IMAGE SPLICING DETECTION SCHEME USING ADAPTIVE THRESHOLD MEAN TERNARY PATTERN DESCRIPTOR

ARAZ RAJAB ABRAHIM

A thesis submitted in partial fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

MAY 2019

DEDICATION

This thesis is dedicated to:

My parents

Who taught me to trust in Allah, accept life no matter how good or bad things seem to me, believe in hard work and achieve a lot out of little.

My wife

This thesis work is dedicated to my wife, who has been a constant source of support and encouragement during the challenges of my study and life. I am truly thankful for having you in my life.

My children

This thesis work is dedicated to my beloved kids: Nidar, Vina, and Muhammed

My brothers and sisters

Who spared no effort in encouraging and supporting what I had been doing and inspired me the patience to challenge the hard time I went through during the period of pursuing my study until achieving this thesis.

My venerable supervisor

Who offered me valuable advices and illimitable support along the period of study that considerably contributed to pave the way for accomplishing this work.

I dedicate this research to you.

ACKNOWLEDGEMENT

First and foremost, all praise is due to Allah, the Lord of the Worlds, who granted me the will, self-trust and determination to accomplish this study. Special thanks go to both **Prof. Dr. Mohd Shafry Bin Mohd Rahim**, and **Prof. Dr. Ghazali bin Sulong** for offering this opportunity to learn and work under them supervision and giving me the chance to share them their broad knowledge and experience.

Special thanks and gratitude to my parents, wife, brothers, and sisters for their unlimited support and all my beloved friends and specially Prof. Dr. Adnan M. Abdullaziz and Dr. Omar Farook, for their permanent encouragement, support, and prayers during the period of pursuing my study and the hard time at preparing this thesis.

ABSTRACT

The rapid growth of image editing applications has an impact on image forgery cases. Image forgery is a big challenge in authentic image identification. Images can be readily altered using post-processing effects, such as blurring shallow depth, JPEG compression, homogenous regions, and noise to forge the image. Besides, the process can be applied in the spliced image to produce a composite image. Thus, there is a need to develop a scheme of image forgery detection for image splicing. In this research, suitable features of the descriptors for the detection of spliced forgery are defined. These features will reduce the impact of blurring shallow depth, homogenous area, and noise attacks to improve the accuracy. Therefore, a technique to detect forgery at the image level of the image splicing was designed and developed. At this level, the technique involves four important steps. Firstly, convert colour image to three colour channels followed by partition of image into overlapping block and each block is partitioned into non-overlapping cells. Next, Adaptive Thresholding Mean Ternary Pattern Descriptor (ATMTP) is applied on each cell to produce six ATMTP codes and finally, the tested image is classified. In the next part of the scheme, detected forgery object in the spliced image involves five major steps. Initially, similarity among every neighbouring district is computed and the two most comparable areas are assembled together to the point that the entire picture turns into a single area. Secondly, merge similar regions according to specific state, which satisfies the condition of fewer than four pixels between similar regions that lead to obtaining the desired regions to represent objects that exist in the spliced image. Thirdly, select random blocks from the edge of the binary image based on the binary mask. Fourthly, for each block, the Gabor Filter feature is extracted to assess the edges extracted of the segmented image. Finally, the Support Vector Machine (SVM) is used to classify the images. Evaluation of the scheme was experimented using three sets of standard datasets, namely, the Institute of Automation, Chinese Academy of Sciences (CASIA) version TIDE 1.0 and 2.0, and Columbia University. The results showed that, the ATMTP achieved higher accuracy of 98.95%, 99.03% and 99.17% respectively for each set of datasets. Therefore, the findings of this research has proven the significant contribution of the scheme in improving image forgery detection. It is recommended that the scheme be further improved in the future by considering geometrical perspective.

ABSTRAK

Pertumbuhan pesat aplikasi penyuntingan gambar memberi kesan ke atas pemalsuan gambar. Pemalsuan gambar adalah satu cabaran besar dalam pengenalan gambar yang sahih. Gambar boleh diubah dengan menggunakan *post-processing efect*, seperti *blurring shallow depth, JPEG compression, homogenous regions,* dan *noise* untuk menjadi gambar palsu. Selain itu, proses ini boleh digunakan dalam gambar yang telah digabungkan untuk menghasilkan gambar komposit. Dalam kajian ini, ciri deskriptor yang sesuai untuk mengesan pemalsuan berkaitan perlu ditakrifkan. Ciri-ciri ini akan mengurangkan *blurring shallow depth, JPEG compression, homogenous regions,* dan *noise* untuk meningkatkan ketepatannya. Oleh itu, teknik untuk mengesan pemalsuan di peringkat gambar pada gambar yang digabungkan telah direka dan dibangunkan. Pada tahap itu, teknik ini melibatkan empat langkah penting. Pertama, mengubah suai gambar warna menjadi tiga saluran warna diikuti dengan membahagikan gambar ke dalam blok bertindih dan setiap blok dibahagi ke dalam sel-sel yang tidak bertindih. Seterusnya *Thresholding Mean Ternary Pattern Adaptive Descriptor* (ATMTP) digunakan pada setiap sel untuk menghasilkan enam kod ATMTP dan akhirnya gambar yang diuji diklasifikasikan. Untuk bahagian seterusnya, objek gambar yang dikesan melibatkan lima langkah utama. Pertama, persamaan di antara setiap daerah jiran dikira dan dua kawasan yang paling setanding dikumpulkan bersama sehingga titik keseluruhan gambar berubah menjadi satu kawasan. Kedua menggabungkan kawasan yang sama mengikut keadaan tertentu yang memenuhi syarat kurang daripada empat piksel di antara kawasan yang sama yang membawa kepada kawasan yang dikehendaki untuk mewakili objek yang wujud dalam gambar yang telah digabungkan. Ketiga, pilih blok rawak dari tepi gambar binari berdasarkan *binary mask*. Keempat, bagi setiap blok, ciri *Filter Gabor* diekstrak untuk menilai tepi dari gambar yang dibahagikan. Akhirnya, *Support Vector Machine* (SVM) digunakan untuk mengklasifikasikan gambar. Penilaian terhadap skema ini telah diuji menggunakan tiga set dataset standard iaitu Institute of Automation, Chinese Academy of Sciences (CASIA) version TIDE 1.0 dan 2.0, dan Columbia University. Keputusan menunjukkan bahawa ATMTP mencapai ketepatan yang lebih tinggi masing-masing sebanyak 98.95%, 99.03% dan 99.17% pada setiap dataset. Oleh itu, penemuan kajian ini telah membuktikan sumbangan penting dalam bidang pengesanan pemalsuan gambar. Adalah disyorkan bahawa skim itu akan dipertingkatkan lagi pada masa akan datang dengan mempertimbangkan perspektif geometrik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2D	-	Two Dimensions
3D	-	Three Dimensions
AEG	-	Average energy gradient
ANN	-	Artificial Neural Network
ATMTP	-	Adaptive Thresholding Mean Ternary Pattern
BMP	-	Bitmap
CBIR	-	Content-Based Image Retrieval
CCD	-	Charge-coupled device
CCM	-	Colour Co – occurrence Matrix
CCPM	-	Conditional Co-occurrence Probabilities Matrix
CFA	-	Color Filter Array
CFS	-	Correlation based Feature Selection
CLBP	-	Completed Local Binary Pattern
CLTP	-	Completed Local Ternary Pattern
CMFD	-	Copy Move Forgery Detection
CMOS	-	Complementary Metal-Oxide-Semiconductor
CRF	-	Camera response function
CRF	-	Camera Response Function
CS-LBP	-	Centre Symmetric – Local Binary Pattern
DCT	-	Discrete Cosine Transform
DWT	-	Discrete Wavelet Transform
FFT	-	Fast Fourier Transform
FM	-	Fractal Matrix
FN	-	False Negative
FP	-	False Positive
FPR	-	False Positive Rate
GF	-	Gabor Feature
GIMP	-	GNU Image Manipulation Program
GLCM	-	Gray Level Co-occurrence Matrix

GMRF	-	Gaussian Markov Random Field
HOG	-	Histogram of Oriented Gradient
IFDS	-	Image Forgery Detection System
IQMs	-	Image Quality Metrics
JPEG	-	Joint Photographic Experts Group
LBP	-	Local Binary Pattern
LCD	-	Liquid Crystal Display
LPIPs	-	Locally Planar Irradiance Points
LPIPs	-	locally planar irradiance points
LPQ	-	Local Phase Quantization
LTP	-	Local Ternary Pattern
MRF	-	Markov Random Fields
NDC	-	Nearest Distance Classifier
NN	-	Neural Network
PCA	-	Principal component analysis
PIDT	-	Passive Image Tampering Detection
PITM	-	Passive Image Tampering Detection
PLS	-	Partial Least Squares
PLS-DA	-	Partial Least Squares - discriminant analysis.
POEM	-	Patterns of Oriented Edge Magnitudes
PRNU	-	Photo Response No Uniformity
PRNU	-	photo-response no uniformity
QDC	-	Quadratic Classifier
QDCT	-	Quaternion Discrete Cosine Transform
RBF	-	Radial Basis Function
RBIR	-	Received Bit Information Rate
RGB	-	Red, Green, and Blue
ROC	-	Receiver Operating Characteristics
ROI	-	Region of Interest
SAR	-	Synthetic Aperture Radar (SAR)
SFD	-	Splicing Forgery Detection
SFS	-	Sequential forward selection
SIFT	-	Scale-Invariant Feature Transform
SNR	-	Signal noise ratio

SPN	-	Sensor pattern noise
SPT	-	Steerable Pyramid Transform
SRIS	-	Selective Region Image Segmentation
SVM	-	Support Vector Machines
TIFF	-	Tagged Image File Format
TN	-	True Negative
TNR	-	True Negative Rate
TP	-	True Positive
TPR	-	True Positive Rate
WLD	-	Weber law Descriptors

LIST OF SYMBOLS

t	-	Thresholding value
m	-	Mean value
$S_{Adaptive}$	-	Adaptive standard deviation for the target window
s_{W}	-	Standard deviation of the window
m_b	-	Mean value of the whole block
S_{min}	-	Minimum standard deviation
s_{max}	-	Maximum standard deviation
max_{level}	-	Maximum gray level value
g_p	-	Neighbouring pixel of the centre pixel
g_{men}	-	Mean gray value of the cell
C	-	Average
m_p^{upper}	-	Upper magnitude
m_p^{lower}	-	Lower magnitude
$\bar{x}$	-	Average
n	-	Sample size
dxy	-	Displacement vector
$C(i,j)$	-	Matrix
P_{ij}	-	Element i,j of the normalized symmetrical CCM.
N	-	Number of gray levels
μ	-	CCM mean
σ^2	-	Variance of the intensities of all reference pixels
x,y,z,w,u	-	Parameters
Cn	-	Channel of image
$(\Delta x, \Delta y)$	-	Translation vector

$(cu \rightarrow cy)$	-	Couple of channel
(r_i, r_j)	-	Pixel local
f	-	Frequency
θ	-	Direction
(m, n)	-	Dimension
π	-	Pi constant
$\sum$	-	Summation
(x', y')	-	Major axis
l	-	Scale
k	-	Orientation
λ	-	aspect ratio
γ	-	sharpness along the major axis x
η	-	sharpness along the major axis y
$x_{l,k}$	-	Gabor wavlet
A ∩ B	-	Intersection
A ∪ B	-	Union

LIST OF ALGORITHM

CHAPTER 1

INTRODUCTION

1.1 Background

Simplicity of changing image content without leaving obvious traces behind has highly contributed to improving image forensic techniques that determine whether image being original or tampered. However, image forensic tools can be classified either into active and passive category. An authentication data inserted in image during acquirement process is deemed essential for active techniques. While passive techniques require image content only for tampering detection.

The importance of passive forensics has noticeably increased given various software tools available that can be used to alter original content without leaving visible traces besides wider awareness of such tampering. Therefore, several passive image tamper detection techniques have been proposed in the literature where some of them use feature extraction methods for detecting both of tampering and forgery object.

Image forgery is defined as an artistic technique adopted in photography that spans across centuries. The earlier photography years identified new avenues utilized in the designing and development of portraits. Photographers have resorted to effective techniques in enhancing quality of image through retouching it which pleases a customer and raises the due income of such work (Fakery, 1999; Farid, 2009).

The Civil War era initiated the retouching of the majority of photos, that had been considered necessary in enhancing the dramatic effect derived from the images. The professional photographers at that time integrated the existent knowledge pertaining to photo composition, which enhanced the merging of multiple photos, considered vital in enhancing the capacity of different artistic photos (see Figure 1.1). Noticeably, General Francis P. Blair on the far right was not appeared in original photograph (middle-top), but he appeared in the one available in the Library of Congress (middle-bottom). These three original photos are spliced to obtain a composited image (left). Many examples borrowed from early years of photography where forgeries in most cases were designed either to enhance insufficient details or to add humorous effects, but were never prepared for deception purposes. However, in early- to mid-20th century, photographers realized that image forgeries could be turned into effective weapon to influence public perception and historical events (Fakery, 1999).

Figure 1.1 Earliest examples of photograph manipulation (Farid, 2008)

Nazi Germany was famous for utilizing propaganda effectively as history witnessed several examples of image manipulations that were intentionally designed for misinformation purposes. Figure 1.2, illustrates image forgery where Hitler's propaganda minister Joseph Goebbels was removed from original image (right photograph).

Figure 1.2 Shows original image on the left where Hitler standing among several people, the forged image on the right where image of Hitler's minister of propaganda Joseph Goebbels was removed (Farid, 2008).

Due to the advent of advanced applications of digital image processing such as GIMP and Photoshop image manipulation becomes handy. Nowadays, armed with the sophisticated tools, any professional forgers can easily produce any kind of tampered images whether copy-move, splicing or retouching. Tools have indeed facilitated and encouraged image manipulation with or without malicious intentions (Jing and Shao, 2012).

Splicing is defined as common image manipulation process and also referred to as photomontage. In an effort to initiate the manipulation, a forger integrates varied areas out of different images into a single image. Retouching of image does not incorporate a change to the entire image, but integrates a slight change to image quality, which identifies the method as a less-corrupting form of image forgery (Elwin *et al.,* 2010; Redi *et al.,*2011).

1.2 Problem Background

Traditional image splicing process necessitated a human inspection, which considered necessary in maintaining high levels of accuracy pertaining to the detection of the specific elements coupled with providing high-quality analysis. However, the traditional image splicing model has been considered less efficient and effective as it entails a lot of time, high levels of human involvement and labor required for process. Increased adoption of new technology pertaining to the image splicing process has influenced a rise in the number of doctored photographs in circulation identified as being bigger than the existent volume that may be verified through human inspection. Poor existence and adoption of image verification processes has led to decreased viability attached to automated content through lack of the necessary and appropriate verification systems. Additionally, development of automated algorithms influence the possible level of manipulation, which delimits the level of human inspection leading to increased manipulation of images due to the lack of necessary verification systems (Sridevi *et al.,* 2012).

Increased technological development has influenced the identification of a rise in the number of digital splicing detection available in the market. The most popular utilization of image splicing detection technology is identified in newspapers and magazines, which necessitates development of computerized solutions geared towards influencing the verification of the authenticity of photographs prior to their publishing. The process necessitates adoption of automated processes considered necessary for publishing houses due to the existence of high throughput that necessitates continuous provision of new articles thus necessitating the value attached to the verification process. Criminal justice system identifies another field that emphasizes the verification of photographs to ensure that images remain permissible in court. It also emphasizes adopting solid verification systems and processes pertaining to any image submitted to court as evidence. The judicial system utilizes computerized algorithms necessary in limiting the potential of malicious human interventions, which influences the adoption of an objective investigation process. Finance industry considered as a pivotal industry to economy, and may experience most benefit through adopting of splicing techniques. The process may influence the analysis process experienced by individuals in a sector pertaining to the analysis of large number of transactions carried out on an almost daily basis. The adoption of the splicing technique in the finance industry may delimit the level of financial fraud in the sector, which will reduce the level of monetary loss through adopting adept detection fraud-detection mechanisms. Additionally, increased utilization of splicing techniques will influence the adoption of fast and reliable tools, which is vital in enhancing the viability attached to the process (Sekeh *et al.,* 2011).

The adoption of digital splicing technology detection tools remains necessary in influencing the level of digital detection as it influences the efficiency attached to the process coupled with the identification of the viability of images presented. However, digital splicing technology is not designed to replace human element attached to the process, but instead seeks to enhance the process through fast verification, which reduces the integration of imperfect decisions regarding the process. However, the response time incurred in relation to criminal justice and financial fraud is considerably longer, but remains instrumental as it provides highest levels of accuracy pertaining to the process.

The importance, attached to the process, necessitates the integration of splicing detection tools, which identifies the first line of defense as it influences the identification of suspicious cases. The process provides human experts with an opportunity to provide the final verdict through analyzing the automated results pertaining to the overall process.

Through the analysis of technical capacity, the process may encounter several shortcomings identified at two specific levels including image-level binary decision and tampering operation identification as illustrated in figure1.3. The process necessitates development of a comprehensive study that integrates novel ideas developing from the identified levels, which identifies the level of urgency attached to the processes (Shivakumar and Baboo, 2011).

Figure 1.3 Technical problems in image splicing.

Above image is considered doctored through integrating image-level binary authenticity decision (classification), and identifies fragments of splicing, which is identified through the analysis of tampering operation identification (identification).

Image-Level Binary Authenticity Decision involves the determination of the authenticity of image in which image may be doctored, but the lack of determination renders doctored image to be considered untrustworthy. In most instances, the global decision remains instrumental in the analysis of a photograph without incorporating additional information.

The definitions presented pertaining to image authenticity remains reliant on the provided situation. In most instances, the terms ‘spliced images’ and ‘natural images’ are used interchangeably. (Brinkmann, 2008) defines natural images as distinct images from range photographs. This study defines a spliced image as an image captured by a single camera in one process. Therefore, the definition maintains that a composite image from multiple captures and locations and incorporates graphics is not authentic.

Tampering Operation Identification: Image splicing develops a varied of technical questions through the identification of the tampering questions utilized in the manipulation of the image. The process influences the understanding of the image together with the development of a binary decision. The identification of the manipulation process to be utilized influences the interpretation process pertaining to practical applications. The individual detectors are developed through the analysis of the existent artifacts from the targeted operations, and hence may be tailored to the specific application.

There exists varied forms of tampering operations including copy and paste (splicing), edge smoothing or matting after splicing (using either 2D filtering or alpha blending), color adjustment together with the provision of duplicates and deletion of scientific images (Fridrich *et al.,* 2001). Splicing has developed into the most common tampering methodology adopted, which have influenced the development of numerous results. The analysis of images and natural scenes remains dependent on the existent levels of inconsistencies among varied image parts. (Fan and De Queiroz, 2003) maintains that splicing detection has been enhanced through the utilization of image-level statistical analysis together with quantization artifacts pertaining to JPEG images (Saha, 2000).

Splicing has been identified as a vital form of forgery as in which one or more images (or parts of an image) are merged into one composite image. In fact, there are more subtle cases found in the standard datasets CASIA v1.0, CASIA v2.0 and Colombia whereby a background is blurred shallow depth, noises, homogenous area, and combined attacks, cases misclassified by all the previous researches. Figure 1.4 illustrates the above cases.

In addition to that, most of the professional forgers normally hide traces of the forgeries by applying some forms of attacks such as photometric manipulation. Such attacks usually generate seamlessly integrated images where forgery detection becomes visually impossible and technically too hard. Therefore, Gaussian noise, blurring shallow depth, colour adjustment, JPEG compression, smoothing edges, and homogenous region are considered as commonly used photometric manipulation techniques.

One of the most common techniques used nowadays is shallow depth of field. It is a technique by which the descriptions of an image are given where a specific area of an image is very sharp while other components stay blurred, given that shallow depth of field and alike is very challenging to assign its authenticity because the blurry influence creates large gap in terms of intensity estimate between the blurry part and the object of interest as shown in Figure 1.4, where above technique applied to capture image of eagle in the center of the interest with sharp resolution, meantime, the sea was out of focus purposely so to give a blurry influence. This actually created a sudden change concerning the intensity value of boundary pixels of the eagle in contrast to the background pixels, which leads to an incorrect classification of image by proposed approach. Simply, photomontage experts use this technology to conceal traces of image splicing in order to produce a faultless digital image.

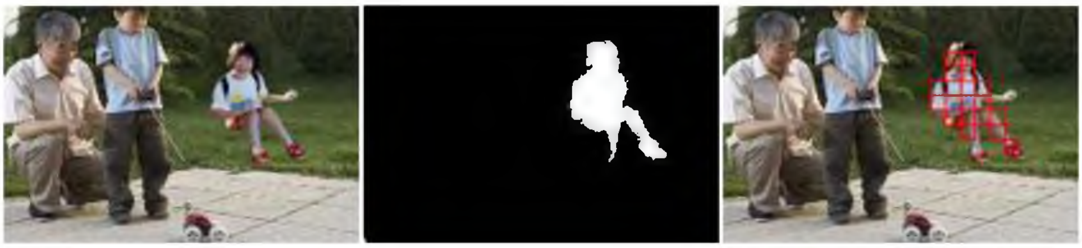
Figure 1.4 Sample of complicated cases that previous researchers failed to detect

Apart from that, another challenging issue is the presence of homogeneous regions in spliced images – same kind of nature such as sky, cloud, wall, ocean, river, bushes, grass et cetera. This type of nature, which normally produces a lot of false negative (i.e. a true object is wrongly detected as a false object), has obviously affected the accuracy (Manu and Mehtre, 2017; Li, *et al.,* 2017; Alahmadi *et al.*, 2017; Agarwal and Chand, 2018). An excerpt of CASIA v1.0, CASIA v2.0 and Colombia dataset for this type of tampered images can be seen in Figure 1.5 below.

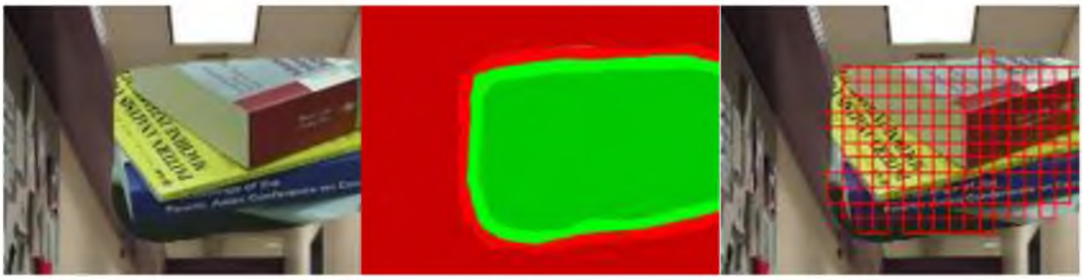
Figure 1.5 Sample of images contain homogeneous region

Detection of suspicious objects within spliced image is also a challenging issue in image forensics. The ability of pinpointing the area of suspicion in an image allows providing convincing explanations about the suspected tampering. For example, once a person within a picture being successfully identified as spliced, will serve as an informative basis for experts to extract further details of image regions (forgery object) and conduct in-depth examination. Figure 1.6 illustrates the above case.

A: Image forgery object in CASIA TIDE V1.0.



B: Image forgery object in CASIA TIDE V2.0.



C: Image forgery object in Colombia.

Figure 1.6 Samples of object forgery detection

Edge smoothening (utilizing either alpha blending or 2D filtering), color adjustment, duplication and deletion splicing (copy-paste) are deemed as some of renowned cases of tampering operations as proposed by (Fridrich *et al.*, 2001). Splicing is the distinctive image altering technique that has been studied for quite a while attached with various solutions being proposed accordingly. According to (Fan and De Queiroz, 2003), majority of studies are dependent on the discrepancy amid various sections of spliced images, for the natural scene images. Arguably, splicing is identified through image-level statistical evaluation, while quantization artifacts definite to JPEG compression set-up are engaged in detecting editing in digital images (Fan and De Queiroz, 2003; Saha, 2000).

1.3 Problem Statement

Image splicing is deemed as one of the main widespread image manipulation techniques, typically employed in manipulating digital image for the purposes of forgery performances. In splicing, copy-pasting of image from one section to another different section or image is considered, forming a composite image. The copied section may be altered due to some pre-processing activities to add some types of photometric attacks such as blurring shallow depth, homogeneous regions, or additive noise to merge the copied section with the complete image.

It involves a myriad of challenges faced by passive technique of detecting image forgeries and equally have their constraints and setbacks. One of the fascinating challenges facing the current scholars and researchers in this field is reducing the rate of counterfeit positive of such approaches in establishing effusive automatic system (Scheme) with capacity to identify image falsification from a wide perspective of image formats, as their performances are ineffective when dealing with the photometric attacks such as (blurring shallow depth, and Gaussian noise), in addition to homogeneous regions and combined attacks (Manu and Mehtre, 2017; Alahmadi et al., 2017). In addition, system detecting such as falsification, is designed to increase its dependability, robustness, and competence of operation. Moreover, detecting forgery object within spliced image is also critical challenge despite the accomplishments obtained by previous studies concerning spliced image detection, as far as author knew, none of them had addressed the improvement of forgery object detection within spliced image to date (A. Alahmadi *et al.,* 2017; Li *et al*., 2017). All objects should be taken into consideration during object forgery detection, image segmentation still, however, represents difficult because of the huge variability of object shape and variation of image quality. Furthermore, low contrast between different structures or even when different structures have similar appearances in image can cause considerable difficulties (Marmanis *et al.,* 2018).

Therefore, current study intends to discuss aforementioned setbacks entailed detecting any image forgery and splicing activities by using additional transform-based aspects for the purposes of augmenting the rate of accuracy.

1.4 Aim

To propose a new detection scheme of splicing image forgery for improving detection accuracy.

1.5 Research Objectives

This study aims at achieving the following goals :

i. Extract suitable features by developing and designing a new image texture descriptor to reduce the impact of blurring shallow depth, homogenous area and noise attacks in order to improve the accuracy of spliced forgery detection.
ii. Extract suitable features by improving segmentation method within a selective region in order to detect the forgery object found in spliced image.
iii. Develop a new spliced image forgery detection scheme to improve the accuracy.

1.6 Research Scope

The focus of the research will be towards:

i. The study utilizes three Standard Dataset CASIA v1.0, CASIA v2.0, and Colombia [(A. A. Alahmadi, Hussain, Aboalsamh, Muhammad, & Bebis, 2013), (Hsu & Chang, 2006)] throughout Splicing Forgery Detection (SFD) process to evaluate the performance of proposed SFD.
ii. The study focuses on the detection of accuracy level.
iii. Presence of blurring shallow depth and homogenous region photometric attacks is beyond the scope of this study
iv. Detect forgery objects inside spliced image is beyond the scope of this study.

1.7 Research Significance

The urgent need to develop verification processes pertaining to image detection requires additional advanced applications pertaining to splicing image detection. Additionally, the varied scope of application use presents a viable opportunity and growing need in the market. Through the identification of available authentication techniques, the study seeks to provide an innate understanding to image splicing and possible solutions.

Hopefully, proposed scheme of Spliced Forgery Detection (SFD) will overcome challenges existing in forgery detection. Proposed SFD may achieve so by reducing the impact of the blurring shallow depth and noise, extracting robust feature against many types of attacks and reducing the false matching.

In spite of the existing SFD studies have shown some encouraging results, but these results as well as employed methods have been designed to deal only with tampered image under a single attack. The main goal of this study is to propose state-of the- art, optimized and innovative techniques of spliced forgery detection.

Proposed technique should not be limited only to deal with the tampered image exposed to single attacks, but also to deal with the type of double attacks. In the light of the issues above-mentioned, the results of this research will contribute to what is currently known Spliced Forgery Detection System. Nonetheless, the significance of this study is not only limited to forgery detection, but also developing a new descriptor can be used in the future in many applications in the field of computer vision.

1.8 Thesis Organization

This thesis incorporates seven chapters: introduction, literature review, research methodology, proposed adaptive threshold meant ternary pattern, forgery object detection based on selection region segmentation, forgery object detection, evaluation and discussion, conclusion and future work recommendations. The introduction provides a full background of study subject to support identification of study objectives.

Chapter two analyses current literature related to image splicing through examining methods and applications available in the markets. This chapter considerably promotes a comprehension of study objectives.

Chapter three provides detailed analysis of methodological processes adopted in research study. It combines both quantitative and qualitative analyses essential to identify current study objectives. It also provides an ethical analysis relevant to study objectives.

In Chapter four, a new image texture descriptor, namely Adaptive Thresholding Mean Ternary Pattern (ATMTP) is presented. That will be used in proposed SFD scheme to improve detection accuracy. Then discusses detailed design and development of proposed SFD scheme, which includes: pre-processing, image partition, Texture features extraction using ATMTP, HOG, and CCM, ANN classifier, results of image spliced detection.

Chapter five discusses detailed design and development of proposed scheme of object forgery detection, which includes: Selective region segmentation, block partition, block-based Gabor feature extraction, SVM score, and results of detect forgery object.

Chapter six discusses detailed evaluation of experimental results, investigations, analyses and discussions regarding achievement of desired goals. Performances of image splicing forgery detection and object forgery detection proposed assessed utilizing different measures. The evaluation and discussion section will provide an analysis of identified results in an effort to determine the existent factors influencing the process and applicability of proposed applications and systems.

Chapter seven highlights the key contributions, significant findings, and recommendations for future work of current study.

REFERENCES

Agarwal, S. and Chand, S. (2015) 'Image forgery detection using multi scale entropy filter and local phase quantization', *International journal of image, graphics and signal processing*. Modern Education and Computer Science Press, 7(10), p. 78.

Agarwal, S. and Chand, S. (2018) 'Image forgery detection using co-occurrence-based texture operator in frequency domain', *Advances in Intelligent Systems and Computing*, pp. 117–122. doi: 10.1007/978-981-10-3373-5_10.

Aizenberg, I., Butakoff, C., Karnaukhov, V., Merzlyakov, N. and Milukova, O. (2003) 'Type of Blur and Blur Parameters Identification Using Neural Network and its Application to Image Restoration', pp. 1–7.

Al-Qershi, O. M. and Khoo, B. E. (2013) 'Passive detection of copy-move forgery in digital images: State-of-the-art', *Forensic Science International*. Elsevier Ireland Ltd, 231(1–3), pp. 284–295. doi: 10.1016/j.forsciint.2013.05.027.

Alahmadi, A. A., Hussain, M., Aboalsamh, H., Muhammad, G. and Bebis, G. (2013) 'Splicing image forgery detection based on DCT and Local Binary Pattern', *2013 IEEE Global Conference on Signal and Information Processing, GlobalSIP 2013 - Proceedings*, pp. 253–256. doi: 10.1109/GlobalSIP.2013.6736863.

Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G. and Mathkour, H. (2017) 'Passive detection of image forgery using DCT and local binary pattern', *Signal, Image and Video Processing*. Springer, 11(1), pp. 81–88.

Ansari, M. D., Ghrera, S. P. and Tyagi, V. (2014) 'Pixel-Based Image Forgery Detection: A Review', *IETE Journal of Education*. Taylor & Francis, 55(1), pp. 40–46. doi: 10.1080/09747338.2014.921415.

Arunkumar, N., Ramkumar, K., Venkatraman, V., Abdulhay, E., Fernandes, S. L., Kadry, S. and Segal, S. (2017) 'Classification of focal and non focal EEG using entropies', *Pattern Recognition Letters*. Elsevier, 94, pp. 112–117.

Atici, A. and Yarman-Vural, F. (1997) 'A heuristic method for Arabic character recognition', *Signal Process*, 62, pp. 87–99.

Bahrami, K. and Kot, A. C. (2015) 'Image Splicing Localization Based on Blur Type Inconsistency', pp. 1042–1045.

Bayram, S., Avc\iba\cs, \.Ismail, Sankur, B. and Memon, N. (2006) 'Image manipulation detection', *Journal of Electronic Imaging*. International Society for Optics and Photonics, 15(4), p. 41102.

Birajdar, G. K. and Mankar, V. H. (2013) 'Digital image forgery detection using passive techniques: A survey', *Digital Investigation*. Elsevier Ltd, 10(3), pp. 226–245. doi: 10.1016/j.diin.2013.04.007.

Box, P. O. (2009) 'EFFECTIVE IMAGE SPLICING DETECTION BASED ON IMAGE CHROMA Wei Wang , Jing Dong and Tieniu Tan National Laboratory of Pattern Recognition , Institute of Automation , Chinese Academy of Sciences ', pp. 1257–1260.

Brahnam, S., Jain, L. C., Nanni, L., & Lumini, A. (Eds.). (2014). Local binary patterns: new variants and applications. Springer Berlin Heidelberg.

Bravo-Solorio, S. and Nandi, A. K. (2011) 'Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics', *Signal Processing*. Elsevier, 91(8), pp. 1759–1770. doi: 10.1016/j.sigpro.2011.01.022.

Brinkmann, R. (2008) *The art and science of digital compositing: Techniques for visual effects, animation and motion graphics*. Morgan Kaufmann.

Bruno, A. and Informatica, I. (2010) 'Copy-Move Forgery Detection via Texture Description', *ACM Workshop on Multimedia in Forensics, Security and Intelligence, Co-located with ACM Multimedia*, pp. 59–64. doi: 10.1145/1877972.1877990.

Cao, H. and Kot, A. C. (2010) 'Identification of recaptured photographs on LCD screens', in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, pp. 1790–1793.

Chen, M.-Y., Kundu, A. and Zhou, J. (1994) 'Off-line handwritten word recognition using a hidden Markov model type stochastic network', *IEEE transactions on Pattern analysis and Machine Intelligence*. IEEE, 16(5), pp. 481–496.

Chennamma, H. R. and Rangarajan, L. (2011) 'Image Splicing Detection Using Inherent Lens Radial Distortion', *International Journal of Computer Science Issues*, 7(6), p. 10. Available at: http://arxiv.org/abs/1105.4712.

Cortes, C. and Vapnik, V. (1995a) 'Support-vector networks', *Machine learning*. Springer, 20(3), pp. 273–297.

Cortes, C. and Vapnik, V. (1995b) 'Support-Vector Networks', *Machine Learning*, 20(3), pp. 273–297. doi: 10.1023/A:1022627411411.

Dice, L. R. . (1945) 'Measures of the Amount of Ecologic Association Between Species', *Ecology*, 26(3), pp. 297–302. doi: 10.2307/1932409.

Elwin, J. G. R., Aditya, T. S. and Shankar, S. M. (2010) 'Survey on passive methods of image tampering detection', in *Communication and computational intelligence (INCOCCI), 2010 international conference on*, pp. 431–436.

Fakery, P. (1999) 'The History and Techniques of Photographic Deception and Manipulation', *Dino Brugioni. Brassy's*.

Fan, Z. and De Queiroz, R. L. (2003) 'Identification of bitmap compression history: JPEG detection and quantizer estimation', *IEEE Transactions on Image Processing*. IEEE, 12(2), pp. 230–235.

Farid, H. (2008) 'Digital image forensics', *Scientific American*. JSTOR, 298(6), pp. 66–71.

Farid, H. (2009a) 'Exposing digital forgeries from JPEG ghosts', *IEEE transactions on information forensics and security*. IEEE, 4(1), pp. 154–160.

Farid, H. (2009b) 'Image forgery detection', *IEEE Signal Processing Magazine*, 26(2), pp. 16–25. doi: 10.1109/MSP.2008.931079.

Farid, H. (2009c) 'Image forgery detection', *IEEE Signal processing magazine*. IEEE, 26(2), pp. 16–25.

Fridrich, J., Goljan, M. and Du, R. (2001) 'Steganalysis based on JPEG compatibility', in *Multimedia Systems and Applications IV*, pp. 275–281.

Gao, X., Ng, T.-T., Qiu, B. and Chang, S.-F. (2010) 'Single-view recaptured image detection based on physics-based features', in *Multimedia and Expo (ICME), 2010 IEEE International Conference on*, pp. 1469–1474.

Gharibi, F., RavanJamjah, J., Akhlaghian, F., Azami, B. Z. and Alirezaie, J. (2011) 'Robust detection of copy-move forgery using texture features', in *Electrical Engineering (ICEE), 2011 19th Iranian Conference on*, pp. 1–4.

Guo, Z., Zhang, L., & Zhang, D. (2010). A completed modeling of local binary pattern operator for texture classification. IEEE Transactions on Image Processing, 19(6), 1657-1663.

Farid, Hany, and Siwei Lyu, (2003). Higher-Order Wavelet Statistics and Their Application to Digital Forensics. Null, IEEE. pp. 94.

Haralick, R. M. and Watson, L. T. (1981) 'A Facet Model for Image Data', *Computer Graphics and Image Processing*, pp. 113–129.

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*. Elsevier, 45(12), pp. 4292–4299. doi: 10.1016/j.patcog.2012.05.014.

Heikkilä, M., Pietikäinen, M., & Schmid, C. (2006). Description of interest regions with center-symmetric local binary patterns. In Computer vision, graphics and image processing (pp. 58-69). Springer, Berlin, Heidelberg.

Hsu, H.-C. and Wang, M.-S. (2012) 'Detection of copy-move forgery image using Gabor descriptor', in *Anti-counterfeiting, security and identification (ASID), 2012 international conference on*, pp. 1–4.

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

Hsu, Y. F. and Chang, S. F. (2006) 'Detecting image splicing using geometry invariants and camera characteristics consistency', *2006 IEEE International Conference on Multimedia and Expo, ICME 2006 - Proceedings*, 2006, pp. 549–552. doi: 10.1109/ICME.2006.262447.

Hsu, Y. F. and Chang, S. F. (2010) 'Camera response functions for image forensics: An automatic algorithm for splicing detection', *IEEE Transactions on Information Forensics and Security*, 5(4), pp. 816–825. doi: 10.1109/TIFS.2010.2077628.

Hussain, M., Muhammad, G., Saleh, S. Q., Mirza, A. M. and Bebis, G. (2013) ‘Image forgery detection using multi-resolution Weber local descriptors’, *Eurocon 2013*, (July), pp. 1570–1577. doi: 10.1109/EUROCON.2013.6625186.

Hussain, M., Wajid, S. K., Elzaart, A. and Berbar, M. (2011) ‘A comparison of SVM kernel functions for breast cancer detection’, *Proceedings - 2011 8th International Conference on Computer Graphics, Imaging and Visualization, CGIV 2011*, pp. 145–150. doi: 10.1109/CGIV.2011.31.

Jaccard, P. (1912) ‘The Distribution of the Flora in the Alphine Zone’, *The New Phytologist*, XI(2), pp. 37–50. doi: 10.1111/j.1469-8137.1912.tb05611.x.

Jing, L. and Shao, C. (2012) ‘Image copy-move forgery detecting based on local invariant feature.’, *Journal of Multimedia*, 7(1).

Johnson, M. and Farid, H. (2008) ‘Detecting Photographic Composites of People’, *Digital Watermarking SE - 3*, 5041, pp. 19–33. doi: 10.1007/978-3-540-92238-4_3.

Johnson, M. K. and Farid, H. (2005) ‘Exposing digital forgeries by detecting inconsistencies in lighting’, *Proceedings of the 7th workshop on Multimedia and security - MM&Sec ’05*, pp. 1–10. doi: 10.1145/1073170.1073171.

Johnson, M. K. and Farid, H. (2006) ‘Metric measurements on a plane from a single image’, *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006-579*. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Metric+Measurements+on+a+Plane+from+a+Single+Image#0.

Johnson, M. K. and Farid, H. (2007) ‘Exposing Digital Forgeries in Complex Lighting Environments’, *Information Forensics and Security, IEEE Transactions on*, 2(3), pp. 450–461. doi: 10.1109/TIFS.2007.903848.

Johnson, M. K. and Farid, H. (2007) ‘Exposing digital forgeries through specular highlights on the eye’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4567 LNCS, pp. 311–325. doi: 10.1007/978-3-540-77370-2_21.

Kakar, P., Sudha, N. and Ser, W. (2011) ‘Exposing digital image forgeries by detecting discrepancies in motion blur’, *IEEE Transactions on Multimedia*, 13(3), pp. 443–452. doi: 10.1109/TMM.2011.2121056.

Kang, X. and Wei, S. (2008) ‘Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics’, *2008 International Conference on Computer Science and Software Engineering*, pp. 926–930. doi: 10.1109/CSSE.2008.876.

Kirchner, M. (2008) ‘Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue’, *Proceedings of the 10th ACM workshop on Multimedia and security - MM&Sec '08*, p. 11. doi: 10.1145/1411328.1411333.

Kong, H. and Box, P. O. (2010) ‘Proceedings of 2010 IEEE 17th International Conference on Image Processing IMAGE TAMPERING DETECTION BASED ON STATIONARY DISTRIBUTION OF MARKOV CHAIN National Laboratory of Pattern Recognition , Institute of Automation , Chinese Academy of Sciences ’, pp. 2101–2104.

Lee, J.-C. (2015) ‘Copy-move image forgery detection based on Gabor magnitude’, *Journal of Visual Communication and Image Representation*. Elsevier, 31, pp. 320–334.

Lee, S., Shamma, D. A. and Gooch, B. (2006) ‘Detecting false captioning using common-sense reasoning’, *digital investigation*. Elsevier, 3, pp. 65–70.

Lee, W.-L. and Fan, K.-C. (2000) ‘Document image preprocessing based on optimal Boolean filters’, *Signal processing*. Elsevier, 80(1), pp. 45–55.

Legault, R. and Suen, C. Y. (1997) ‘Optimal local weighted averaging methods in contour smoothing’, *IEEE Transactions on Pattern Analysis and Machine Intelligence*. IEEE, 19(8), pp. 801–817.

Leu, J.-G. (2000) ‘Edge sharpening through ramp width reduction’, *Image and Vision Computing*. Elsevier, 18(6), pp. 501–514.

Li, C., Ma, Q., Xiao, L., Li, M. and Zhang, A. (2017) ‘Image splicing detection based on Markov features in QDCT domain’, *Neurocomputing*. Elsevier, 228, pp. 29–36.

Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J. F. and Pan, J.-S. (2013) 'An efficient scheme for detecting copy-move forged images by local binary patterns', *Journal of Information Hiding and Multimedia Signal Processing*, 4(1), pp. 46–56.

Liang, W., Tang, M., Jing, L., Sangaiah, A. K. and Huang, Y. (2017) 'SIRSE: A secure identity recognition scheme based on electroencephalogram data with multi-factor feature', *Computers & Electrical Engineering*. Elsevier.

Lin, C. and Chang, S. (1998) 'Generating Robust Digital Signature for Image / Video Authentication', *Multimedia and Security Workshop at ACM Multimedia '98, Bristol, U.K.*, (September).

Liu, C. and Wechsler, H. (2002) 'Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition.', *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society*, 11(4), pp. 467–476. doi: 10.1109/TIP.2002.999679.

Liu, L., Zhao, L., Long, Y., Kuang, G., & Fieguth, P. (2012). Extended local binary patterns for texture classification. Image and Vision Computing, 30(2), 86-99.

Liu, Q. and Sung, a. H. (2009) 'A new approach for JPEG resize and image splicing detection', *Proceedings of the First ACM workshop on Multimedia in forensics - MiFor '09*, p. 43. doi: 10.1145/1631081.1631092.

Lukas, J., Fridrich, J. and Goljan, M. (2006) 'Detecting digital image forgeries using sensor pattern noise', *Proceedings of the SPIE*, 6072, p. 60720Y–60720Y–11. doi: 10.1117/12.640109.

Mahdian, B. and Saic, S. (2009) 'Using noise inconsistencies for blind image forensics', *Image and Vision Computing*. Elsevier B.V., 27(10), pp. 1497–1503. doi: 10.1016/j.imavis.2009.02.001.

Mahdian, B. and Saic, S. (2010) 'A bibliography on blind methods for identifying image forgery', *Signal Processing: Image Communication*. Elsevier, 25(6), pp. 389–399. doi: 10.1016/j.image.2010.05.003.

Manu, V. T. and Mehtre, B. M. (2017) 'Blind technique using blocking artifacts and entropy of histograms for image tampering detection', in *Second International Workshop on Pattern Recognition*, p. 104430T.

Marmanis, D., Schindler, K., Wegner, J. D., Galliani, S., Datcu, M. and Stilla, U. (2018) 'Classification with an edge: Improving semantic image segmentation with boundary detection', *ISPRS Journal of Photogrammetry and Remote Sensing*, 135, pp. 158–172. doi: 10.1016/j.isprsjprs.2017.11.009.

Moreno, P., Bernardino, A. and Santos-Victor, J. (2005) 'Gabor parameter selection for local feature detection', in *Iberian Conference on Pattern Recognition and Image Analysis*, pp. 11–19.

Muhammad, G., Al-Hammadi, M. H., Hussain, M. and Bebis, G. (2014) 'Image forgery detection using steerable pyramid transform and local binary pattern', *Machine Vision and Applications*, 25(4), pp. 985–995. doi: 10.1007/s00138-013-0547-4.

Ng, R., Levoy, M., Duval, G., Horowitz, M. and Hanrahan, P. (2005) 'Light Field Photography with a Hand-held Plenoptic Camera', *Informational*, pp. 1–11. doi: 10.1.1.163.488.

Ng, T.-T., Chang, S.-F., Hsu, J., Xie, L. and Tsui, M.-P. (2005) 'Physics-motivated features for distinguishing photographic images and computer graphics', in *Proceedings of the 13th annual ACM international conference on Multimedia*, pp. 239–248.

Ng, T., Chang, S. and Sun, Q. (2004) 'A data set of authentic and spliced image blocks', *Columbia University, ADVENT …*.

Ng, T. T., Chang, S. F., Lin, C. Y. and Sun, Q. (2006) 'Passive-blind Image Forensics', *Multimedia Security Technologies for Digital Rights Management*, pp. 383–412. doi: 10.1016/B978-012369476-8/50017-8.

Ojala, T. and Pietikäinen, M. (2004) 'Texture Classification. Machine Vision and Media Processing Unit, University of Oulu, Finland'. ed.

Pan, Q., Darabos, C. and Moore, J. (2012) *Lecture Notes in Computer Science, Evolutionary Computation, Machine Learning and Data Mining in Bioinformatics*. doi: 10.1007/978-3-642-29066-4{_}11.

Pevzner, P. and Waterman, M. (2002) *Lecture Notes in Bioinformatics*, *Systems Biology*. doi: 10.1109/TIM.2002.802244.

Polesel, A., Ramponi, G. and Mathews, V. J. (1997) 'Adaptive unsharp masking for contrast enhancement', in *Image Processing, 1997. Proceedings., International Conference on*, pp. 267–270.

Qu, Z., Qiu, G. and Huang, J. (2009a) 'Detect Digital Image Splicing with Visual Cues.', *Information Hiding*, 5806, pp. 247–261. Available at: http://dblp.uni-trier.de/db/conf/ih/ih2009.html#QuQH09.

Qu, Z., Qiu, G. and Huang, J. (2009b) 'Detect digital image splicing with visual cues', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 5806 LNCS, pp. 247–261. doi: 10.1007/978-3-642-04431-1_18.

Rassem, T. H., & Khoo, B. E. (2014). Completed local ternary pattern for rotation invariant texture classification. The Scientific World Journal, 2014.

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

Redi, J. A., Taktak, W. and Dugelay, J. L. (2011) 'Digital image forensics: A booklet for beginners', *Multimedia Tools and Applications*, 51(1), pp. 133–162. doi: 10.1007/s11042-010-0620-1.

Redi, J. A., Taktak, W. and Dugelay, J. L. (2011) 'Digital Image Forensics: for Beginners.', *Multimedia Tools and Applications*, 51(1 SRC-GoogleScholar FG-0), pp. 133–162.

Reinhardt, J. M. and Higgins, W. E. (1996) 'Comparison between the morphological skeleton and morphological shape decomposition', *IEEE transactions on pattern analysis and machine intelligence*. IEEE, 18(9), pp. 951–957.

Rosales-Roldan, L., Cedillo-Hernandez, M., Nakano-Miyatake, M., Perez-Meana, H. and Kurkoski, B. (2013) 'Watermarking-based image authentication with recovery capability using halftoning technique', *Signal Processing: Image Communication*. Elsevier, 28(1), pp. 69–83. doi: 10.1016/j.image.2012.11.006.

Saha, S. (2000) 'Image compression—from DCT to wavelets: a review', *Crossroads*. ACM, 6(3), pp. 12–21.

Samuel, O. W., Asogbon, G. M., Sangaiah, A. K., Fang, P. and Li, G. (2017) 'An integrated decision support system based on ANN and Fuzzy_AHP for heart failure risk prediction', *Expert Systems with Applications*. Elsevier, 68, pp. 163–172.

Samuel, O. W., Zhou, H., Li, X., Wang, H., Zhang, H., Sangaiah, A. K. and Li, G. (2017) ‘Pattern recognition of electromyography signals based on novel time domain features for amputees’ limb motion classification’, *Computers & Electrical Engineering*. Elsevier.

Schaefer, G. and Stich, M. (2003) ‘UCID - An Uncompressed Colour Image Database’, *SPIE, Storage and Retrieval Methods and Applications for Multimedia*, 5307, pp. 472–480. doi: 10.1117/12.525375.

Sekeh, M. A., Maarof, M. A., Rohani, M. F. and Motiei, M. (2011) ‘Sequential Straightforward Clustering for Local Image Block Matching’, *World Academy of Science, Engineering and Technology*, 5(2), pp. 693–697.

Sengupta, M. and Mandal, J. K. (2013) ‘Authentication Through Hough Transformation Generated Signature on G-Let D3 Domain (AHSG)’, *Procedia Technology*. Elsevier B.V., 10, pp. 121–130. doi: 10.1016/j.protcy.2013.12.344.

Serra, J. (1994) ‘Morphological filtering: an overview’, *Signal processing*. Elsevier, 38(1), pp. 3–11.

Shah, H., Shinde, P. and Kukreja, J. (2013) ‘Retouching detection and steganalysis’, *International Journal of Engineering Innovations and Research*. International Journal of Engineering Innovations and Research (IJEIR), 2(6), p. 487.

Shen, L. L., Bai, L. and Fairhurst, M. (2007) ‘Gabor wavelets and General Discriminant Analysis for face identification and verification’, *Image and Vision Computing*, 25(5), pp. 553–563. doi: 10.1016/j.imavis.2006.05.002.

Shen, X., Shi, Z. and Chen, H. (2016) ‘Splicing image forgery detection using textural features based on the grey level co-occurrence matrices’, *IET Image Processing*. IET, 11(1), pp. 44–53.

Shieh, J.-M., Lou, D.-C. and Chang, M.-C. (2006) ‘A semi-blind digital watermarking scheme based on singular value decomposition’, *Computer Standards & Interfaces*, 28, pp. 428–440. doi: 10.1016/j.csi.2005.03.006.

Shivakumar, B. L. and Baboo, S. S. (2011) ‘Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods’, *Global Journal of Computer Science and Technology*, 10(7), pp. 61–65.

Solihin, Y. and Leedham, C. G. (1999) 'Integral ratio: a new class of global thresholding techniques for handwriting images', *IEEE Transactions on Pattern Analysis and Machine Intelligence*. IEEE, 21(8), pp. 761–768.

Sonka, M., Hlavac, V. and Boyle, R. (2012) 'Image Processing, Analysis, and Machine Vision', pp. 180–182.

Sonka, M., Hlavac, V. and Boyle, R. (2014) *Image processing, analysis, and machine vision*. Cengage Learning.

Sridevi, M., Mala, C. and Sanyam, S. (2012) 'Comparative study of image forgery and copy-move techniques', *Advances in Intelligent and Soft Computing*, 166 AISC(VOL. 1), pp. 715–723. doi: 10.1007/978-3-642-30157-5_71.

Suliman, A., Sulaiman, M. N., Othman, M. and Wirza, R. (2011) 'Chain Coding and Pre Processing Stages of Handwritten Character Image File', *electronic Journal of Computer Science and Information Technology*, 2(1).

SUN, S.-J., WU, Q. and LI, G.-H. (2009) 'Detection of Image Compositing Based on a Statistical Model for Natural Images', *Acta Automatica Sinica*. The Chinese Association of Automation and The Institute of Automation, Chinese Academy of Sciences, 35(12), pp. 1564–1568. doi: 10.1016/S1874-1029(08)60124-X.

Tan, X., & Triggs, B. (2007, October). Enhanced local texture feature sets for face recognition under difficult lighting conditions. In International Workshop on Analysis and Modeling of Faces and Gestures (pp. 168-182). Springer, Berlin, Heidelberg.

Wang, W., Dong, J. and Tan, T. (2010) 'Image tampering detection based on stationary distribution of Markov chain', in *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pp. 2101–2104.

Wei, W., Gulla, J. A. and Fu, Z. (2010) 'Advanced Intelligent Computing Theories and Applications', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6215(2), pp. 380–391. doi: 10.1007/978-3-642-14922-1.

Weiqi, L. U. O., Zhenhua, Q. U., Feng, P. a N. and Jiwu, H. (2007) 'A Survey of Passive Technology for Digital Image Forensics', *Frontiers of Computer Science in China*, 2, pp. 1–14. doi: 10.1007/s11515-007-0000-0.

Wu, J.-Y. (2011) 'MIMO CMAC neural network classifier for solving classification problems', *Applied Soft Computing*. Elsevier B.V., 11(2), pp. 2326–2333. doi: 10.1016/j.asoc.2010.08.013.

Xia, C., Hsu, W. and Lee, M. L. (2005) 'ERkNN: efficient reverse k-nearest neighbors retrieval with local kNN-distance estimation', *14th ACM international conference on Information and knowledge management*, pp. 533–540.

Yang, J. and Li, X. (1995) 'Boundary detection using mathematical morphology', *Pattern Recognition Letters*. Elsevier, 16(12), pp. 1277–1286.

Yu-Feng Hsu, S.-F. C. (2007) 'IMAGE SPLICING DETECTION USING CAMERA RESPONSE FUNCTION CONSISTENCY Department of Electrical Engineering Columbia University', *Image (Rochester, N.Y.)*, pp. 28–31.

Yu, H., Ng, T.-T. and Sun, Q. (2008) 'Recaptured photo detection using specularity distribution', in *Image Processing, 2008. ICIP 2008. 15th IEEE International Conference on*, pp. 3140–3143.

Yuan, J. H., Huang, D. S., Zhu, H. D., & Gan, Y. (2014, July). Completed hybrid local binary pattern for texture classification. In Neural Networks (IJCNN), 2014 International Joint Conference on (pp. 2050-2057). IEEE.

Zach, F., Riess, C. and Angelopoulou, E. (2012) 'through Classification of JPEG Ghosts', pp. 185–194.

Zhang, J., Feng, Z. and Su, Y. (2008) 'A new approach for detecting copy-move forgery in digital images', in *Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on*, pp. 362–366.

Zhang, R., Shen, J., Wei, F., Li, X. and Sangaiah, A. K. (2017) 'Medical image classification based on multi-scale non-negative sparse coding', *Artificial intelligence in medicine*. Elsevier, 83, pp. 44–51.

Zhang, Z., Kang, J. and Ren, Y. (2008) 'An effective algorithm of image splicing detection', *Proceedings - International Conference on Computer Science and Software Engineering, CSSE 2008*, 1(60473022), pp. 1035–1039. doi: 10.1109/CSSE.2008.1621.

Zhao, X., Wang, S., Li, S. and Li, J. (2011) 'Passive detection of image splicing using conditional co-occurrence probability matrix', *APSIPA ASC 2011 - Asia-Pacific Signal and Information Processing Association Annual Summit and Conference 2011*.

Zhao, Y., Huang, D. S., & Jia, W. (2012). Completed local binary count for rotation invariant texture classification. IEEE transactions on image processing, 21(10), 4492-4497.

Zhao, Y., Jia, W., Hu, R. X., & Min, H. (2013). Completed robust local binary pattern for texture classification. Neurocomputing, 106, 68-76.

Zheng, N., Wang, Y. and Xu, M. (2013) 'A LBP-Based Method for Detecting Copy-Move Forgery with Rotation', in *Multimedia and Ubiquitous Engineering*. Springer, pp. 261–267.

Zhi-ping, Z. and Xiao-xiang, Z. (2010) 'Image splicing detection based on image quality and analysis of variance', *Education Technology and Computer*