VIDEO COPY-MOVE FORGERY DETECTION SCHEME BASED ON DISPLACEMENT PATHS

OMAR ISMAEL IBRAHIM

A thesis submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2017

To the Source of Kindness Who Provided Me with Ambition,
My Parents "Assoc. Prof Dr. Ismael and Mrs. Asma".

To My Beloved Wife "Amina", for her Love and Support this Research Would Have Never Been Completed.

To My Brother "Ibrahim" and My Sisters "Noor" and "Marwa" for being patience, supportive, and understanding.

To all my family, my relatives and friends receives my deepest gratitude and love for their patience and support during the years of my study.

ACKNOWLEDGEMENT

Thanks to Allah SWT for everything I was able to achieve and for everything I tried but I was not able to achieve.

First of all, I would like to take this opportunity to gratefully acknowledge the wholehearted supervision of Professor Dr. Ghazali bin Sulong during this work. His dedication, skillful guidance, helpful suggestions and constant encouragement made it possible for me to deliver a dissertation of appreciable quality and standard.

I am forever indebted to my parents for their patience and understanding, alleviating my family responsibilities and encouraging me to concentrate on my study.

Finally, and most importantly, I would like to express special thanks to my brothers, sisters and friends for their support when it was most required. Without their help and encouragement, this study would not have been completed.

In addition, I want to thank my beloved friends Dr. Mohammed Al-Ali, Dr. Ahmed Abdullah Ahmed, Dr. Akeel Shebeeb, Dr. Mohamed Shaban, Dr. Saeed Al Hameed, and Omar Alzaide for their constant support through good and bad times. Thank you for being the friend that I always wanted, I always needed and I always deserved Finally, I would like to offer my special thanks to the faculty of computing staff, your help will never be forgotten.

ABSTRACT

Sophisticated digital video editing tools has made it easier to tamper real videos and create perceptually indistinguishable fake ones. Even worse, some post-processing effects, which include object insertion and deletion in order to mimic or hide a specific event in the video frames, are also prevalent. Many attempts have been made to detect such as video copy-move forgery to date; however, the accuracy rates are still inadequate and rooms for improvement are wide-open and its effectiveness is confined to the detection of frame tampering and not localization of the tampered regions. Thus, a new detection scheme was developed to detect forgery and improve accuracy. The scheme involves seven main steps. First, it converts the red, green and blue (RGB) video into greyscale frames and treats them as images. Second, it partitions each frame into non-overlapping blocks of sized 8x8 pixels each. Third, for each two successive frames (S2F), it tracks every block's duplicate using the proposed two-tier detection technique involving Diamond search and Slantlet transform to locate the duplicated blocks. Fourth, for each pair of the duplicated blocks of the S2F, it calculates a displacement using optical flow concept. Fifth, based on the displacement values and empirically calculated threshold, the scheme detects existence of any deleted objects found in the frames. Once completed, it then extracts the moving object using the same threshold-based approach. Sixth, a frame-by-frame displacement tracking is performed to trace the object movement and find a displacement path of the moving object. The process is repeated for another group of frames to find the next displacement path of the second moving object until all the frames are exhausted. Finally, the displacement paths are compared between each other using Dynamic Time Warping (DTW) matching algorithm to detect the cloning object. If any pair of the displacement paths are perfectly matched then a clone is found. To validate the process, a series of experiments based on datasets from Surrey University Library for Forensic Analysis (SULFA) and Video Tampering Dataset (VTD) were performed to gauge the performance of the proposed scheme. The experimental results of the detection scheme were very encouraging with an accuracy rate of 96.86%, which markedly outperformed the state-of-the-art methods by as much as 3.14%.

ABSTRAK

Kecanggihan alat penyuntingan video digital telah membuat lebih mudah untuk mengubah video gangguan sebenar dan memalsukannya supaya ia tidak dapat dibezakan. Lebih buruk lagi, terdapat beberapa kesan pasca-pemprosesan, yang berleluasa termasuk sisipan dan penghapusan objek untuk meniru atau menyembunyikan peristiwa tertentu dalam bingkai video. Pelbagai cubaan telah dibuat untuk mengesan pemalsuan video salinan-langkah sehingga kini; walau bagaimanapun, kadar ketepatan masih tidak mencukupi dan ruang untuk penambahbaikan adalah terbuka luas dan keberkesanannya terbatas kepada pengesanan bingkai dan kawasan setempat yang tidak diganggu. Oleh itu, satu skim pengesanan baru telah dibangunkan untuk mengesan pemalsuan dan meningkatkan ketepatan. Skim ini melibatkan tujuh langkah utama. Pertama, ia menukarkan video merah, hijau dan biru (RGB) ke dalam bingkai skala kelabu dan menganggap mereka sebagai imej. Kedua, ia menyekat setiap bingkai ke dalam blok bukan pertindihan piksel setiap satu bersaiz 8x8. Ketiga, bagi setiap dua bingkai berturut-turut (S2F), ia menjejaki dua salinan setiap blok dengan menggunakan teknik pengesanan dua peringkat yang dicadangkan dan melibatkan carian Berlian dan Pengubah Slantlet untuk mencari blok pendua. Keempat, bagi setiap pasangan blok pendua daripada S2F, ia mengira anjakan menggunakan konsep aliran optik. Kelima, berdasarkan nilai-nilai anjakan dan ambang pengiraan empirikal, skim ini mengesan kewujudan sebarang objek terpadam yang dijumpai di dalam bingkai. Setelah selesai, ia kemudiannya mengekstrak objek yang bergerak menggunakan pendekatan berasaskan ambang-sama. Keenam, pengesanan anjakan bingkai demi bingkai dilakukan untuk mengesan pergerakan objek dan mencari laluan anjakan objek yang bergerak. Proses ini diulangi untuk satu lagi kumpulan bingkai bagi mencari jalan anjakan seterusnya untuk objek kedua yang bergerak sehingga kesemua bingkai habis. Akhirnya, laluan anjakan dibandingkan antara satu sama lain dengan menggunakan algoritma sepadan Lengkungan Masa Dinamik (DTW) yang hampir sama untuk mengesan objek pengklonan. Jika mana-mana pasangan daripada laluan anjakan merupakan bandingan yang sempurna maka pengklonan akan ditemui. Bagi mengesahkan proses ini, satu siri eksperimen berdasarkan set data dari Perpustakaan Universiti Untuk Analisis Forensik (SULFA) dan Video Mengganggu Set Data (VTD) telah dijalankan untuk mengukur prestasi skim yang dicadangkan. Keputusan eksperimen skim pengesanan sangat menggalakkan dengan kadar ketepatan 96.86%, yang ketara mengatasi kaedah terkini sebanyak 3.14%.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

GOP	-	Group of Pictures
SULFA	-	Surrey University Library for Forensic Analysis
VTD	-	Video Tampering Dataset
NLF	-	Noise Level Function
CCN	-	Circular Correlation Norm
HHT	-	Hilbert-Huang transform
DCT	-	Discrete Cosine Transform
DS	-	Diamond Search
SLT	-	Slantlet Transform
DTW	-	Dynamic Time Warping
Th1	-	Threshold
Th2	-	Threshold
TP	-	True Positive
TN	-	True Negative
FN	-	False Negative
FP	-	False Positive
S2F	-	Two Successive Frame
Oflow	-	optical flow
LDS	-	Large Diamond Search
SDS	-	Small Diamond Search
MAD	-	Mean Absolute Difference
MAE	-	Mean Absolute Error
DWT	-	Discrete Wavelet Transform
GS	-	Gaussian Smoothing

LIST OF ALGORITHMS

CHAPTER 1

INTRODUCTION

1.1 Overview

In the last of few years, with the advent of digital media such as video, images and audio through internet, the means and the incentive to create digital forgeries have also multiplied with it. As a matter of fact, powerful tamper media or editing software and tools allow the creation of perceptually persuasive digital forgeries techniques. Evolutions in visual digital video technologies such as digital transmission, compression, storage, and video-conferencing have supported society in many ways. Compared with digital image, the tampering of digital video is often more sophisticated and time-consuming (Richao *et al.*, 2014) although it is becoming easier with the popularity of video editing tools, such as Video Editor and Adobe Photoshop.

The video processing software is commonly used to delete or incorporate moving objects and change the forged regions with information garnered from their neighbouring areas (Su *et al.*, 2015). In this background video authentication refers to a process that confirms the authenticity of a specific video as captured by camera through searching and detecting various forensic types as to the tampering method. In this regard, a video sequence can be modified through several forensic methods like modification, combination or create of new video contents. The aim behind video manipulation is to tamper, doctor or fake an authentic video. The real videos may be utilized as sources of their tampered counterparts, and such tampering can be conducted on a single video source or on many sources (Upadhyay and Singh, 2012).

Video forgeries mainly fall into two types of techniques that can be used for video tampering detection: active forgeries and passive forgeries. In active forgeries, (Di Martino and Sessa, 2012; Ram *et al.*, 2009), the tampered region can be extracted using a pre-embedded information such as watermark and fingerprint. However, this scheme must have source files to embed the watermark first otherwise the detection process will fail (Ng *et al.*, 2006).

In passive approaches, techniques can be divided into three categories (C.-S. Lin and Tsay, 2013) namely, source identification (sensor type of camera such as noise), splicing techniques (multiple video-based forgery), and copy-move detection techniques (single video-based forgery).

Source camera identification (C.-C. Hsu *et al.*, 2008; Kang *et al.*, 2012) is a crucial issue that focuses on many issues that are linked to camera that is concerned with identifying the source of a digital device; for example, mobile phones, camcorders, and cameras. On the other hand, in splicing techniques forgery (Wahab *et al.*, 2014), two videos are combined to create one tampered video or a composite of two or more videos are combined to create a fake video. Furthermore, splicing tampering becomes difficult if the directions and lighting conditions are different during recording with a dynamic camera (He *et al.*, 2012; Y.-F. Hsu and Chang, 2007).

One of the major challenges that are faced by digital forensics is video copy-move forgery or digital content tampering (Li and Huang, 2014). More recently, there have been various types of forgery methods developed by hackers, with operation duplication operation or copy-move on top of the list. In the context of cloning, the main objective is to hide or incorporate an object from the same video scene to develop a new scene. This process has become widely used as a malicious way of hiding evidence (Qadir *et al.*, 2012).

(a) (b)

Figure 1.1 Example of video Copy-Move forgery (a) Original video (b) Tampered video from VTD dataset

Figure 1.1 illustrates an example of video copy-move forgery, where (a) the original video and (b) the tampered video. For example, the ducks are recorded in the video twice by taking part of the video (e.g., white car) and pasting it in another region within the same video. It is challenging to detect this type of video forgery if the copy-move procedure is carefully and actually carried out. Therefore, it is necessary to have reliable and efficient methods to detect copy-move forgery for applications in law enforcement, particularly forensics (Milani *et al.*, 2012).

1.2 Background of Research

Dynamic developments in digital technologies and extensively utilized digital video recording systems along with sophisticated video editing software, high quality processing tools and algorithms, and low cost accessibility as well as easy to operate digital multimedia devices have led to the increased video tampering and the challenge of video authentication.

Video copy-move forgery has been identified as a vital form of forgery as it utilizes the same video frames sources and destination-apart from this, the video frame is copied and pasted on another part of the same video. In fact there are more subtle cases found in the standard dataset video copy-move forgery whereby copied frames are pasted on several places on the same video (many-to-many). Figure 1.2 illustrates the above cases.

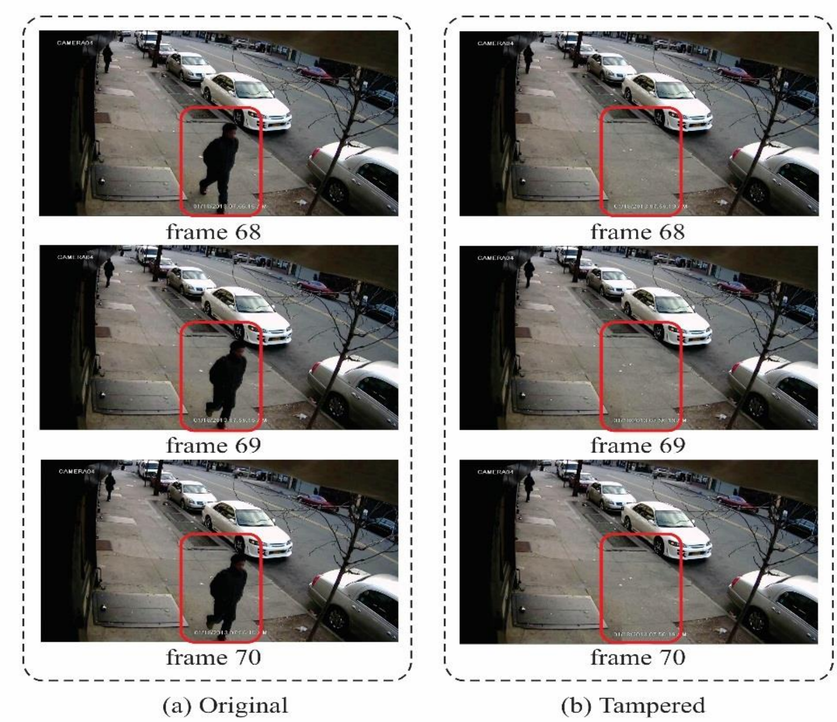

Figure 1.2 Sample of video copy-move forgery (a) Original video (b) Tampering video from VTD dataset

In the beginning, the problem of copy-move lies in appointing video authentication that plays a key role in detecting and determining region duplication, frame duplication or object duplication of video forgery, and locating the factors that affect video forgery (Richao, *et al.*, 2014).

Pioneering methods depend on intrinsic features such as pixel value and statistical features as well as video files characteristics. Among the many methods that are considered for video forgery detection are those that are based on the identification of acquisition device and detection of whether or not two video clips stem from the one source. In relation to this, (Kot and Cao, 2013) stated that owing to the statistical source features sensitive nature towards tampering and modifications, it is suitable to be used in addressing tampering.

A majority of the previous works (Pathak and Patil, 2014; D'Amiano, *et al.*, 2015; Bestagini *et al.*, 2013) have used Local Binary Patterns (LBP)-based features to identify duplicated image regions. Though LBP is effective against distortions, scaling, JPEG compression, blurring and noise adding, it however becomes ineffective when forged areas are small. This failure may lead to inadvertent errors in the subsequent important processes such as detection of moving objects and deleting objects. This is to emphasise that precise duplicated region detection is utmost important in video copy-move forgery detection. Failure which will result in low detection accuracy.

Beside the duplicated region, detection of moving objects, which traverse from frame to frame, is also important. Most of the previous works (Pathak and Patil, 2014; D'Amiano, *et al.*, 2015; Bestagini *et al.*, 2013) used LESH (Local Energy based Shape Histogram) along with lexicographical sorting to determine objects' trajectory similarity. The method is similar to shape-based image retrieval approach. The method has a good efficiency in detecting copy-move. However, the efficiency falls as the quality of the video frames degrades. Video tampering refers to the generation of faked videos by adding, deleting or altering new video object. It usually consists of detection/tracking, video manipulation, video in-painting and video layer fusion (Kot and Cao, 2013).

The detection methods in passive blind video copy-move forgeries can be categorized into four and they are pixel-based approach, format-based approach, camera-based approach and geometric-based approach (Lin and Tsay, 2014).

1.2.1 Pixel-Based Approach

According to (Wang and Farid, 2007), pixel-based approaches make use of high correlation between authentic and forged areas in video frames for the detection of copy-paste forgery. The drawback lies in the fact that high correlation between frames is common in normal videos rendering the method useless if the copied regions are in use from other video frames. In (G.-S. Lin *et al.*, 2011) proposed a video detection method known as a coarse-to-fine grained method that uses the variation in colour histograms of adjacent frames that are similar spatially and temporally – it makes use of the macro-block based correlation algorithm to identify duplication. However, their method is not able to determine region forgery.

In a similar study, (Zhang *et al.*, 2009) brought forward a method that uses ghost shadow artefacts presented by the consistencies in painting in order to detect forged moving object region. Their approach differentiates static background from moving foreground through block matching that is sensitive to the noise property (illumination alterations), but due to its inaccuracy, the tampered region in each frame cannot be identified by their method.

1.2.2 Format-Based Approach

An appearance of format-based approach in the video makes up part of the forgery chain-of-evidence. A study of high MPEG is usually initialized with compression video coding standard since some of the research in MPEG video forgeries focus on the properties of the frames compression efficiency and how it is affected when a video is tampered.

In this background, (Wang and Farid, 2006), proposed spatio-temporal domain artefacts of doubly compressed MPEG video frames in type of I-frame that is like a frame sequence of JPEG compressed image although there is considerable correlation among frames in GOP (Group of Pictures). In relation to this, the determination of predictive coded I-frame double compression is akin to double compression detection, and in the case of GOP, insertion or removal of frames will increase the error of motion estimation. Their method effectively works in detecting frame manipulation but not in locating tampered object regions. In (Luo *et al.*, 2008) study, the authors brought forward a new method using the temporal blocking artefacts patterns to detect whether deletion or insertion has been done on MPEG video prior to recompression with different GOP structures. Their approaches are effective in frame-level forgery but not in region-level tampering and localization.

1.2.3 Camera-Based Approach

The main steps of this approach is extracting different types of fingerprints based on a set of videos then applying pattern recognition techniques in order to detect forgery. Some fingerprints recognition, which can be used in these techniques include noise patterns, lens distortion, and inconsistence-related artifacts (Kancherla and Mukkamala, 2012).

As aforementioned, another set of video source camera identification method is based on the extraction and measurement of noise characteristics that stem from camera sensors. Noise is generally random, unwanted and variation of pixel values in digital file (e.g., videos and images) that are sensors-generated. According to (Bayram *et al.*, 2005), the noise patterns are mostly utilized as a part of identification process source owing to their deterministic properties that stem from CCD sensors.

(Kobayashi *et al.*, 2010) proposed photon approach shot noise to detect tampered level regions by using noise characteristics. Their method exploited the inconsistencies of photon shot noise caused by various video source cameras to detect between the original and forgery regions. But, their methods approach can merely detect forgery regions in static scene videos and not suspicious level regions in videos captured by a moving camera.

1.2.4 Geometric-Based Approach

Geometric-based approaches make use of measurements of objects in the video and their positions relative to the moving video camera. Based on (Conotter *et al.*, 2011) study, a forgery technique approach to detect physically inconsistent implausible trajectory of objects in video frame sequences was employed. However, their technique can detect manipulation regions in a video sequence and limits the form of the video frame (i.e., de-interlaced or interlaced).

The research questions regarding automatic video copy-move forgery detection that are answered in this thesis are:

1. What different techniques for video forgery copy-move detection have been proposed to date and where does state-of-the-art methods stand today in terms of detection rates?

2. Which type of features can be extracted to characterizing the video frames?

3. Can a new video forgery copy-move detection technique, which could achieve better performances in comparison to existing techniques in terms of detection rate, be proposed?

4. How can the exact location of forged area in video forgery copy-move detection be located?

1.3 Problem Statement

Malicious manipulations and video tampering without any evidence being left behind has become very affordable and highly used, due to existence of extremely powerful editing tools such as Adobe Photoshop and video editing software. Therefore, there has been a swift augmentation of the digitally altered videos on the Internet and mainstream media. This tendency depicts grave vulnerabilities as well as minimizes the reliability of digital video. For such reasons, upcoming techniques in verification of the authenticity and integrity of digital video have been regarded as being significant, more so when putting into consideration the videos presented as news items, as evidence in forensic investigation, such as murder surveillance, or part of video forensics. From such a perspective, the principal goal in video forensics is to determine and detect video forgery forensics (Amerini *et al*., 2013).

There entail a myriad of challenges faced by passive technique of detecting video forgeries and equally have their constraints and setbacks. One of the fascinating challenges facing the current scholars and researchers in this field is the reduction of counterfeit positive rate of such approaches, in establishing effusive automatic system with the capacity to identify image falsification from a wide perspective of video formats. Additionally, the system detecting such falsification is made to increase its dependability, robustness, and competence of operation. The key setback realized in passive approaches is their requirement for several initial videos to approximate the internal traces, whereas in capable situations there entails nothing else rather than the video in query (Chen Mo*et al.*, 2008). Additional studies regarding this analysis can be accessed in (Lanjewar *et al.*, 2014).

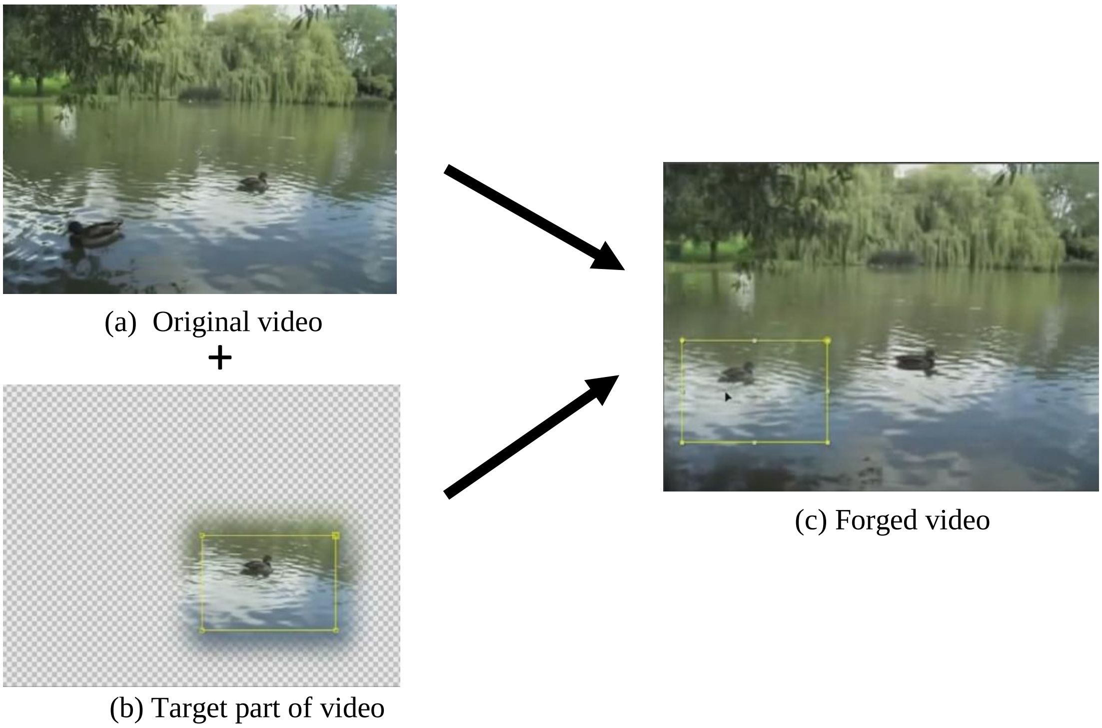

Figure 1.3 Example of video copy-move forgery (Qadir, *et al.*, 2012)

Figure 1.3 shows an example of video copy-move forgery in which a region from one image is copied and pasted within the same video (Muhammad Ghulam *et al.*, 2014). For instance, there has been a continuous problem in identifying copy-move areas that have been rotated and scaled from different angles (Lanjewar *et al.*, 2014).

Against this backdrop, this research therefore concludes that existing video copy-move detection methods still suffer many drawbacks, which include, among others:

i. Their performance is mediocre when it comes to video compression, and in GOP, where addition or deletion of frame increases the estimation of motion error (Dong *et al.*, 2012; Li and Huang, 2014; Shanableh, 2013). Their method's effectiveness is confined to the detection of frame tampering and not localization of tampered regions.

ii. The presence of homogeneous regions in the tampering video further complicates the video copy-move forgery detection, which normally increases the false positive and the accuracy rate is far from satisfactory (Hyun *et al.*, 2013; Su*, et al.*, 2015; Subramanyam and Emmanuel, 2013).

iii. Notwithstanding the achievements realized by prior studies entailing high correlations between original and forged regions in copy-move forgery detection (e.g., Hsu *et al*., 2008; Thakur, 2013; Wang *et al*., 2014), high correlation is known to be common in natural videos and the methods proposed are not effective if the copied regions are within-frame object tampering calling for more enhancements.

Thus, the remaining issues and drawbacks of the previous works, which have been mentioned above, compel the author to pursue the research to seek a new approach to improve the detection rate of video copy-move forgery. With that in mind, a specific and focused research goal along with its objectives and scope are articulated and given in the following sub-sections.

1.4 Research Goal

The study aims to design and develop a new video copy-move forgery detection scheme with high accuracy based on optical flow methods.

1.5 Research Objectives

In order to achieve the goal, this study aims to fulfil the following main objectives:

i. To develop a new method to trace duplicated blocks from each pair of successive frames of a video using a two-tier approach comprising Diamond search and Slantlet transform.

ii. To propose a new method to detect and localise both deleted objects and moving objects using block displacements.

iii. To propose a new cloning object detection method based on displacement paths of moving objects using Dynamic Time Warping (DTW) matching algorithm.

1.6 Research Scope

The scope of this research is limited to the following:

i. Datasets: two sets of datasets namely, SULFA (Surrey University Library for Forensic Analysis) (Qadir, et al., 2012) and VTD (Video Tampering Dataset) are employed to evaluate the performance of the proposed scheme. The former is a standard dataset obtained from http://sulfa.cs.surrey.ac.uk/forged.php. On the other hand, the latter is a self -created dataset which can be found at: https://www.youtube.com/channel/UCZuuu-iyZvPptbIUHT9tMrA.

ii. Performance evaluation: This study's only concern is the accuracy rate, while the computational complexity is beyond its domain.

iii. Type of forgery: This study only focus on copy-move or copy-paste-move forgery, while other kinds are out of scope of this study.

1.7 Significance of the Study

It is strongly believed that several applications like video copy-move forgery detection investigations of digital video for forensic investigation such as in the case of video surveillance, and presenting video evidence in courts of law need more advanced detection and authentication techniques to prove the trustworthiness of digital video. In light of the above mentioned issues, the results of this research are expected to contribute to what is currently known about video copy-move forgery detection. Nonetheless, the significance of this study is not only limited to forgery detection, but also to the development of a new method that can be used in the future in many applications in the field of computer vision.

1.8 Thesis Outline

The organization of this thesis is given in this section. The rest of the chapters in this thesis begin with brief sections that highlight the aims of each section of the chapter, and sums up with a short conclusion. Chapter 1, provides an overview of the research problem and a brief background. The objectives of the research are also described in this chapter.

In Chapter 2, an in-depth review of the existing literature on authentication of video digital processing on the whole, as well as passive methods in attaining the study's objective, specifically are presented. The currently employed approaches and criteria within the context of counterfeit digital video recognition are highly defined in this chapter. A review of a current study is conducted inclusive of recent techniques and methods employed in sensing video forgery tampering. This study area is moderately novel hence the meagre sources relative to the study topic. Therefore, the reviewed and availed approaches relate to extensive processing of digital videos, but only somewhat related to forgery detection in videos forensic. All the chapters are independent but a flow and coherency of ideas throughout the entire thesis are ensured.

Chapter 3, presents a clear roadmap of this study to guide the reader to achieve a quick grasp of the detailed research framework. The advantages of using the popular dataset in the newly developed methods are emphasised. The layout of the entire research framework, strategies, and procedures are highlighted. This is followed by Chapter 4, where a detailed design of the proposed method is provided along with the step-by-step processes and the proposed algorithms employed in it. The chapter also provides a discussion of the proposed methods entailing the proposed method's implementation on video copy-move forgery detection.

The next chapter (Chapter 5), provides the results of the proposed method used on two datasets SULFA and the VTD dataset of video copy-move forgery detection, along with the experimental results, detailed analyses, and discussion. It explains the qualitative and quantitative measurements that are carried out for the performance evaluations and implementation of the method for every phase with the inclusion of the detection of the tampered videos and localisation of the forgery region. The qualitative measurements are based on visual human inspection, while the quantitative measurements are performed using standard approaches. Lastly, Chapter 6 concludes the study by emphasizing the major contributions, enumerating the major achievements achieved and providing recommendations for future studies.

Conotter, V., O'Brien, J. F. and Farid, H. (2012). Exposing digital forgeries in ballistic motion. *Information Forensics and Security, IEEE Transactions on*, 7(1), 283-296.

Dalal, N. and Triggs, B. (2005). Histograms of oriented gradients for human detection. Proceedings of the 2005 Computer Vision and Pattern Recognition, 2005. *CVPR 2005. IEEE Computer Society Conference on*, 886-893.

D'Amiano, L., Cozzolino, D., Poggi, G. and Verdoliva, L. (2015). Video forgery detection and localization based on 3D patchmatch. *Proceedings of the 2015 Multimedia & Expo Workshops (ICMEW), 2015 IEEE International Conference on*, 1-6.

Davarzani, R., Yaghmaie, K., Mozaffari, S. and Tapak, M. (2013). Copy-move forgery detection using multiresolution local binary patterns. *Forensic science international*, 231(1), 61-72.

Di Martino, F. and Sessa, S. (2012). Fragile watermarking tamper detection with images compressed by fuzzy transform. *Information Sciences*, 195, 62-90.

Dice, L. R. (1945). Measures of the amount of ecologic association between species. *Ecology*, 26(3), 297-302.

Dong, Q., Yang, G. and Zhu, N. (2012). A MCEA based passive forensics scheme for detecting frame-based video tampering. *Digital Investigation*, 9(2), 151-159.

Elnagar, A. and Basu, A. (1995). Motion detection using background constraints. *Pattern Recognition*, 28(10), 1537-1554.

Esmaeilani, R. (2014). *Source identification of captured video using photo response non-uniformity noise pattern and svm classifiers*. Master thesis, Universiti Teknologi Malaysia.

Fan, X. and Tjahjadi, T. (2015). A spatial-temporal framework based on histogram of gradients and optical flow for facial expression recognition in video sequences. *Pattern Recognition*, 48(11), 3407-3416.

Farid, H. (2003). A picture tells a thousand lies. *New Scientist*, (2411), 38-41.

Farid, H. (2009). Image forgery detection. *Signal Processing Magazine, IEEE*, 26(2), 16-25.

Fridrich, A. J., Soukal, B. D. and Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. *Proceedings of the 2003 in Proceedings of Digital Forensic Research Workshop*, 1-10.

Fu, A. W.-C., Keogh, E., Lau, L. Y., Ratanamahatana, C. A. and Wong, R. C.-W. (2008). Scaling and time warping in time series querying. *The VLDB Journal—The International Journal on Very Large Data Bases,* 17(4), 899-921.

Garg, R., Varna, A. L. and Wu, M. (2011). Seeing ENF: natural time stamp for digital video via optical sensing and signal processing. *Proceedings of the 2011 Proceedings of the 19th ACM international conference on Multimedia*, 23-32.

Ghanbari, M. (1990). The cross-search algorithm for motion estimation. *IEEE Transactions on Communications,* 38(7), 950-953.

Ghanem, K. (2013). Towards more accurate clustering method by using dynamic time warping. *International Journal of Data Mining & Knowledge Management Process (IJDKP),* 3(2), 107-118.

Gironi, A., Fontani, M., Bianchi, T., Piva, A. and Barni, M. (2014). A video forensic technique for detecting frame deletion and insertion. *Proceedings of the 2014 Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, 6226-6230.

Goldman, D. B., Gonterman, C., Curless, B., Salesin, D. and Seitz, S. M. (2008). Video object annotation, navigation, and composition. *Proceedings of the 2008 Proceedings of the 21st annual ACM symposium on User interface software and technology*, 3-12.

He, Z., Lu, W., Sun, W. and Huang, J. (2012). Digital image splicing detection based on Markov features in DCT and DWT domain. *Pattern Recognition*, 45(12), 4292-4299.

Hikmat N, A. and Safa'a AA, A. (2010). Implementation of 8-point Slantlet transform based polynomial cancellation coding-OFDM system using FPGA. *Proceedings of the 2010 Systems Signals and Devices (SSD), 2010 7th International Multi-Conference on*, 1-6.

Hsu, C.-C., Hung, T.-Y., Lin, C.-W. and Hsu, C.-T. (2008). Video forgery detection using correlation of noise residue. *Proceedings of the 2008 Multimedia Signal Processing, 2008 IEEE 10th Workshop on*, 170-174.

Hsu, Y.-F. and Chang, S.-F. (2007). Image splicing detection using camera response function consistency and automatic segmentation. *Proceedings of the 2007 Multimedia and Expo, 2007 IEEE International Conference on*, 28-31.

Hyun, D.-K., Lee, M.-J., Ryu, S.-J., Lee, H.-Y. and Lee, H.-K. (2013). Forgery detection for surveillance video. *The Era of Interactive Media* (pp. 25-36): Springer.

Ince, S. and Konrad, J. (2008). Occlusion-aware optical flow estimation. *IEEE Transactions on Image Processing*, 17(8), 1443-1451.

Jaccard, P. (1912). The distribution of the flora in the alpine zone. *New phytologist*, 11(2), 37-50.

Jaiswal, S. and Dhavale, S. (2013). Video Forensics in Temporal Domain using Machine Learning Techniques. *International Journal of Computer Network and Information Security*, 5(9), 58.

Jing, G., Rajan, D. and Siong, C. E. (2005). Motion detection with adaptive background and dynamic thresholds. *Proceedings of the 2005 2005 5th International Conference on Information Communications & Signal Processing*, 41-45.

Johnson, M. K. and Farid, H. (2006). Exposing digital forgeries through chromatic aberration. *Proceedings of the 2006 Proceedings of the 8th workshop on Multimedia and security*, 48-55.

Johnson, M. K. and Farid, H. (2007). Exposing digital forgeries through specular highlights on the eye. *Proceedings of the 2007 Information Hiding*, 311-325.

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

Kang, X., Li, Y., Qu, Z. and Huang, J. (2012). Enhancing source camera identification performance with a camera reference phase sensor pattern noise. *Information Forensics and Security, IEEE Transactions on*, 7(2), 393-402.

Kattoush, A. H. (2012). A radon slantlet transforms based OFDM system design and performance simulation under different channel conditions. *ISRN Communications and Networking*, 2012, 1-10.

Kim, C. and Vasudev, B. (2005). Spatiotemporal sequence matching for efficient video copy detection. Circuits and Systems for Video Technology, *IEEE Transactions on*, 15(1), 127-132.

Kitagawa, G. (1994). The two-filter formula for smoothing and an implementation of the Gaussian-sum smoother. *Annals of the Institute of Statistical Mathematics*, 46(4), 605-623.

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

Kobayashi, M., Okabe, T. and Sato, Y. (2010). Detecting forgery from static-scene video based on inconsistency in noise level functions. *IEEE Transactions on, Information Forensics and Security,* 5(4), 883-892.

Koga, T. (1981). Motion-compensated interframe coding for video conferencing. *Proceedings of the 1981 Proc*. NTC 81, (pp. C9-6).

Kopparapu, S. and Satish, M. (2014). Optimal Gaussian Filter for Effective Noise Filtering. *Computer Science*, 12(2), 1-7.

Kot, A. C. and Cao, H. (2013). Image and Video Source Class Identification. *Digital Image Forensics* (pp. 157-178): Springer.

Kroeger, T., Timofte, R., Dai, D. and Van Gool, L. (2016). Fast Optical Flow using Dense Inverse Search. *Computer Vision and Pattern Recognition,* 1(3), 1-25.

Kurosawa, K., Kuroki, K. and Saitoh, N. (1999). CCD fingerprint method-identification of a video camera from videotaped images. *IEEE International Conference on Image Processing*, vol.3, 537-540.

Lanjewar, S. B., P. A. Khaire, and R. Meshram, (2014). An approach towards image forgery detection. *International Journal of Advanced Research in Computer Science.* vol.5, no.8, 205-209.

Le Gall, D. (1991). MPEG: A video compression standard for multimedia applications. *Communications of the ACM*, 34(4), 46-58.

Li, F. and Huang, T. (2014). Video copy-move forgery detection and localization based on structural similarity. *Proceedings of the 2014 Proceedings of the 3rd International Conference on Multimedia Technology (ICMT 2013)*, 63-76.

Li, R., Yu, S. and Yang, X. (2007). Efficient spatio-temporal segmentation for extracting moving objects in video sequences. *IEEE Transactions on Consumer Electronics,* 53(3), 1161-1167.

Li, X., Jing, T. and Li, X. (2010). Image splicing detection based on moment features and Hilbert-Huang Transform. *Proceedings of the 2010 Information Theory and*

Information Security (ICITIS), 2010 IEEE International Conference on, 1127-1130.

Liao, S.-Y. and Huang, T.-Q. (2013). Video copy-move forgery detection and localization based on Tamura texture features. *Proceedings of the 2013 Image and Signal Processing (CISP), 2013 6th International Congress on*, 864-868.

Lin, C.-S. and Tsay, J.-J. (2013). Passive approach for video forgery detection and localization. *Proceedings of the 2013 The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*, 107-112.

Lin, C.-S. and 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.

Lin, G.-S., Chang, J.-F. and Chuang, C.-H. (2011). Detecting frame duplication based on spatial and temporal analyses. *Proceedings of the 2011 Computer Science & Education (ICCSE), 2011 6th International Conference on*, 1396-1399.

Lucas, B. D. and Kanade, T. (1981). An iterative image registration technique with an application to stereo vision. *Proceedings of the 1981 International Joint Conference on Artificial Intelligence, 674-679*.

Luo, W., Wu, M. and Huang, J. (2008). MPEG recompression detection based on block artifacts. *Proceedings of the 2008 Electronic Imaging 2008*, 68190X-68190X-68112.

Mahajan, A., Sharma, K. and Kumar, D. (2014). Comparative Analysis of Pixel Based Motion Estimation with Block Based Motion Estimation. *International Journal of Recent Research Aspects*, 1(2), 78-83.

Malviya, A. V. and Ladhake, S. A. (2016). Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram. *Procedia Computer Science*, 79, 383-390.

Manzanera, A. and Richefeu, J. C. (2007). A new motion detection algorithm based on Σ–Δ background estimation. *Pattern Recognition Letters, 28(3)*, 320-328.

Metkar, S. and Talbar, S. (2013). Performance Evaluation of Block Matching Algorithms for Video Coding Motion Estimation Techniques for Digital Video Coding (pp. 13-31): *Springer*.

Milani, S., Bestagini, P., Tagliasacchi, M. and Tubaro, S. (2012). Multiple compression detection for video sequences. *Proceedings of the 2012 Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on*, 112-117.

Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., et al. (2012). An overview on video forensics. *APSIPA Transactions on Signal and Information Processing*, 1, 1-18.

Mondaini, N., Caldelli, R., Piva, A., Barni, M. and Cappellini, V. (2007). Detection of malevolent changes in digital video for forensic applications. *Proceedings of the 2007 Electronic Imaging 2007*, 65050T-65050T-65012.

Muhammad, Ghulam, Munner H. Al-Hammadi, Muhammad Hussain, and George Bebis, (2014). Image Forgery Detection Using Steerable Pyramid Transform and Local Binary Pattern. *Machine Vision and Applications.* vol.25, no.4, pp.985-995.

Mutt, S. and Kumar, S. (2009). Secure image Steganography based on Slantlet transform. *Proceedings of the 2009 Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on*, 1-7.

Ng, T.-T., Chang, S.-F., Lin, C.-Y. and Sun, Q. (2006). Passive-blind image forensics. *Multimedia Security Technologies for Digital Rights*, 15, 383-412.

Pathak, A. and Patil, D. (2014). Video Forgery Detection Based on Variance in Luminance and Signal to Noise Ratio using LESH Features and Bispectral Analysis. *International Journal of Computer Science and Mobile Computing*, 3(7), 318-327.

Peng, F., Nie, Y.-y. and Long, M. (2011). A complete passive blind image copy-move forensics scheme based on compound statistics features. *Forensic science international*, 212(1), e21-e25.

Podilchuk, C. I. and Zeng, W. (1998). Image-adaptive watermarking using visual models. *Selected Areas in Communications, IEEE Journal on*, 16(4), 525-539.

Popescu, A. C. and Farid, H. (2004). Statistical tools for digital forensics. *Proceedings of the 2004 Information Hiding*, 128-147.

Popescu, A. C. and Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on, Signal Processing*, 53(10), 3948-3959.

Qadir, G., Yahaya, S. and Ho, A. T. (2012). Surrey university library for forensic analysis (SULFA) of video content. *IET Conference on, Proceedings of the 2012 Image Processing (IPR 2012),* 1-6.

Qin, Y.-l., Sun, G.-l., Wang, S.-z. and ZHANG, X.-p. (2010). Blind detection of video sequence montage based on GOP abnormality. *Act Electronica Sinica*, 38(7), 1597-1602.

Ram, S., Bischof, H. and Birchbauer, J. (2009). Active fingerprint ridge orientation models *Advances in Biometrics* (pp. 534-543): Springer.

Ratanamahatana, C. A. and Keogh, E. (2004). Everything you know about dynamic time warping is wrong. *Proceedings of the 2004 Third Workshop on Mining Temporal and Sequential Data,* 53-63.

Redi, J. A., Taktak, W. and Dugelay, J.-L. (2011). Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications*, 51(1), 133-162.

Ren, Y., Chua, C.-S. and Ho, Y.-K. (2003). Motion detection with no stationary background. *Machine Vision and Applications*, 13(5-6), 332-343.

Richao, C., Gaobo, Y. and Ningbo, Z. (2014). Detection of object-based manipulation by the statistical features of object contour. *Forensic science international*, 236, 164-169.

Richardson, I. E. (2004). *H. 264 and MPEG-4 video compression: video coding for next-generation multimedia*: John Wiley & Sons.

Schneider, M. and Chang, S.-F. (1996). A robust content based digital signature for image authentication. *Proceedings of the 1996 Image Processing, 1996. Proceedings., International Conference on,* 227-230.

Selesnick, I. W. (1999). The slantlet transform. *IEEE Transactions on Signal Processing,* 47(5), 1304-1313.

Shaid, S. (2009). *Estimating optimal block size of copy-move attack detection on highly textured image*. Universiti Teknologi Malaysia.

Shanableh, T. (2013). Detection of frame deletion for digital video forensics. *Digital Investigation*, 10(4), 350-360.

Shih, T. K., Tang, N. C. and Hwang, J.-N. (2007). Ghost shadow removal in multi-layered video inpaintinga. *Proceedings of the 2007 Multimedia and Expo, 2007 IEEE International Conference on*, 1471-1474.

Shih, T. K., Tang, N. C., Tsai, J. C. and Hwang, J.-N. (2011). Video motion interpolation for special effect applications. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 41(5), 720-732.

Shivakumar, B. and Baboo, L. D. S. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. *Global Journal of Computer Science and Technology*, 10(7).

Sowmya, K. and Chennamma, H. (2015). A Survey on video forgery detection. *International Journal of Computer Engineering and Applications*, 9(2), 17-27.

Srinivasan, R. and Rao, K. (1985). Predictive coding based on efficient motion estimation. *IEEE Transactions on Communications*, 33(8), 888-896.

Su, L., Huang, T. and Yang, J. (2015). A video forgery detection algorithm based on compressive sensing. *Multimedia Tools and Applications*, 74(17), 6641-6656.

Su, Y., Zhang, J. and Liu, J. (2009). Exposing digital video forgery by detecting motion-compensated edge artifact. *Proceedings of the 2009 Computational Intelligence and Software Engineering*, 2009. CiSE 2009. International Conference on, 1-4.

Subramanyam, A. and Emmanuel, S. (2012). Video forgery detection using HOG features and compression properties. *Proceedings of the 2012 Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on*, 89-94.

Subramanyam, A. and Emmanuel, S. (2013). Pixel estimation based video forgery detection. *Proceedings of the 2013 Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, 3038-3042.

Sun, T., Wang, W. and Jiang, X. (2012). Exposing video forgeries by detecting MPEG double compression. *Proceedings of the 2012 Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*, 1389-1392.

Thakur, M. K. (2013). *Tampered videos: detection and quality assessment*. PhD thesis, Jaypee Institute of Information Technology.

Upadhyay, S. and Singh, S. K. (2011). Learning based video authentication using statistical local information. *Proceedings of the 2011 Image Information Processing (ICIIP), 2011 International Conference on*, 1-6.

Upadhyay, S. and Singh, S. K. (2012). Video Authentication: Issues and Challenges. *International Journal of Computer Science Issues*, 9(1), 409-418.

Vazquez-Padin, D., Fontani, M., Bianchi, T., Comesaña, P., Piva, A. and Barni, M. (2012). Detection of video double encoding with GOP size estimation. *2012 IEEE International Workshop on, Proceedings of the Information Forensics and Security (WIFS), 151-156*.

Wahab, A. W. A., Bagiwa, M. A., Idris, M. Y. I., Khan, S., Razak, Z. and Ariffin, M. R. K. (2014). Passive video forgery detection techniques: a survey. *10th International Conference on, Proceedings of the 2014 Information Assurance and Security (IAS), 29-34*.

Wang, Q., Li, Z., Zhang, Z. and Ma, Q. (2014). Video inter-frame forgery identification based on consistency of correlation coefficients of gray values. *Journal of Computer and Communications*, 2(04), 51.

Wang, W. (2009). *Digital video forensics*. PhD thesis, Dartmouth College, Hanover, New Hampshire.

Wang, W. and Farid, H. (2006). Exposing digital forgeries in video by detecting double MPEG compression. *Proceedings of the 2006 Proceedings of the 8th workshop on Multimedia and security*, 37-47.

Wang, W. and Farid, H. (2007a). Exposing digital forgeries in interlaced and deinterlaced video. *Information Forensics and Security, IEEE Transactions on*, 2(3), 438-449.

Wang, W. and Farid, H. (2007b). Exposing digital forgeries in video by detecting duplication. *Proceedings of the 2007b Proceedings of the 9th workshop on Multimedia & security*, 35-42.

Wang, W. and Farid, H. (2009). Exposing digital forgeries in video by detecting double quantization. *Proceedings of the 2009 Proceedings of the 11th ACM workshop on Multimedia and security*, 39-48.

Wang, W., Jiang, X., Wang, S., Wan, M. and Sun, T. (2013). Identifying video forgery process using optical flow *Digital-Forensics and Watermarking* (pp. 244-257): Springer.

Wang, Z. (2006). Time series matching: a multi-filter approach. *Courant Institute of Mathematical Sciences New York*.

Wolf, S. and Pinson, M. (2009). A no reference (NR) and reduced reference (RR) metric for detecting dropped video frames. *Proceedings of the 2009 Fourth*

International Workshop on Video Processing and Quality Metrics for Consumer Electronics (VPQM-09).,

Wu, X., Li, J., Zhang, Y. and Tang, S. (2008). Spatio-temporal visual consistency for video copy detection. *Proceedings of the 2008 Visual Information Engineering, 2008. VIE 2008. 5th International Conference on*, 414-419.

Wu, Y., Jiang, X., Sun, T. and Wang, W. (2014). Exposing video inter-frame forgery based on velocity field consistency. *Proceedings of the 2014 Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, 2674-2678.

Xiaoling, C. and Huimin, Z. (2012). A Novel Video Tamper Detection Algorithm Based on Semi-fragile *Watermarking Advances in Information Technology and Industry Applications* (pp. 489-497): Springer.

Yu, D., Yu, X., Hu, Q., Liu, J. and Wu, A. (2011). Dynamic time warping constraint learning for large margin nearest neighbor classification. *Information Sciences*, 181(13), 2787-2796.

Yu, J. and Srinath, M. D. (2001). An efficient method for scene cut detection. *Pattern Recognition Letters*, 22(13), 1379-1391.

Zeng, F.-z., LU, Y.-s. and ZHOU, Y. (2011). The video tamper detection algorithm based on semi-fragile watermark with compressive sensing [J]. *Journal of Circuits and Systems*, 4, 016.

Zhang, J., Su, Y. and Zhang, M. (2009). Exposing digital video forgery by ghost shadow artifact. *Proceedings of the 2009 Proceedings of the First ACM workshop on Multimedia in forensics*, 49-54.

Zheng, J., Li, B., Zhou, B. and Li, W. (2005). Fast motion detection based on accumulative optical flow and double background model. *Proceedings of the 2005 International Conference on Computational and Information Science*, 291-296.

Zhu, C., Lin, X., Chau, L.-P., Ang, H.-A. and Ong, C.-Y. (2004). Efficient inner search for faster diamond search. *Signal processing*, 84(3), 527-533.

Zhu, S. and Ma, K.-K. (2000). A new diamond search algorithm for fast block-matching motion estimation. *Image Processing, IEEE Transactions on*, 9(2), 287-290.

Table of Corrections

Required Corrections	Page No.	The Amendment Made	Page No.
Title		Video Copy-Move Forgery Detection Scheme Based On Displacement Paths	
Abstract		Amended	
Chapter 1			
Typographical errors including English language and UTM Formatting		Checked and amended	2, 9 and 11
Background of Research	4	Added two paragraphs about motivation of previous works	5
Problem statement	8	Added a paragraph about motivation of this study	9
Figure 1.3 adding (a), (b) and (c)	10	Added figure 1.3 the link motivation of this study	10
Adding reference at paragraph 1 line 2	10	Added (Muhammad Ghulam et al., 2014)	10
Adding paragraphs about motivation of this study	10	Added two paragraph in page 10 to link a motivation of Problem Statement	11
Chapter 2			
Typographical errors including English language and UTM Formatting		Checked and amended	16, 26, 37 and 51
Give critical analysis (short coming, advantage of other works)	22	Critical analyses are given in four separate pages	24, 25, 32 and 50
Chapter 3			
Typographical errors including English language and UTM Formatting		Checked and amended	59 and 62
Research framework should be contributions and link to objective	59	Research framework is amended to include the contributions and link to objectives	60 and 61
Adding words	78	Add “see in Figure 3.11” words	78
Chapter 4			
Typographical errors including English language and UTM Formatting		Checked and amended	89, 94, 98, 100, and 106

Chapter title need to be changed	81	Changed to “ PROPOSED VIDEO COPY-MOVE FORGERY DETECTION SCHEME”	82
Need to tie up with the research problem	81	Added paragraph about the proposed method’s main components and link with research problem and objectives	82
Insert small caption in Fig. 4.1	83	Changed caption of Figure 4.1: “Proposed video copy-move forgery detection scheme”	84
Chapter 5			
Typographical errors including English language and UTM Formatting		Checked and amended	160,193, 194, 195 and 196
Indicating the figure with a symbol in the relevant figures and tables	180	Each video in Table 5.2 indicated to the name of each video in both datasets SULA and VTD	181
Indicating the figure with a symbol in the relevant figures and tables	184	Each video in Table 5.3 indicated to the name of each video in both datasets SULA and VTD	185
Changing words in Figure 5.28	193	Changing words from “ (red ball) “ to “(Elephant) “ words in Figure 5.28	194
Changing words in Figure 5.29	194	Changing words from “ (red ball) “ to “(red car)“ words in Figure 5.29	195
Changing words in Figure 5.30	195	Changing words from “ (red ball) “ to “(white ball) “ words in Figure 5.30	196
Changing words in Figure 5.31	196	Changing words from “ (red ball) “ to “(white car)“ words in Figure 5.31	197
Indicating the figure with a symbol in the relevant figures and tables	198	Each video in Table 5.4 indicated to the name of each video in dataset SULA	199
Indicating the figure with a symbol in the relevant figures and tables	200	Each video in Table 5.5 indicated to the name of each video in dataset SULA	201
Chapter 6			
Typographical errors including English language and UTM Formatting		Checked	
second paragraph is a revisit to problem background, objectives	205	A new paragraph (2nd. Paragraph) is added to address the issue	206
References			
Reference has been deleted form References	212	Al-Sanjary, O. I., Ahmed, A. A. and Sulong, G. (2016). Development of a video tampering dataset for forensic investigation. Forensic Science International, 266, 565-572.	213