The video is divided into frames; each frame is further divided into NXN blocks. The blurring feature from the blocks background and foreground are obtained using the wiener deconvolution filter. The cross correlation of the blurring feature between blocks of background and foreground frame blocks are computed thereby generating the histograms of blurring correlation. Super-imposed regions are identified using the variation of background and foreground block correlations.

6.2 Implication of Research

The implication of this research is that the two techniques proposed for video inpainting and chroma key forgery detection would help in ensuring the authenticity of a digital video that may be a suspect of these two kind of forgeries without relying on the pre-embedded information in the video such as a digital watermark which may not always be present in the video. Furthermore, the techniques proposed would also help in providing essential information about a video such as its production technique.In addition to this, new researchers in video forgery detection can also make use of the result from the proposed techniques as a benchmark for newer techniques.

6.3 Originality and Contribution to Body of Knowledge

The original contribution of this research studyto body of knowledge is an implementation of a statistical correlation technique that can be used for video inpainting and chroma key forgery detection in digital videos using proposed novel features that are extracted from a digital video. This is to aid digital forensic experts in the evaluation of the authenticity and validity of a digital video especially when such a video is presented as admissible evidence in courts when relating a suspect to a crime. This would minimize the rate of wrong conviction based on inconclusive digital video evidence.

6.4Future Research Directions

This researchprofits from the advantage of extended research in the area of digital video forensics. With regards to the first contribution for digital video inpainting detection, future research can extend the proposed framework for complex inpainting detection that involves moving object removal on a non-stationary background. The technique proposed in this thesis can only detect inpainting for object removal in a video that is on a static background. Therefore, it will be of great benefit if the proposed

video inpainting forgery detection technique in this study is extended to deal with anon-stationary background.

Concerning the second contribution for chroma key forgery detection, this thesis implements a blurring feature technique, using a block based approach, for feature extraction from video frame blocks. However, issues may arise if both videos used for the matting process have an equal blurring quality. Therefore, it could be useful if another distinctive feature can be used to enhance the reliability of the proposed technique. Another area that may be looked into is the effect of double compression. Double compression of a matted video will affect the blurring distribution in a video by making the blurring effect of tampered and non-tampered region uniform in most of the regions of the video. Although, the proposed technique will also be useful in the case of double compressed forged videos, however the accuracy of the technique would be reduced.

Finally, looking from an implementation point of view, the amalgamation of the proposed techniques for video inpainting forgery detection with other forgery detection systems, as an integrated module, will also be of great benefit. This will exploit the advantages of different kinds of video forgery detection techniques, and increase overall detection accuracy.

REFERENCES

Aaboe, A., & Aaboe, A. (1964). *Episodes from the early history of mathematics* (Vol. 13): Mathematical Association of America Washington, DC.

Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice.* Murdoch University.

Adelson, E. H. (1990). Digital signal encoding and decoding apparatus: Google Patents.

Amer, A., & Schroder, H. (1996). *A new video noise reduction algorithm using spatial subbands.* Paper presented at the Electronics, Circuits, and Systems, 1996. ICECS'96., Proceedings of the Third IEEE International Conference on.

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A sift-based forensic method for copy–move attack detection and transformation recovery. *Information Forensics and Security, IEEE Transactions on, 6*(3), 1099-1110.

Antonini, M., Barlaud, M., Mathieu, P., & Daubechies, I. (1992). Image coding using wavelet transform. *Image Processing, IEEE Transactions on, 1*(2), 205-220.

Arai, I., Hori, M., Kawai, N., Abe, Y., Ichikawa, M., Satonaka, Y., . . . Mukai, M. (2010). Pano UMECHIKA: A crowded underground city panoramic view system *Distributed Computing and Artificial Intelligence* (pp. 173-180): Springer.

Barghout, L., & Sheynin, J. (2013). Real-world scene perception and perceptual organization: Lessons from Computer Vision. *Journal of Vision, 13*(9), 709-709.

Bay, H., Ess, A., Tuytelaars, T., & Van Gool, L. (2008). Speeded-up robust features (SURF). *Computer vision and image understanding, 110*(3), 346-359.

Bertalmio, M., Sapiro, G., Caselles, V., & Ballester, C. (2000). *Image inpainting.* Paper presented at the Proceedings of the 27th annual conference on Computer graphics and interactive techniques.

Bestagini, P., Milani, S., Tagliasacchi, M., & Tubaro, S. (2013). *Local tampering detection in video sequences.* Paper presented at the Multimedia Signal Processing (MMSP), 2013 IEEE 15th International Workshop on.

Boddington, R., Hobbs, V., & Mann, G. (2008). Validating digital evidence for legal argument.

Bornard, R., Lecan, E., Laborelli, L., & Chenot, J.-H. (2002). *Missing data correction in still images and image sequences.* Paper presented at the Proceedings of the tenth ACM international conference on Multimedia.

Brassil, J. T., Low, S., Maxemchuk, N. F., & O'Gorman, L. (1995). Electronic marking and identification techniques to discourage document copying. *Selected Areas in Communications, IEEE Journal on, 13*(8), 1495-1504.

BROAD, W. J. (2009). http://www.nytimes.com/2009/05/05/science/05tesla.html.

Casey, E. (2011). *Digital evidence and computer crime: forensic science, computers and the internet*: Academic press.

Chen, R., Dong, Q., Ren, H., & Fu, J. (2012). Video forgery detection based on non-subsampled Contourlet transform and gradient information. *Information Technology Journal, 11*(10), 1456-1462.

Cheng, M., Mitra, N. J., Huang, X., Torr, P. H., & Hu, S. (2015). Global contrast based salient region detection. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 37*(3), 569-582.

Cheong, H.-Y., Tourapis, A. M., Llach, J., & Boyce, J. (2004). *Adaptive spatio-temporal filtering for video denoising.* Paper presented at the Image Processing, 2004. ICIP'04. 2004 International Conference on.

Chuang, W.-H., Su, H., & Wu, M. (2011). *Exploring compression effects for improved source camera identification using strongly compressed video.* Paper presented at the Image Processing (ICIP), 2011 18th IEEE International Conference on.

Coe, B. (1977). *The birth of photography: the story of the formative years, 1800-1900*: Taplinger Publishing Company.

Cole, B. (1991). *Art of the Western World: From Ancient Greece to Post Modernism*: Simon and Schuster.

Criminisi, A., Perez, P., & Toyama, K. (2003). *Object removal by exemplar-based inpainting.* Paper presented at the Computer Vision and Pattern Recognition, 2003. Proceedings. 2003 IEEE Computer Society Conference on.

Das, S., Shreyas, G. D., & Devan, L. D. (2012). Blind Detection Method for Video Inpainting Forgery.

De, A., Chadha, H., & Gupta, S. (2006). *Detection of forgery in digital video.* Paper presented at the The 10th World Multi Conference on Systemics Cybernetics and Informatics.

Dollár, P., Rabaud, V., Cottrell, G., & Belongie, S. (2005). *Behavior recognition via sparse spatio-temporal features.* Paper presented at the Visual Surveillance and Performance Evaluation of Tracking and Surveillance, 2005. 2nd Joint IEEE International Workshop on.

Efros, A. A., & Leung, T. K. (1999). *Texture synthesis by non-parametric sampling.* Paper presented at the Computer Vision, 1999. The Proceedings of the Seventh IEEE International Conference on.

Foster, J. (2010). *The green screen handbook: real-world production techniques*: John Wiley & Sons.

Frangi, A. F., Niessen, W. J., Vincken, K. L., & Viergever, M. A. (1998). Multiscale vessel enhancement filtering *Medical Image Computing and Computer-Assisted Interventation—MICCAI'98* (pp. 130-137): Springer.

Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). *Detection of copy-move forgery in digital images.* Paper presented at the in Proceedings of Digital Forensic Research Workshop.

Goldstein, J. S., Reed, I. S., & Scharf, L. L. (1998). A multistage representation of the Wiener filter based on orthogonal projections. *Information Theory, IEEE Transactions on, 44*(7), 2943-2959.

Gopi, E., Lakshmanan, N., Gokul, T., KumaraGanesh, S., & Shah, P. R. (2006). *Digital image forgery detection using artificial neural network and auto regressive coefficients.* Paper presented at the Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on.

Grigoras, C. (2009). Applications of ENF analysis in forensic authentication of digital audio and video recordings. *Journal of the Audio Engineering Society, 57*(9), 643-661.

Hartung, F., & Girod, B. (1998). Watermarking of uncompressed and compressed video. *Signal processing, 66*(3), 283-301.

Heeger, D. J., & Bergen, J. R. (1995). *Pyramid-based texture analysis/synthesis.* Paper presented at the Proceedings of the 22nd annual conference on Computer graphics and interactive techniques.

Hsu, C.-C., Hung, T.-Y., Lin, C.-W., & Hsu, C.-T. (2008). *Video forgery detection using correlation of noise residue.* Paper presented at the Multimedia Signal Processing, 2008 IEEE 10th Workshop on.

Jain, A. K. (1987). Advances in statistical pattern recognition *Pattern recognition theory and applications* (pp. 1-19): Springer.

Kalker, T., & Haitsma, J. (2000). *Efficient detection of a spatial spread-spectrum watermark in MPEG video streams.* Paper presented at the Image Processing, 2000. Proceedings. 2000 International Conference on.

Kancherla, K., & Mukkamala, S. (2012). Novel blind video forgery detection using markov models on motion residue *Intelligent Information and Database Systems* (pp. 308-315): Springer.

Khan, S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A. W. A., & Bagiwa, M. A. (2014a, 2-4 Sept. 2014). *Forensic challenges in mobile cloud computing.* Paper presented at the Computer, Communications, and Control Technology (I4CT), 2014 International Conference on.

Khan, S., Shiraz, M., Abdul Wahab, A. W., Gani, A., Han, Q., & Bin Abdul Rahman, Z. (2014b). A Comprehensive Review on Adaptability of Network Forensics Frameworks for Mobile Cloud Computing. *The Scientific World Journal, 2014*, 27. doi: 10.1155/2014/547062

Kobayashi, M., Okabe, T., & Sato, Y. (2009). Detecting video forgeries based on noise characteristics *Advances in Image and Video Technology* (pp. 306-317): Springer.

Kong, X., Liu, Y., Liu, H., & Yang, D. (2004). Object watermarks for digital images and video. *Image and Vision Computing, 22*(8), 583-595.

Kumar, G., & Bhatia, P. K. (2014). *A detailed review of feature extraction in image processing systems.* Paper presented at the Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on.

Lee, S. U., Chung, S. Y., & Park, R. H. (1990). A comparative performance study of several global thresholding techniques for segmentation. *Computer Vision, Graphics, and Image Processing, 52*(2), 171-190.

Levy, K. L. (2007). Time-varying video watermark: Google Patents.

Li, L., Dong, Z., Lu, J., Dai, J., Huang, Q., Chang, C.-C., & Wu, T. (2015). AN H. 264/AVC HDTV watermarking algorithm robust to camcorder recording. *Journal of Visual Communication and Image Representation, 26*, 1-8.

Li, L., Wang, X., Zhang, W., Yang, G., & Hu, G. (2013). Detecting removed object from video with stationary background *Digital Forensics and Watermaking* (pp. 242-252): Springer.

Li, W., Zhang, D., & Xu, Z. (2003). Image alignment based on invariant features for palmprint identification. *Signal Processing: Image Communication, 18*(5), 373-379.

Lie, W.-N., Lin, T.-I., & Cheng, S.-L. (2006). Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques. *Information Forensics and Security, IEEE Transactions on, 1*(3), 330-341.

Lin, C.-S., & Tsay, J.-J. (2013). *Passive approach for video forgery detection and localization.* Paper presented at the The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013).

Lin, C.-S., & Tsay, J.-J. (2014). A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. *Digital Investigation, 11*(2), 120-140.

Lisin, D., Mattar, M., Blaschko, M. B., Learned-Miller, E. G., & Benfield, M. C. (2005). *Combining local and global image features for object class recognition.* Paper presented at the Computer Vision and Pattern Recognition-Workshops, 2005. CVPR Workshops. IEEE Computer Society Conference on.

Lowe, D. G. (1999). *Object recognition from local scale-invariant features.* Paper presented at the Computer vision, 1999. The proceedings of the seventh IEEE international conference on.

Lu, C.-S., Chen, J.-R., & Fan, K.-C. (2005). Real-time frame-dependent video watermarking in VLC domain. *Signal Processing: Image Communication, 20*(7), 624-642.

Lu, C.-S., & Liao, H.-Y. (2001). Multipurpose watermarking for image authentication and protection. *Image Processing, IEEE Transactions on, 10*(10), 1579-1592.

Mairal, J., Sapiro, G., & Elad, M. (2007). *Multiscale sparse image representationwith learned dictionaries.* Paper presented at the Image Processing, 2007. ICIP 2007. IEEE International Conference on.

Mıhçak, M. K., Kozintsev, I., & Ramchandran, K. (1999). *Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising.* Paper presented at the Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on.

Muthukumar, S. (2010). Analysis of image inpainting techniques with exemplar, poisson, successive elimination and 8 pixel neighborhood methods. *Analysis, 9*(11).

Olivier, M. S. (2009). On metadata context in database forensics. *Digital Investigation, 5*(3), 115-123.

Olshausen, B. A. (1996). Emergence of simple-cell receptive field properties by learning a sparse code for natural images. *Nature, 381*(6583), 607-609.

Palmer, G. (2001). A road map for digital forensics research-report from the first Digital Forensics Research Workshop (DFRWS). *Utica, New York*.

Pathak, A., & Patil, D. (2014). Video Forgery Detection Based on Variance in Luminance and Signal to Noise Ratio using LESH Features and Bispectral Analysis.

Pilant, L. (1999). Electronic Evidence Recovery. *Police Chief, 66*(2), 37-38.

Poisel, R., & Tjoa, S. (2011). *Forensics investigations of multimedia data: A review of the state-of-the-art.* Paper presented at the IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on.

Porter, S. V., Mirmehdi, M., & Thomas, B. T. (2000). *Video cut detection using frequency domain correlation.* Paper presented at the Pattern Recognition, 2000. Proceedings. 15th International Conference on.

Qadir, G., Yahaya, S., & Ho, A. T. (2012). Surrey university library for forensic analysis (SULFA) of video content.

Rieder, P., Gotze, J., Nossek, J. A., & Burrus, C. S. (1998). Parameterization of orthogonal wavelet transforms and their implementation. *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on, 45*(2), 217-226.

Rieder, P., & Scheffler, G. (2001). New concepts on denoising and sharpening of video signals. *Consumer Electronics, IEEE Transactions on, 47*(3), 666-671.

Rigoni, R., Freitas, P. G., & Farias, M. C. (2016). Detecting tampering in audio-visual content using QIM watermarking. *Information Sciences, 328*, 127-143.

Rocha, A., Scheirer, W., Boult, T., & Goldenstein, S. (2011). Vision of the unseen: Current trends and challenges in digital image and video forensics. *ACM Computing Surveys (CSUR), 43*(4), 26.

Rusu, R. B., & Cousins, S. (2011). *3d is here: Point cloud library (pcl).* Paper presented at the Robotics and Automation (ICRA), 2011 IEEE International Conference on.

Ryan, D. J., & Shpantzer, G. (2002). *Legal aspects of digital forensics.* Paper presented at the Proceedings: Forensics Workshop.

S Mahajan, K., & Vaidya, M. (2012). Image in Painting Techniques: A survey. *IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Vol, 5*, 45-49.

Sahoo, P. K., Soltani, S., & Wong, A. K. (1988). A survey of thresholding techniques. *Computer Vision, Graphics, and Image Processing, 41*(2), 233-260.

Sato, Y., Nakajima, S., Atsumi, H., Koller, T., Gerig, G., Yoshida, S., & Kikinis, R. (1997). *3D multi-scale line filter for segmentation and visualization of curvilinear structures in medical images.* Paper presented at the CVRMed-MRCAS'97.

Schindelin, J., Arganda-Carreras, I., Frise, E., Kaynig, V., Longair, M., Pietzsch, T., . . . Schmid, B. (2012). Fiji: an open-source platform for biological-image analysis. *Nature methods, 9*(7), 676-682.

Shapiro, L., & Stockman, G. C. (2001). Computer Vision. 2001. *ed: Prentice Hall*.

Shen, J., & Chan, T. F. (2002). Mathematical models for local nontexture inpaintings. *SIAM Journal on Applied Mathematics, 62*(3), 1019-1043.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2013). *Operating system concepts* (Vol. 8): Wiley.

Sinha, S. N., Frahm, J.-M., Pollefeys, M., & Genc, Y. (2006). *GPU-based video feature tracking and matching.* Paper presented at the EDGE, Workshop on Edge Computing Using New Commodity Architectures.

Steder, B., Rusu, R. B., Konolige, K., & Burgard, W. (2011). *Point feature extraction on 3D range scans taking into account object boundaries.* Paper presented at the Robotics and automation (icra), 2011 ieee international conference on.

Su, K., Kundur, D., & Hatzinakos, D. (2001). *A content dependent spatially localized video watermark for resistance to collusion and interpolation attacks.* Paper presented at the Image Processing, 2001. Proceedings. 2001 International Conference on.

Su, P.-C., Wu, C.-S., Chen, I.-F., Wu, C.-Y., & Wu, Y.-C. (2011). A practical design of digital video watermarking in H. 264/AVC for content authentication. *Signal Processing: Image Communication, 26*(8), 413-426.

Su, Y., Zhang, J., Han, Y., Chen, J., & Liu, Q. (2010). Exposing digital video logo-removal forgery by inconsistency of blur. *International Journal of Pattern Recognition and Artificial Intelligence, 24*(07), 1027-1046.

Su, Y., Zhang, J., & Liu, J. (2009). *Exposing digital video forgery by detecting motion-compensated edge artifact.* Paper presented at the Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on.

Subramanyam, A., & Emmanuel, S. (2013). *Pixel estimation based video forgery detection.* Paper presented at the Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on.

Uzunay, Y., Incebacak, D., & Bicakci, K. (2007). Towards Trustable Digital Evidence with PKIDEV: PKI Based Digital Evidence Verification Model *EC2ND 2006* (pp. 105-114): Springer.

van Houten, W., Geradts, Z., Franke, K., & Veenman, C. (2010). Verification of video source camera competition (camcom 2010) *Recognizing Patterns in Signals, Speech, Images and Videos* (pp. 22-28): Springer.

Wang, L., Wang, X., & Feng, J. (2006). On image matrix based feature extraction algorithms. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 36*(1), 194-197.

Wang, W., & Farid, H. (2009). *Exposing digital forgeries in video by detecting double quantization.* Paper presented at the Proceedings of the 11th ACM workshop on Multimedia and security.

Wexler, Y., Shechtman, E., & Irani, M. (2004). *Space-time video completion.* Paper presented at the Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on.

Wexler, Y., Shechtman, E., & Irani, M. (2007). Space-time completion of video. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29*(3), 463-476.

Xu, J., Yu, Y., Su, Y., Dong, B., & You, X. (2012). Detection of blue screen special effects in videos. *Physics Procedia, 33*, 1316-1322.

Xu, Z., & Sun, J. (2010). Image inpainting by patch propagation using patch sparsity. *Image Processing, IEEE Transactions on, 19*(5), 1153-1165.

Yang, J., Wright, J., Huang, T., & Ma, Y. (2008). *Image super-resolution as sparse representation of raw image patches.* Paper presented at the Computer Vision and Pattern Recognition, 2008. CVPR 2008. IEEE Conference on.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy, 1*(4), 15-23.

Zhang, J., Li, J., & Zhang, L. (2001). *Video watermark technique in motion vector.* Paper presented at the Computer Graphics and Image Processing, 2001 Proceedings of XIV Brazilian Symposium on.

Zhang, J., & Su, Y. (2009). *Detecting logo-removal forgery by inconsistencies of blur.* Paper presented at the Industrial Mechatronics and Automation, 2009. ICIMA 2009. International Conference on.

Zhang, J., Su, Y., & Zhang, M. (2009). *Exposing digital video forgery by ghost shadow artifact.* Paper presented at the Proceedings of the First ACM workshop on Multimedia in forensics.

Zhi-yu, H., & Xiang-hong, T. (2011). *Integrity authentication scheme of color video based on the fragile watermarking.* Paper presented at the Electronics, Communications and Control (ICECC), 2011 International Conference on.

Zlokolica, V., Pižurica, A., & Philips, W. (2006). Wavelet-domain video denoising based on reliability measures. *Circuits and Systems for Video Technology, IEEE Transactions on, 16*(8), 993-1007.

LIST OF PUBLICATIONS, PAPERS PRESENTED AND ACHIEVEMENTS

Articles on Research Topic

1. Mustapha Aminu Bagiwa, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Suleman Khan, Digital Video Inpainting Detection Using Correlation of Hessian Matrix (2016). Malaysian Journal of Computer Science, 29(3). (*ISI-Cited Publication*).
2. Mustapha Aminu Bagiwa, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Suleman Khan, Kim-Kwang Raymond Choo. Chroma Key Background Detection for Digital Video Using Statistical Correlation of Blurring Artifact (2016). Journal of Digital Investigation, 19, pp.29-43. (*ISI-Cited Publication*).

Conference Proceedings on Research Topic

1. Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan, Zaidi Razak, Muhammad Rezal Kamel Ariffin. 2014. Passive Video Forgery Detection Techniques: A Survey. 10th International Conference on Information Assurance and Security (IAS 2014), Okinawa, Japan; 29-34.

Articles in Collaboration with Group Members

1. Suleman khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Muhammad Shiraz, Mustapha Aminu Bagiwa, Samee U. Khan, Raj Kumar Buyya, and Albert Y. Zomaya. (2016). Cloud Log Forensics: Foundations, State-of-the-art, and Future Directions, ACM Computing Surveys. (*ISI-Cited Publication*). Q1

Conference Proceedings in Collaboration with Group Members

1. Khan, S. Ahmad, E. Shiraz, M. Gani, A. Wahab, A.W. A. Bagiwa, M. A. (2014). Forensic challenges in mobile cloud computing. IEEE International conference on Computer, Communications, and Control Technology (I4CT), Malaysia. pp. 343-347, 2nd-4th September 2014. doi: 10.1109/I4CT.2014.6914202.
2. Khan, S., Gani, A., Wahab, A. W. A., & Bagiwa, M. A. (2015, June). SIDNFF: Source identification network forensics framework for cloud computing. IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE (pp. 418-419).
3. Suleman khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Ahmed AbdelAziz, Mustapha Aminu Bagiwa, FML: A novel Forensics Management Layer for Software Defined Networks, IEEE 6th International Conference on Cloud system and Big Data Engineering Confluence-2016, Noida, Uttar Pardesh, India, 2016.

Seminars

1. Postgraduate Research Excellence Symposium (PGRes) Held in Faculty of Computer Science and Information Technology, Universiti Malaya. Malaysia. May, 2014.
2. Postgraduate Research Excellence Symposium (PGRes) Held in Faculty of Computer Science and Information Technology, Universiti Malaya. Malaysia. June, 2015.

Awards

1. **Gold Medal -** GSceenINQUIRE: Green Screen Identification Module, National Invention, Innovation, Design & Research (NIIDR), 2015, (NATIONAL).
2. **1st Place** (RM500 + trophy + certificate) award for 3 Minutes Thesis Competition. March 2016. Faculty Level. Faculty of Computer Science and Information Technology, University of Malaya.
3. **1st Place and UM3MT Champion 2016** (RM3000 + trophy + certificate) award for 3 Minutes Thesis Competition. April 2016. University Level. University of Malaya.
4. Certificate of Participation. National Malaysia 3MT Competition held at University Utara Malaysia. May 2016

Intellectual Property Rights

1. Method and System for Digital Video Inpainting Detection, **Patent Pending**, PI 2015704794, 2015, (International).
2. Method of Detecting Chroma Key Background in Video Composition, **Patent Pending**, PI 2016700558, 2016, (International).