ANALYZING DIGITAL IMAGE MANIPULATION DETECTION ALGORITHMS

SINAN NAZAR MAJEED

AUGUST 2015

ANALYZING DIGITAL IMAGE MANIPULATION DETECTION ALGORITHMS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
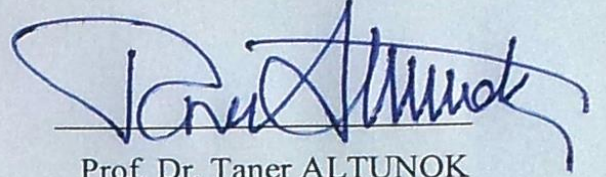**SCIENCES OF**
ÇANKAYA UNIVERSITY

BY
SINAN NAZAR MAJEED

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
MATHMATICS AND COMPUTER SCIENCE
INFORMATION TECHNOLOGY PROGRAM

AUGUST 2015

Title of the Thesis: **Analyzing Digital Image Manipulation Detection Algorithms.**

Submitted by **Sinan Nazar MAJEED**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.
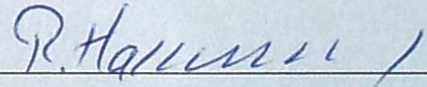
Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Billur KAYMAKÇALAN
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Reza HASSANPOUR
Supervisor

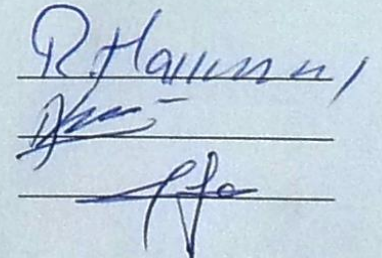**Examination Date:**   13.08.2015

Examining Committee Members:

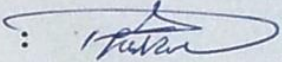|		
Assist. Prof. Dr. Reza HASSANPOUR	(Çankaya Univ.)	
Assist. Prof. Dr. Abdül Kadir GÖRÜR	(Çankaya Univ.)	
Assoc. Prof. Dr. Fahd JARAD	(UTAA)	

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name   : Sinan, MAJEED

Signature   :

Date   : 13.08.2015

ABSTRACT

ANALYZING DIGITAL IMAGE MANIPULATION DETECTION ALGORITHMS

MAJEED, Sinan Nazar

M.Sc., Department of Mathematics and Computer Science / Information Technology Program

Supervisor: Assist. Prof. Dr. Reza ZARE HASSANPOUR

August 2015, 51 pages

In recent years tampering in digital image is becoming very widespread and more interesting. With powerful Image software, editing tools make a tampered image easy, thus the field of image forensic has become very important and crucial. In this thesis, investigation is made on the image by depending on the traces that occur when the soft correlation between rows and columns are divested in altered images, in term of linear dependency and exploitation of these traces in image forensic, depending on the properties of singular value decomposition and derived features which can be helpful and accurate sufficiently to reveal the tampering that is done on the genuine digital image.

Keywords: Singular Value Decomposition, Image Forensics, Image Authentication, Fisher Linear Analysis**.**

ÖZ

DIJITAL GÖRÜNTÜ MANIPÜLASYONU ALGILAMA ALGORITMALARI ANALIZI

MAJEED, Sinan Nazar

Yüksek Lisans, Matematik-Bilgisayar Anabilim Dalı / Bilgi Teknolojileri Bölümü

Tez Danışmanı: Yrd. Doç. Dr. Reza ZARE HASSANPOUR

Ağustos 2015, 51 sayfa

Dijital görüntü kurcalama/bozma son yıllarda çok yaygın ve çok ilginç hale geliyor. Güçlü görüntü yazılım araçları son zamanlarda tahrif edilmiş resimleri, görüntüleri kolaylıkla düzeltilebilmekte ve böylece adli tıp alanında çok önemli ve hayati bir araç haline gelmektedir. Bu tezde araştırma ve sorgulama; satırlar ve sütunlar arasındaki yumuşak korelasyon ilişkilerinin bozuk görüntülerden tecrit edilmesi suretiyle ortaya çıkan izler üzerinde yapılmış ve yoğunlaştırılmıştır. Doğrusal bağlılık anlamında ve adli tıp alanında sözkonusu görüntü izlerinin incelenmesi bağlamında, tekil değer ayrışma özelliklerine bağlı olarak türetilen ve ortaya konan özellikler; original dijital görüntü üzerindeki bozulmaları, oynamaları ve manülasyonları ortaya çıkarmada faydalı ve yeterli olabilir.

Anahtar Kelimeler: Tekil değer ayrışımı , Adli Tıp ve Görüntü , Görüntü Doğrulama , Fisher Doğrusal Analizi

ACKNOWLEDGEMENTS

First of all, thanks to Almighty for granting me the strength and capacity to complete my study and to achieve success in my life.

I would also like to express my deep and sincere gratitude to all the professors of the Department of Mathematics and Computer Science for not sparing any efforts to help me throughout my study.

I am particularly grateful for the support and guidance given to me by my supervisor Dr. Reza HASSANPOUR and for his advice which has been of great help to me in completing my thesis.

Last but not the least, I would also like to express my profound appreciation of my parents, family and friends due to their continuous support and help that motivated me to go on with my study.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

FIGURES

LIST OF TABLES

TABLES

TABLES

LIST OF ABBREVIATIONS

BDCT   Block Discrete Cosine Transformation Domain

CCD   Charge-Coupled Device

CFA   Color Filter Array

CRF   Camera Response Function

DCT   Discrete Cosine Transform

DMWT   Discrete Meyer Wavelet Transform

DWT   Discrete Wavelet Transform

FAR   False Accept Rate

FLD   Fisher Linear Discriminant

IQM   Image Quality Metrics

JPEG   Joint Photographic Experts Group

MBDCT   Multi-size Block Discrete Cosine Transform

NMV   Normalized Mean Value

NSD   Normalized Standard Deviation

PCA   Principal Component Analysis

QDCT   Quantization Discrete Cosine Transform Coefficient

RBF   Radius Basis Function

SVD   Singular Value Decomposition

SVM   Support Vector Machine

CHAPTER 1

INTRODUCTION

1.1 Glance on Images' History

Nowadays images have become increasingly important in various fields of life. A simple example of the importance of images is in passports. Could one see a passport without a person's image? The answer is definitely not. In France, more specifically the region of east-central France, "Burgundy", the earliest lasting image in the form of a photograph was captured via camera in 1826 or 1827, by Joseph Nicéphore Niépce [1]. The first image manipulation recorded was in 1860, only a few decades after Niépce captured his photograph [2]. Even the famous picture of President Abraham Lincoln is, in fact, an altered picture; it is a mix of John Calhoun's (a southern politician) body, and Lincoln's head.
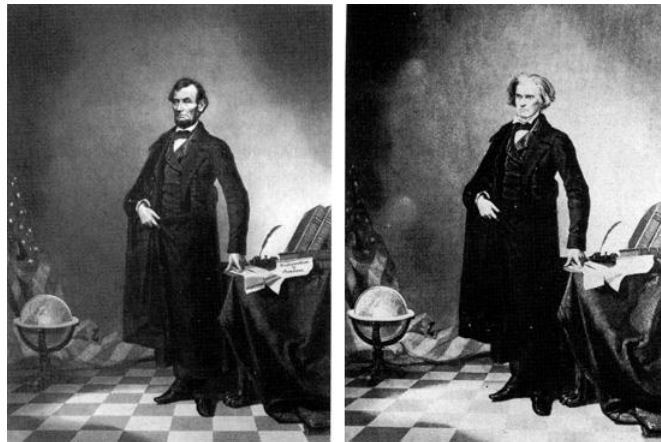
Figure 1 Example of altered image

Towards the 20th century, image manipulation increased in popularity. Adolf Hitler and Stalin were known for removing people from their photographs as they desired [2].
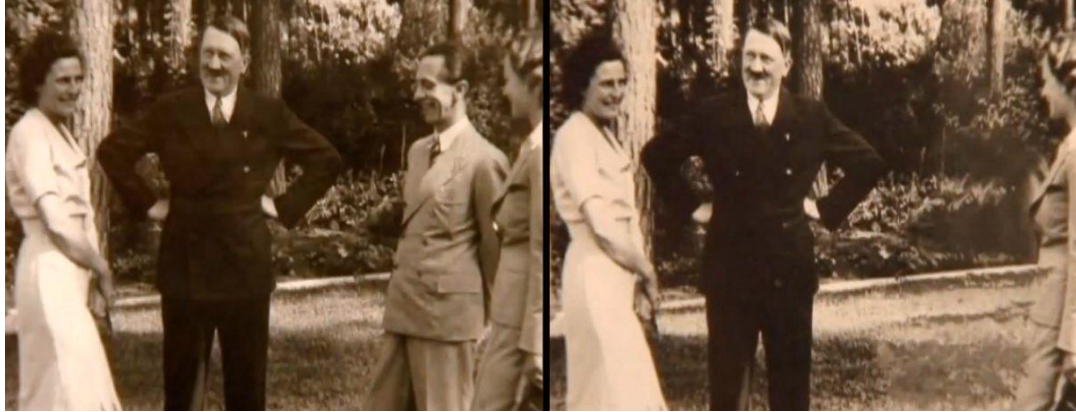
Figure 2 An example of forged image, the left image is original and the right image is modified

The first digital camera was invented by Steven Sasson in 1975 in Kodak laboratories, while the first digital image was created by Russell Kirsch in 1957 when he scanned his son's photograph. The image was of low resolution; (176×176) pixels, due to the incapability of computers to store much information at that time [3].

1.2 The Harms of Forging Images

Television, daily newspapers, magazines, websites, etc., are important sources of information, and they all make use of millions of images on a daily basis. Thanks to the rapid development in technology, it is not difficult to use graphics software, such as Photoshop, Coral, PhotoImpact, GIMP, etc., in fact, their easy use and low cost software make image modification very widespread.

Fake or tampered images can be submitted as evidence in the court of law to be used for making critical decisions, so one can imagine the horrific damage that these images may cause.

Another example of harm caused by manipulating images is the creation of ethnic tension. For instance, in India, the government put certain limitations on the inflow of

information to avoid the ethnic tension in the country that may be caused by forged images [2]. Hence, one can define image forgery as manipulating images without leaving any traces of the process. There are many types of image forgery including the following;

- Image splicing/composition: In this type, the mechanism aims to splice two or more images to form a new one [4]. An example for this is shown in figure 3. The modifications done to the "helicopter rescue" image are obvious; it has been scaled up and horizontally flipped to look more persuasive after the "the Shark" has been pasted on to it.

- Copy-move forgery: This type mostly aims to hide unwanted parts of an image by cloning another part from the same image and pasting it onto the unwanted part.
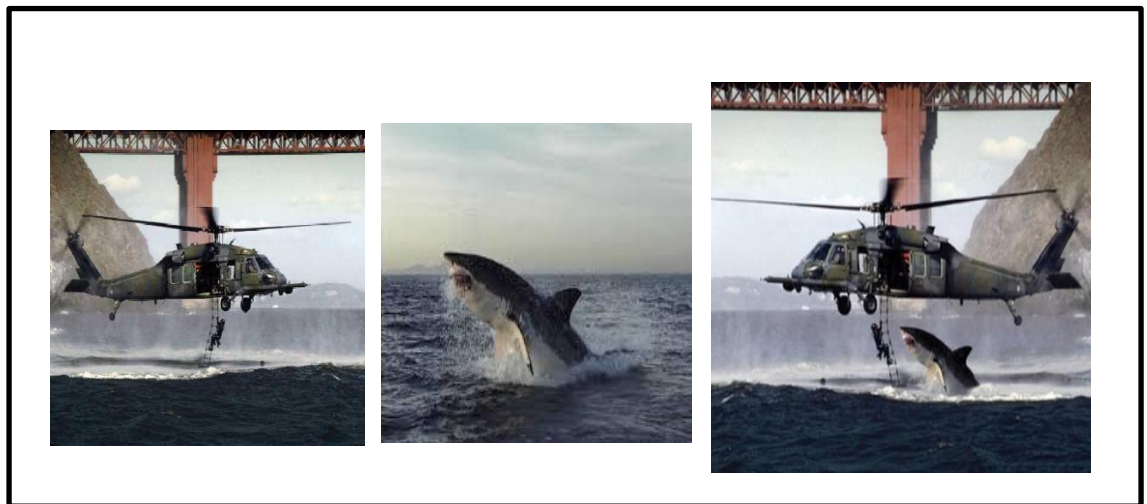
Figure 3 Example of image spliced

Figure 4 Example of copy-move forgery. The vehicle in the left image is covered by one of the trees' branches in the right image

1.3 Image Forensic

After reading section (1.2), one can understand the need for authenticating images that might have been modified in some way, which is the very thing the field of image forensics was created for.

Although there is no global technique for pointing out whether an image has been tampered with or not, there are plenty of methods to identify image tampering.

The most extensive research on doctoring detection has been carried out by studying the characteristics; i.e. deformations, if any, of an image to identify the doctoring. Studying techniques include Joint Photograph Expert Group (JPEG) compression, resampling, lens distortions, Gamma correction, and Additive noise. Every one of these techniques converts the statistic of an image in a particular behavior, consequently by extracting specific prominent feature can be identified [5]. Increasing number of tampering makes the use of statistical technique possible under the concept of digital forensic. So pre trained classifiers can supply an appropriate method for detecting forgeries. There are three types of classifiers which are clairvoyant classifier, semi-blind classifier and blind classifier.

- Clairvoyant classifier: in this type of classifier, the classifier informs of the type of manipulation and the type of strength as well, for example an original image is blurred and the size of blurred function is n pixels then it wants to make a distinction between both the images (original and modified image). Clearly, this

type of doctoring is unrealistic anyway, though it is helpful for realizing the behavior of image doctoring.

- Semi-blind classifier: in this type, the classifier only informs about the type of manipulation, but not its strength. For instance, an image is blurred so it determines the blurred which occurred after capturing whatever is the blurred size.

- Blind classifier: actually, this is the most realistic one, it is as an image downloaded from the internet, here we have no knowledge about the type of manipulation and its strength.

1.4 Thesis Structure

This thesis consists of five chapters including the current chapter. Chapter 2, is the "literature review", which discusses the forensics' studies techniques with availability of watermarking technique. Moreover, the forensics' studies in absence of watermarking technique and these studies consist of two types, image forgery detection techniques studies and source digital camera detection techniques studies.

Chapter 3 explains the singular value decomposition (SVD) and fisher discriminant analysis. Besides, this chapter also includes the proposed method that is implemented on image by using SVD based features.

Chapter 4 contains the results that are extracted from whole images after applying our proposed method and discussing these results. Moreover, chapter 4 also contains the results that are extracted after making cropping on the images. Finally, the comparison between the results before and after the cropping images is applied.

Chapter 5 includes the thesis conclusion and the potential area of future works.

CHAPTER 2

RELATED WORKS

Image forensics research in recent decades has turned into an emerging field because of the advanced image editing tools. So, the need for methods for investigating images and checking the authenticity of the same are quite important as stated in (1.3). Below several techniques used for checking the validation of images are given in sufficient detail.

2.1 Watermarking

Not long ago, watermarking schema is used to verify the genuine image from the fake one. The watermarking may be based on date, time, camera information or picture information, etc.

Watermarking is an emerging technology which essential goal is to conceal some information into the digital media to prevent the copyright property or to verify the authentication of content. The primary demand of watermarking is to be resistant to the offensive targeting to smash the watermarking or the protocol of watermarking [39].

The challenge with the watermarking schema depends on the watermarking embedded at the time of the formation multimedia. However, several digital devices (Cameras and Video records) in the market did not have the abilities to add watermark during image creation. Furthermore, the majority of images on the internet have not been watermarked.
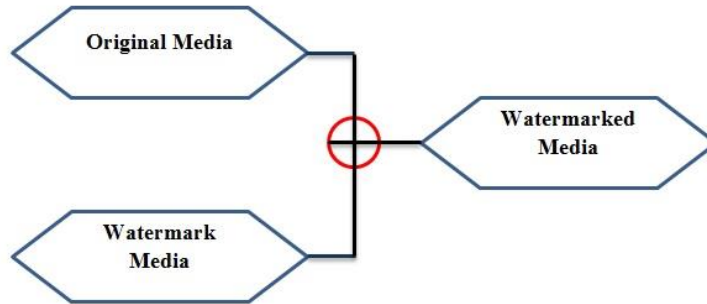
Figure 5 Watermarking schema

In the absence of watermarking techniques to authenticate the validation of images, there are other forensics ways to check whether the images are genuine or not. In fact, there are two basic essential methods which are forgery detection techniques and source identification techniques that is.

Forgery detection concentrates on to figure out the fingerprints of tampering by assessing the genuineness of the digital media (audio clips, video clips, images, etc.), while the source identification concentrates on knowing the source of digital devices (cameras, mobile phones, camcorders, etc.) using the media produced by them.
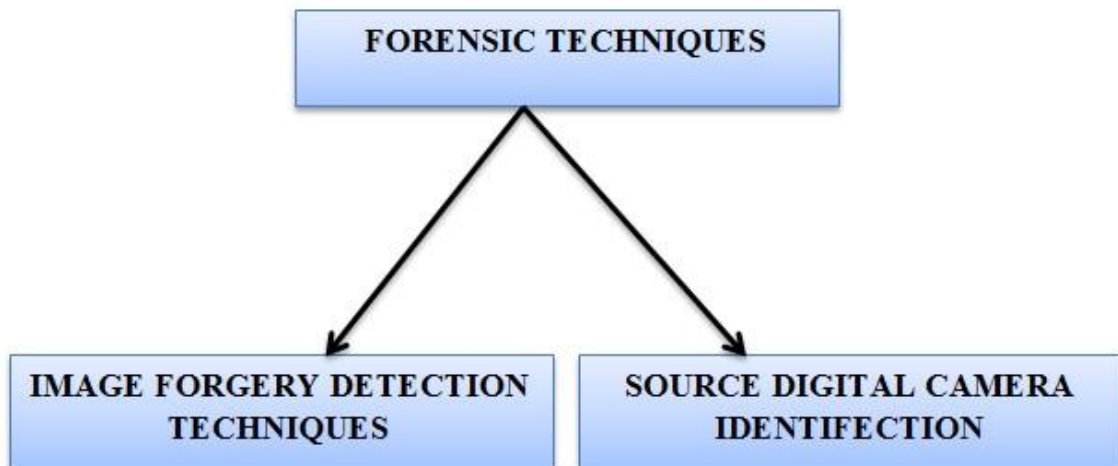
Figure 6 Methods of forensic techniques

2.2 Image Forgery Detection Techniques

There are several types of forgery detection techniques and those are explained below.

2.2.1 Using Joint Photograph Expert Group compression

Joint Photographic Expert Group (JPEG) compression is generally used in digital cameras to make encoding for the images. The manufacturers typically made their devices with various compression levels and parameters. The detecting of double JPEG compression has a major importance in digital forensics. The reason of that firstly is; it is very beneficial to recapture the history of processing. Secondly, during the tampering on the images, the double compressed images are frequently produced as well. In singular image segment, by revealing the trails of recompression, it could be exploited to reveal and identify the non-genuine part of the image, thus the genuine part of image will display trails of double compression [8].

Double JPEG compression means that a JPEG image has been compressed once more by JPEG compression. At least there are two motives noticed in the detection of double JPEG compression. [7], [8]. The doubly compressed JPEG images often result due to image forgery. An example of such is the image-splicing, which creates a new composite image when a part of source image is cloned to the goal image. Thus, if the source image or target image is in JPEG format, the spliced image may necessarily be JPEG compressed, hence exhibiting trail of double JPEG compressed. This trail could be used to uncover the tampered image or even identify the tampered area [9], [10].

Another reason behind the detection of double JPEG compression has a major importance which is, if the input cover image is in JPEG format, it may generate doubly compressed images in some JPEG steganographic schemas, for example F5[11]. and out – Guess [12]. Detection of double JPEG compression can assist to identify the steganographic algorithm or enhance the accuracy rate of detection of the steganalytic schemes.

Farid [13]. has used a variety in compression to know whether the images are modified or not. He takes advantage of knowing digital cameras database and comparing it against

JPEG quantization table from an image after extracting for the source identification. Furthermore, it can also be matched against photo editing software database for any hint of tampering. The number of digital cameras that are used for experiments by Tran Van Lanh et al. [37]. are 204 and out of those 62 cameras had individual quantization table whereas the other tables are in equivalence classes ranging between 2 to 8 in size. By using more than one version of Adobe Photoshop to be exact, five different types, an uncompressed image is saved after each of the 13 compression levels as a separate version. As for those of the 204 cameras, the JPEG quantization tables used were different and it was found that for any particular photo editing software the unique existence of JPEG quantization tables can be detected. It can be seen whether the image was already modified by using photo editing software or not.

Popescu et al. [14]. refers to the overwhelming of images format that are taken by cameras which already have JPEG format and any tampering on them by using software editing will cause double JPEG compression issue to exist.

Battiato et al. [15]. propose a novel way that has ability to recapture the coefficients of the first compression in a double compressed JPEG image under several presumptions. Their method exploited how consecutive sequential quantization followed by dequantizations entering some regularities (e.g., sequence value of zero and non-zero) by analyzing coefficient distributions histograms; this could detect the genuine compression parameters.

Huang et al. [16]. proposed an algorithm to reveal double JPEG compression with the same quantization matrix. The algorithm is depended on the monitoring of the process of recompressing a JPEG image with same quantization matrix repeatedly (over and over again), the number of various JPEG coefficients i.e., the Quantization Discrete Cosine Transform Coefficient (QDCTC) between the two sequential versions would be monotonically drawn out. For instance, the number of different JPEG coefficient between the singly and doubly compressed images are mostly larger than the number of different JPEG coefficients between the corresponding doubly and triply compressed images.

Through a novel random perturbations strategy carried out on the JPEG coefficient of the recompressed test images, Huang et al. [16]. could find a "proper" randomly anxious

ratio. For dissimilar images this global "proper" ratio will generate a dynamically changed threshold, which can be noticed to distinguish the singly compressed image and doubly compressed image. Furthermore their method has possibility to detect triple JPEG compression, four times JPEG compression, etc.

2.2.2 Using Chromatic Aberration

The lack in optical imaging systems causes various types of aberrations into the captured images. The causes of chromatic aberration are due to the lack in the lens to perfectly focus light dissimilar wavelengths in a digital camera, which excite an inconsistency in the location whereby the sensor receives light of various wavelengths.

Longitudinal and lateral are two types of Chromatic aberration. Longitudinal aberration causes the dissimilar wavelengths to focus at various distances from the lens, whereas lateral aberration is attributed to different wavelengths concentrating at different places on the sensor. Any tampering operation applied on image leads to the aberration across the image conflict, this detects the presence of existence forgery according to Gajanan K. Birajdar et al. [17].

Johnson et al. [18]. as an indication of tampering in an image, checked for the inconsistency of side chromatic aberration. Their model side chromatic aberration is the extension or the contraction of a color channel with respect one to another, which causes a misalignment of the color channel. The researchers discussed how to quantify the alignment model parameters to get the color channels back into alignment and metric based on reciprocal information. By calculating the average angular error between the displacement vectors at each pixel, the error between the local and global model parameters is quantified. If the average angular error overrides an exact threshold, it is probable that aberration has been inconsistent across the image because of tampering.

The average angular error is 14.8° with around 98.0% of the errors below 60°. This is discovered from the experiment done by Tran et al. [37]. For the aim of forensics, the image is examined in blocks and if the block's local estimation varies from the global estimation by more than 60°, it is considered to be conflicted with the global estimation and points out signs of modification. One visible challenge pointing here is that, it is

hard to assess chromatic aberration from a block with little bit or no spatial frequency content which is like a hugely constant patch of sky. Therefore, it is out of the way to detect it by an algorithm if the modified areas of the image consist of content with small spatial frequency (e.g. hiding of features in the sky).

2.2.3 Using Lighting

One of the trails which cannot be taken away from image forgery is inconsistency in light. Digital image forgery usually splices the background or goal of diverse images. Though the image editing software can facilely create or isolate the shadow or light, it is very hard to conceal the direction of illumination and the light source direction of different objects and background in an image which can be calculated. Therefore, conflicts in the light source direction can be as a robust clue to expose the image forgery. Johnson et al. [19]. proposed a method to reveal inconsistencies in the direction of illuminating light source in an image for any person or object by using 2-D model, which is based on the work by Nillius et al.[20]. The three contrastive situations which are infinite, local and multiple light sources tested to decide the error in the estimated light source direction related to the existing direction. In case the evaluated light direction with unsteady reflectance yielded an error of 10.9°, the errors are typically less than 2° except for the infinite light source.

On sample image test, the algorithm is effective in detecting contradicting light source directions. When the only resource for the lighting is the Sun (for outdoor scenes) this method should work well, while for indoor scenes with more than one resource for the analysis, it might not be easy because of multiple occluding limits.

To find whether the images are authenticated by detecting inconsistency in light source direction, a blind identification was proposed by Yingda Lv et al. [21]. to compute the light source direction for infinite and local light source images. The search means and least-squares methods are used respectively. This is done in accordance with the error function between the real intensity and studied intensity, as well as the restriction function proper for different light source models, and also to determine whether the image has been modified or not, by analyzing whether the light source direction between

varied objects and background in one image are harmonious. The result from their experiments showed that the right direction rates of the blind identification for infinite and local light source images which were 85.47% and 87.31% respectively. These results showed that the proposed method is an efficacious way to compute the light source direction for images. But there are still some errors in test outcomes and the reason of that is firstly, the influence of the shadow image which may make the error happen when measuring the surface normal of pixels of image and the second one is the reflection of surface as it is not in line with the prevalent reflection conditions of Lambert illumination model.

Figure 7 The left image is the outdoor scene where the sun is the only resource for lighting, whereas the right image is the indoor scene and has multi resources for lighting.

2.2.4 Using Camera Response Function

Camera Response Function (CRF) is another method for detecting forgery image. Hsu et al [22],[23]. proposed a method of revealing image splicing, using geometry invariants and CRF. The authors' ideas are comparable to the work by Lin et al. [24]. that reveals splicing by watching abnormality in the camera's response function CRF. The suspicious splicing boundary is manually identified at the beginning. The geometry invariants from the pixels in every area on either side of this boundary are measured and used to estimate the CRF. The CRFs from every area are then tested for uniformity with

each other using cross-fitting technique. The image is likely to be genuine if the data from one area fits well to the CRF from another area, otherwise it is spliced. Finally, the cross-fitting error from every area is represented using a 6-diminsional vector and is fed into a RBF Support Vector Machine (SVM) classifier to classify it into genuine or not. Only one image in RAW or BMP format is examined and each spliced image is formed in Adobe Photoshop using authentic images from 2 cameras with no post-processing to focus on the effect of splicing. In 6 runs, the accuracy of classification is 87.55% with the spliced image detection rate as high as 90.74%. However, the False Acceptance Rate (FAR) is also the least i.e. 15.58%. Here, only uncompressed images are examined although the accuracy is rationally high. Whether would this technique work well with JPEG compressing images that stays unknown? Furthermore; spliced image which is created from a genuine one and taken by the same camera or even the same model is improbable to be detected as forgery.

2.2.5 Using Bicoherence and Higher Order Statistics

Based on Farid's [25]. earliest success in applying bicoherence features for revealing human-speech splicing, Ng et al. [26],[27]. researched on the probability using bicoherence feature to reveal the presence of unexpected discontinuities in an image or the absence of optical low-pass property as a clue of splicing. In addition to the use of the original features that describe the mean of magnitude and phase entropy, the researchers proposed two different ways to increase the performance, one estimating the bicoherence features of the genuine counterpart, and the second, incorporating image features that capture the characteristics of different object interface.

By using Support Vector Machine (SVM) classification, 71.48% is the mean accuracy that was obtained. Although the primary results look good and promising, but the accuracy is not high enough, and more effective features must be derived to model sensitivity of bicoherence because of splicing.

2.2.6 Using Robust Matching

Fridirich et al [28]. concentrated on the detection of a particular type of some specific kind of tampering, the copy-move attack, where a part of an image is copied or duplicated in another area of the same image, usually used for hiding an important feature which is similar to the approached used by Popescu et al. [29]. For uncompressed images, identification is done between blocks of size B×B to detect for exact replicas. To extend this method in order to save image lossy JPEG format, the authors used a robust representation consisting of quantized Discrete Cosine Transform (DCT) coefficients, instead of matching the pixel representation of every B×B block.

The good outcomes of experiment on sample modified image have been produced, with the copied-and pasted regain successfully matched and identified. However, the algorithm might have falsely identified matching segments in plane, uniform field, for instance the ocean, and the authors also have knowledge about that. So interpretation of human is needed to interpret the algorithm output.

2.2.7 Feature Extracted

While Zhen Zhang et al. [30]. were running image splicing revealed a blind passive and effective splicing reveal planner which was proposed. The method concentrated on moment features extracted from Multi-size Block Discrete Cosine Transform (MBDCT) and some Image Quality Metrics (IQM) extracted from the given tested image, which are critical to spliced image when comparing between real image and spliced image. The statistical difference can be computed by the above model. The experimental outcomes showed that this new splicing detection algorithm is active and trustworthy; explaining that this proposed way has a wide implementing possibility.

Researchers proposed a new algorithm to classify spliced images from authentic images. The authenticated images having statistical features are dissimilar from unauthenticated ones. To form the model of features extraction, researchers describe those dissimilarity using moment features and several quality images. In comparison with the other technique, this novel method is unsophisticated in form and has large value detection. In

their work what they have done and what other researchers have not done are, firstly introducing image quality metrics into blind detection of image splicing. Secondly, to extract the image features by conjoining moment features with image quality.

2.2.8 Using Approximate Run Length

Zhongwei et al. [32]. a novel approach is proposed with an approximate run length based schema to reveal image splicing which can gain high precision with fewer features. At first, they measure the edge gradient matrix of an image, and compute approximate run length along the edge gradient direction, and then from the histogram of the approximate, they run several length features which are constructed. The approximate run length is applied on the predict-error image and rebuilt images based on Discrete Wavelet transform (DWT) to gain more features. Eventually, SVM is used to classify the genuine and spliced image using the features that have been built. The proposed method can realize a comparatively high precision with less cost of computational yet fewer features when matched with others.
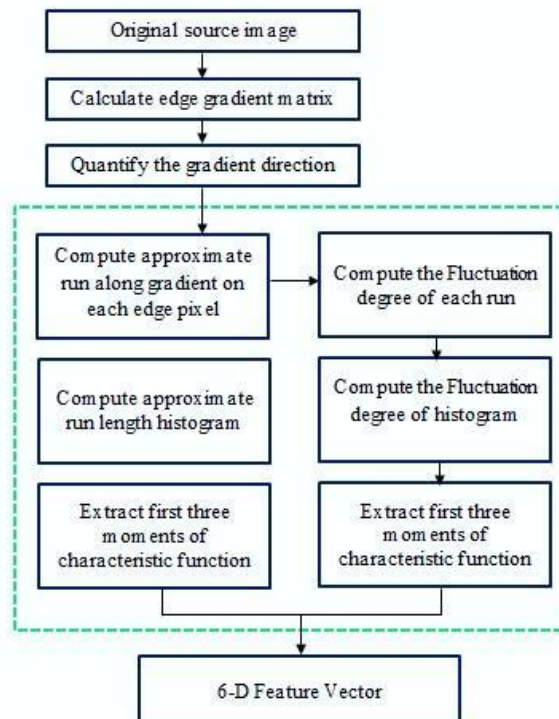
Figure 8 Develop an improved method based on approximate run length [32].

To a certain degree for splicing detection on big-scale analysis and real application, the original run length based technique is proper, furthermore; it is easy and quick. But the precision of this detection technique is not large enough. So, by making several changes on this technique as it is done by Zhongwei et al. [32]. The technique developed this modification firstly, rather of measuring all the run length of an image; just measuring of the run lengths on the edge pixel is done. The reason behind that the splicing process is fully uninfluenced on the run lengths in general. Because of splicing normally inserts additional edges to the image, contrariwise calculating run lengths on the edge pixel is better. Secondly, instead of calculating run length along, four particular linear directions (i.e. 0, 45, 90 and 135) which are only every edge pixel the researchers calculated run length along the respective gradient orientation. Measuring run lengths along particular linear directions is unnecessary for an unsophisticated example of spliced image. Finally, calculating run length in a various sense instead of calculating the rigorous run length, which needs all the pixels in a "run" have precisely the same value of gray-scale. Despite the proposed method being easy and effectual, its detection performance is as yet slightly less than satisfactory. After deep scanning they found that the image with complicated texture is most probable to be misclassified and they accounted it for 80% of the fiasco case. Due to twofold, complex texture majorly intimidate the precision of the edge detection on an image, which is really important to the proposed method. Another one is the change of gray-scale values of successive pixels which are going to be resorted more dramatically in an image with composite texture, thus it makes the real images and the spliced one less distinguishable and of course the researchers are aware of that.

2.2.9 Two-D Noncausal Markov Model

One of the most vigorous tools that have proven for image-tampering detection and image steganalysis is the Markov model. Almost all the image forgery detecting approaches built on the Markov models in Block Discrete Cosine Transformation Domain (BDCT) or (DWT)) deal with image as a 1-D causal signal. Hence, the classical models just describe the state dependencies between close states along specific

directions (e.g., horizontal, vertical). To gather more information into consideration, a 2-D noncausal Markov model is proposed by Xudong Zhao et al. [31]. It is a good model, the 2-d image as every state in the proposed model depends on its circling state together. As a result, there is no direct analytic solution for this model.

They decompose the non-causal model into four 2-d casual sub-models and resolve these sub-models successively. For every casual sub-model, the existing state depends on its closest state in the 2-D sense (2-D dependency or Markovian property for 2-D). The previous probabilities of every state describe the causal sub-models, which are the state transition probability matrix and the parameters of likelihood density function of every state. All these model parameters are examined as special features for rating. They applied their model in the BDCT domain and Discrete Meyer Wavelet Transform domain (DMWT), and the model showed its popularization and efficiency in the two different domains. The experimental outcomes display that the proposed nun-causal Markov model, outperforms some state-of-the art methods through two published image-splicing detection valuation data sets.

From two parts, their detection technique consists of feature extraction and classification. From the source matrix they extract the 2-D noncausal Markov model-based features, after that, to determine whether the image has been spliced or not, these extracted features that are fed into the support vector machine (SVM).

2.2.10 Exposing Photo Manipulation with Inconsistent Perspective Geometry

ZHOU Ya-jian et al. [33]. proposed a geometric-based forensic method which takes advantage of demise points. Intersection points of the projected parallel lines are calculated through edge detection and straight lines extraction. The Normalized Mean Value (NMV) and Normalized Standard Deviation (NSD) of this area between crossroad points are used as a clue for image forensics. The proposed method appoints basic rules of linear perspective projection, and makes lower presumption.

The algorithm is run with York Urban database [34]. (102 indoor outdoor images) in order to ensure the efficiency of the proposed technique. The only request is the parallel lines must be contained in the image. Unlike other forensic methods which are based on

low-level statistics. This technique is less sensitive to image operations that do not change image content, like image resampling, color manipulation and lossy compression. It is explained with image from York Urban database. It displays the properties or specialty that the proposed method has a definite advantage at separating authenticated and false images.

Straight line extraction is the critical step of this method. The challenge of this method is the image that may not include straight lines, in other words, the image containing the curved lines which are taken in authors' considerations in a future work.

2.3 Source Digital Camera Identification

Several methods of source digital camera identification are explained below.

2.3.1 Using Lens Aberration

As a fingerprint to distinguish source camera Choi et al.[35]. proposed lens radial distortion. In this case on the output image, straight lines look as curved lines because of radial distortion and it happened when the transverse magnification M_T (the image distance ratio to the object distance) is not steady while a function of the off-axis image distance r. Various manufacturers use diverse lens system design to compensate for radial distortion and thus the degree of radial distortion is affected by the lens focal length. Thus, every device model goes over a unique radial distortion pattern that aids to identify it and this is what the Choi et al.[35]. argue on or about. On three various camera models two experiments performed by Gul et al. [37] gaining medium classification precision of 91.53% and 91.39 respectively. Though this technique is checked for two devices of the same model and depended on researchers' arguments on radial distortion could anticipate precision which is not high. Moreover, if there is no rectum lines in the image this technique will fail to compute radial distortion, since the distortion is computed using the rectum line. Finally, the center of the image is the center of distortion that is supposed by the authors, however, that may not be the issue. A large precision may be a good potential, if this is taken into account.

2.3.2 Using Color Filter Array Interpolation (CFA)

As we know, any manufacturer has its own proprietary with regard to the cameras pipeline and the abundance of its details which are considered manufacturers' proprietary information. However, there are some similarity to a large extent between all digital cameras form, the side of general sequence and the substructure of stage in the camera pipeline. The Figure 9 shows the essential structure of digital camera pipeline.
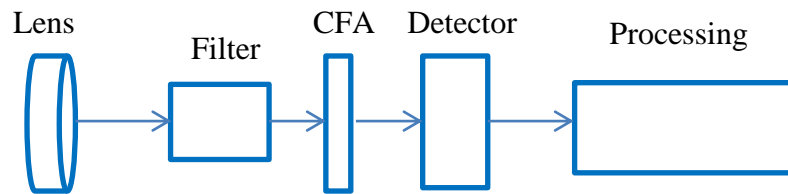
Figure: 9 The more important stage of digital camera pipeline [36]

From the lens, the light enters the camera then it passes through filters, the anti-aliasing filter is considered the most important one. The antialiasing filter is needful when the distance between the elements (pixels) of the Charge-Coupled Device (CCD) array is smaller than the spatial frequency of the scene [36].

In the digital camera, the main component is the CCD array and also it is the most costly component. Every light sensing element of CCD array combines the indicated light over all spectra and gets an electric signal representation of the scene. Because each CCD element is basically monochromatic, for every color component, separate CDD array is required when capturing color images. However, because the cost is taken into account, instead of using multiple arrays, the CCD is ordered in a pattern by using various spectral filters Red, Green and Blue (RGB). In front of the sensor there is a mask called color filter array (CFA) [36].

R	G	G	R	B
R	B	B	R	B
B	R	R	B	G
B	G	B	R	G
G	R	G	B	G

Y	C	M	M	Y
M	C	C	M	Y
Y	M	Y	C	C
C	Y	Y	M	M
Y	M	M	C	Y

Figure 10 From the left hand CFA pattern is using RGB values while on the right hand CFA pattern is using YMCA values

İn simple words, CFA contains three channels or layers, Red, Green and Blue, when displayed simultaneously, we can sense these colors for every pixel location in the image as there is a unique set of Red, Green and Blue values [42].

Color Filter Array Sensor
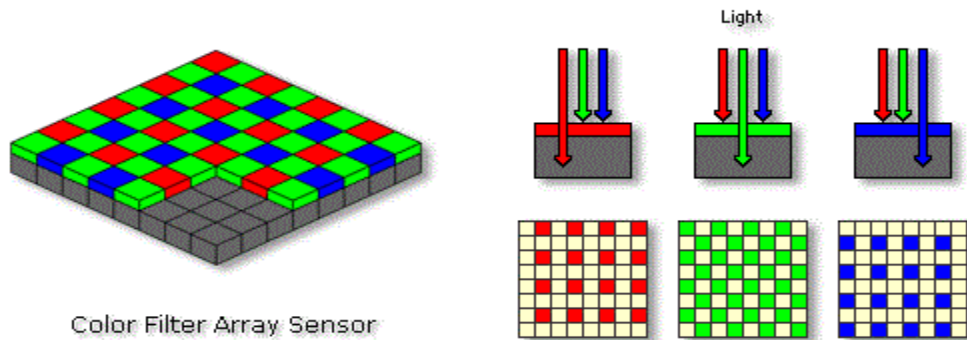
Figure 11 Mosaic sensors with a GRGB CFA capture only 25% of the red and blue and just 50% of the green components of light [43].

The tracing of color interpolation in color bands, is meant to determine the correlation structure present in every color band which can be exploited for image classification, Bayram et al. [36] searched the Color Filter Array (CFA) interpolation process. The algorithm of interpolation and the design of the CFA filter pattern of every manufacture slightly varied from others that are the major presumption which leads to distinguishable correlation structures in the images that are captured. Using the refined Expectation Maximization (EM) algorithm, the interpolation coefficients from the image and the

peak location and magnitudes in the frequency spectrum of the probability maps are gained for classification.

The classification precision is 83.33% when comparison is made among three cameras However, this precision comes to be high more specifically when two different cameras are used, it becomes 95.71% using 5×5 interpolation kernel. The issue in this method is the determining of the effect on the classification precision and a large number of set of cameras need to be used. There is no any experiment carried out for cameras that belong to the same model. For compressed image, this method probably will not work, as pointed out by researchers. Tran Van Lanh et al. [37]. expected failure in this method due to the using of devices which is exactly the same model usually sharing the exact same CFA filter and interpolation algorithm.

2.3.3 Using Image Features

A set of image features is identified by Kharrazi et al. [38]. that can be exploited to the uniquely classified camera model. The 34 suggested features are labeled into three sets; Color features, Image Quality Metrics and Wavelet Domain Statistic. Images that are captured from two cameras, then these features are extracted then used to work out and examine the classifier. For uncompressed images the outcome is as high as about 98.73% and for JPEG images compressed down are about 93.43% with quality factor of 75%. When using five cameras, the precision rate is come down to about 88%.

2.4 Conclusion

After all the above observations, it is obviously the techniques of forgery detection which have lower rates if they are matched with camera identification techniques, of course in the absence of watermarking technique in the digital device. However, if the digital devices have watermarking technique which absolutely gives great results and then it is more preferable in forensic field to authenticate the images.

CHAPTER 3

PROPOSED METHOD

Image and image manipulation is subjected to a paradigm shift naturally with coming and developing of digital technology. To the algebraic matrix, an image is converted through numbers of the image pixels' values which are then well represented.

3.1 Singular Value Decomposition (SVD)

The process of SVD has several fascinating mathematical properties. The essential algebraic image properties are represented by SVD.

To extract algebraic and geometric features from an image, SVD is a matrix factorization and gives a novel way to the image. Actually, in several fields SVD is used like a pattern analysis in a single processing and data compression.

In this thesis, the proposed way to detect tampering image is done by SVD which is a very advantageous tool in linear algebra. It decomposes a matrix into $A \in IR^{M \times N}$ to the orthonormal matrices $U \in IR^{M \times M}$, $V \in IR^{M \times N}$ whereas $S \in IR^{M \times N}$ is the diagonal matrix, and the matrix A can be represented as follows:

$$A = USV^T \tag{3.1}$$

The diagonal matrix S is the descending array, the elements are positive and are in descended arrangement

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 \ldots \ldots \geq \sigma_{\min(M,N)} \tag{3.2}$$

Where M and N are the dimensional of matrix A and from these elements in the diagonal matrix S we get a vector called singular value vector.

$$Sv = Diag(S) \tag{3.3}$$

In terms of liner dependency the soft relationship between image rows/columns pointed out to the singular value of matrix, the singular value resorts to be zero if the image rows/columns resort to become linearly Gokhan et al. [40]. Two rows/columns of a matrix are called linearly dependent when defined as $c_2 = K \cdot c_1$ where k is an integer. According to the defined relative linear dependency, the closeness of K to an integer is between the two rows/columns.

A good model of relative linear dependency of image rows/columns is precise enough to detect the image tampering. Certain types of linear dependencies introduced in images (original images) so that any tampering on images would be destroyed of these dependencies. Spatial domain represents a robust dependency between pixels in local neighborhoods; the features for this are extracted from sub-blocks representing locality in the spatial domain rather than the entire image. The entire image on the other hand does not supply rich statistics and does not represent local dependency at all.

To represent the entire image, the extracted features from sub-blocks image merged with one another to represent the whole image. Firstly, this image is divided into sub-blocks of the size of $w \times w$ (w=3,4...,20). It is clear that when sub-block size (w) is large, then the number of estimated blocks is less and consequently gets the less inter-block dependencies which are taken into account respectively [40]. Overlapping blocks are proportional to the block size which is able to take into account the connections both within and among the image blocks that are taken in order to handle and lessen the problem of the less inter-block dependencies.

The sub-blocks image are overlapped according to the following schema:

- If $3 \leq w \leq 9$ non overlapping
- If $10 \leq w \leq 15$ 50% overlapping
- If $16 \leq w \leq 20$ 75% overlapping

From this sub-block scheme, three various types of features are derived, each feature is for steady sub-block size and various steady index of singular values. In the following, B is the integer number $w \times w$ according to sub-block size w. First type of singular value decomposition (SVD) based features are defined as follows:

- Type one features are the means of the number of zeros at index i in Sv vectors of sub-block.

$$f_{sv}^1(w,i) = \frac{1}{B}\sum_B \delta\big(Sv(i)\big), i = 2,3 \ldots w, w = 3,4, \ldots .20 \qquad (3.4)$$

Where $\delta(k)$ indicates the unit impulse function $i = 1$ is out of consideration since it is non-zero if and only if all elements of A are zero.

Where $\delta(k) = \begin{cases} 1, & k = 0 \\ 0, & k \neq 0 \end{cases}$

- Type two features are the means of whole sub-block that contain singular values, the mean of Sv vectors of sub-block size $w \times w$

$$f_{sv}^2(w) = \frac{1}{B}\sum_B mean(Sv), \ w = 3,4, \ldots ..20 \qquad (3.5)$$

- Type three features are the mean of odd address in Sv vector plus the mean of even address in same Sv vector.

$$f_{sv}^3(w) = \frac{1}{B}\sum_B(P(Sv) + E(Sv)), \quad w = 3,4, \ldots ..20 \qquad (3.6)$$

Where $P(Sv)$ is indicated to the mean of odd locations in Sv vector while $E(Sv)$ indicates the mean of even locations.

3.2 Fisher Linear Discriminant (FLD)

The reduction of dimensionality in Principal Component Analysis (PCA) is performed with no supervision. Through the dominant eigenvectors of the covariance matrix on the subspace, feature vectors are projected on the subspace. In order to calculate the subspace and lessen the dimensionality, taking location in supervised style must be done. The decreasing of dimensionality in PCA, is carried out with no supervision. Through the dominant eigenvectors of the covariance (autocorrelation) matrix, feature vectors are projected on the subspace spanned. In this section, computation of the subspace to reduce dimensionality happens with supervision. Through the solution of an eigendecomposition problem, this subspace is determined as well, although, the corresponding matrix is not similar [41].

The goal in two-classes is to find a one direction, w, thus Fisher's discriminant ratio is maximize by the respective projections y of the l-dimensional feature vectors $x \in Rl$. a scalar feature y in a 2-class classification task for Fisher's discriminant ratio is known as:

$$FDR = \frac{(\mu_1 - \mu_2)^2}{\sigma_1^2 + \sigma_2^2} \tag{3.7}$$

The mean value of y represented in μ_1 and μ_2 , in fact, the essential objective for the mean values in the two classes for data points is quite far apart as possible as can be where the variances of y $\sigma_1^2 and$ σ_2^2 in the two classes is quite small as well. Via the maximum eigenvector of the matrix $S_w^{-1} S_b$, it is obvious that w is given for two equiprobable classes

$$S_w = \frac{1}{2} (S_1 + S_2) \tag{3.8}$$

S_w is defined as the within-class scatter matrix, while S_1, S_2 being the respective covariance matrices

$$S_b = \frac{1}{2} (m_1 - m_0)(m_1 - m_0)^T + \frac{1}{2} (m_2 - m_0)(m_2 - m_0)^T \tag{3.9}$$

25

S_b is defined as the between-class scatter matrix. Where m_0 represents the comprehensive means of the data x in the original R^1 space and the mean values of two classes are m_1, m_2 respectively

$$m_0 = \frac{m_1 + m_2}{2} \tag{3.10}$$

In the situation where eigenanalysis step in this special two-classes can be bypassed then solving is immediately given by

$$w = S_w^{-1}(m_1 - m_2) \tag{3.11}$$

The purpose is to discover the $m \leq c - 1$ directions in the c class, thus that the so-called J_3 criterion is maximized and is known as

$$J_3 = trace\{S_w^{-1} S_b\} \tag{3.12}$$

In the preceding equation

$$S_w = \sum_{i=1}^{c} P_i S_i , \quad S_b = \sum_{i=1}^{c} P_i (m_i - m_0)(m_i - m_0)^T \tag{3.13}$$

And the P_i's indicates the respective class prior probabilities. In the multiclass this is the generalization of the FRD criterion in the situation with variation in prior probabilities. The directions of m are given by the m dominant eigenvectors of the matrix product $S_w^{-1} S_b$

Here it must be realized that the rank of the S_b matrix is $c - 1$ mostly, though it is given as a sum of c matrices, just $c - 1$ are independent in these terms. This is why m is upper bounded by $c - 1$; just $c - 1$ is the greatest eigenvalues which mostly are nonzero. This may be a challenge as the reason for this belongs to the maximum number of features, this process can generate which is bound by the classes numbers in some situations [41].

After all the above discussion, the main idea from FLD is to find out the suitable projection to a line samples from various classes which are well separated.
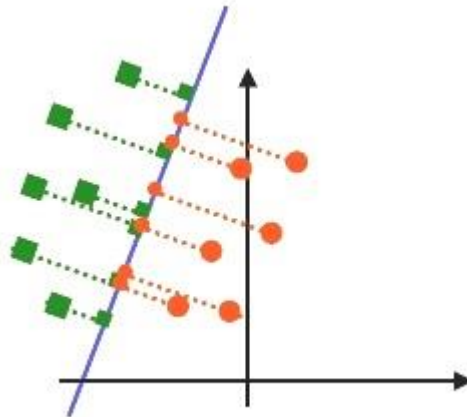
Figure 12 Bad line to project two classes are maximized up
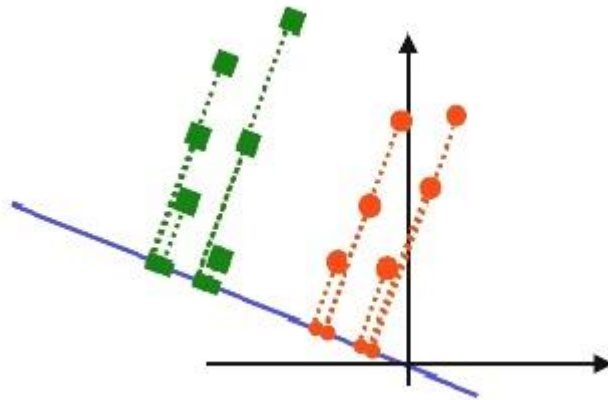
Figure 13 Good line to project two classes are well separated

Figure 14 Sample of an original image

3.3 Explaining the Process of the Proposed Method

The above image size 716×540 pixels, is one of image samples worked on. Below explained the process steps that are done on it and also we have shown the results obtained after applying the features equations on the above shown image.

The process steps that explain the proposed method are:

- Read image
- Divided image to the sub-Blocks
- Applying SVD function
- Take the diagonal matrix from each block
- Extract features
- Apply FLD
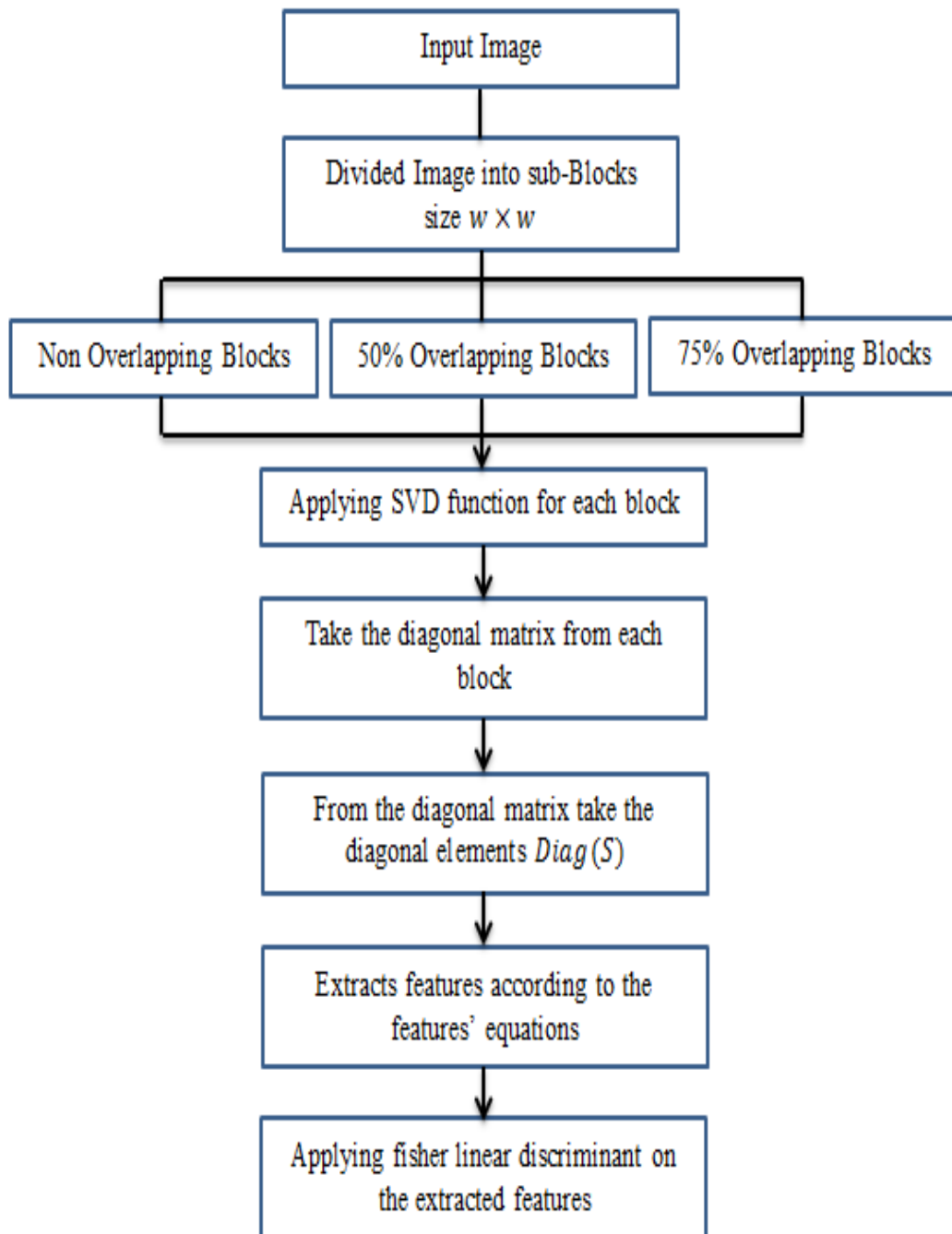
Figure 15 The processing of the proposed method
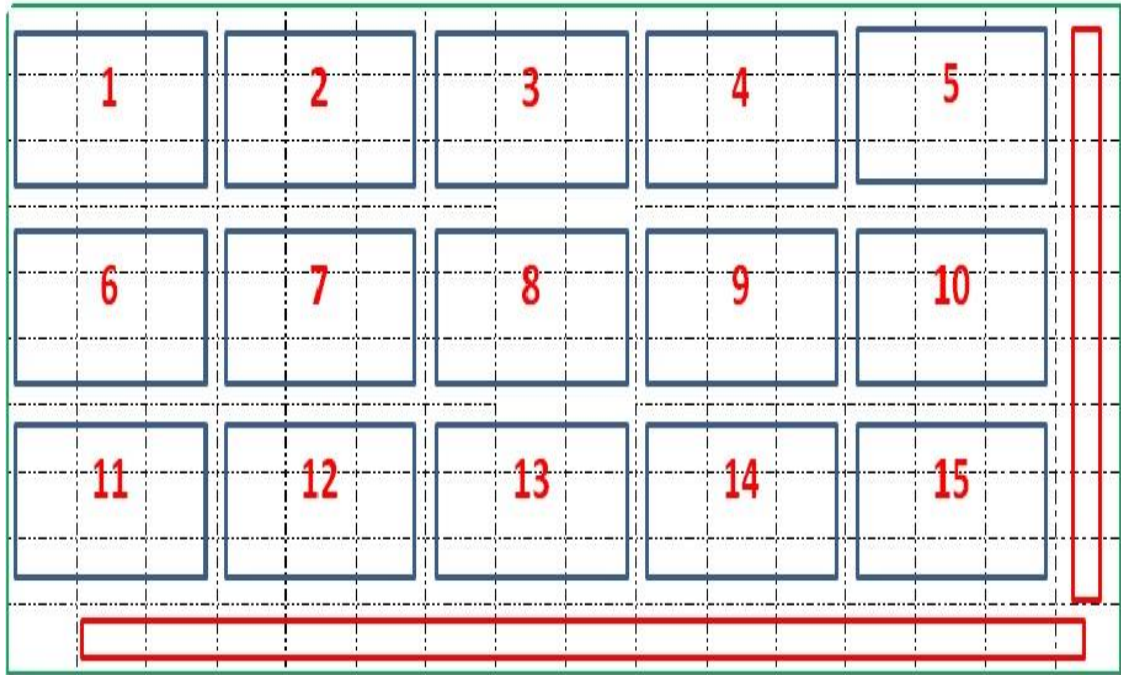
Figure 16 Non-overlapping blocks

When image is divided into non-overlapping blocks from the left top corner and then this process is continued through the image. On closing to the right image's side the size of block is greater than the remained image's pixels which ignore these pixels from our computations. Likewise, when closing the bottom side of the image, again the remained pixels are ignored, too.

The fact that the size of the blocks determines the number (for us) of the remaining pixels that will be ignored, maybe there is none remaining pixels left and the whole image's pixels undergoes our computations.

Let's suppose that one has an image size of 716×540 pixels which needs to be divided, it can be divided into the non-overlapping blocks according to the w strategy in the section (3.1)

When $w = 3 \rightarrow (716 \, DIV \, w) = 238$, by multiplying $(238 \times w) = 714$, the remaining pixels are 2 and these pixels are ignored from the right side of image. And in case from bottom side of image $(540 \, DIV \, w) = 180$, by multiplying $(180 \times w) = 540$, here there are no remained pixels to be ignored. The total blocks that are gained for the whole image are then 42840 blocks.

Moreover, when $w = 4 \rightarrow (716\ DIV\ w) = 179$, by multiplying $(238 \times w) = 716$, there are no remaining pixels to ignore from the right side of the image. Same as from the bottom side of image $(540\ DIV\ w) = 135$, by multiplying $(135 \times w) = 540$, there are no remaining pixels to be ignored. The total blocks gained from the whole image are 24165 blocks.

In fact, the person who wants to make a modification, in other words to make tampering on an image he/she will mostly make his/her modified on the great area to some extent, and in the middle area of the same image at the most.

64	64	62	57	51	48	51	54	54	54	50	44	45	52	57	57	55	62	62	52	43
64	63	60	55	51	49	50	51	49	49	45	40	40	46	50	50	46	54	58	51	45
64	60	56	53	51	50	48	47	44	46	43	38	38	43	45	43	41	50	55	52	48
63	58	53	51	51	50	47	44	44	46	45	41	40	43	43	41	43	51	56	53	48
62	57	53	51	51	50	46	42	43	46	45	41	41	43	43	40	44	52	56	52	48
59	57	54	52	51	48	45	43	41	44	43	39	39	42	43	40	42	49	53	50	48
58	58	57	54	50	47	45	45	41	43	42	38	38	43	44	42	42	48	50	48	47
56	58	59	56	50	46	45	46	43	44	43	39	39	45	47	46	45	50	51	47	46
53	56	55	49	44	45	47	48	42	38	35	39	46	49	45	40	45	48	47	42	42

Table 1 Part of Image's Blocks Values When $w = 3$

For each block shaded/non shaded blocks, applying SVD function and taking the diagonal elements from the diagonal matrix S

$$[U, S, V] = svd(image\ block) \tag{3.14}$$

Since the block dimensions are equal, (block matrix are quadrate) that leads to the number of elements in the Sv which equals to the block size (w), the reason behind that belongs to the $S \in IR^{M \times N}$ as mentioned previously in section (3.1).

185.8022	155.1835	149.5705	137.0649	139.6757	153.8621	156.1567
3.239748	3.012064	3.555087	0.417518	1.641138	2.217257	5.914669
0.212641	1.15E-15	0.174899	0.209691	0.01745	1.242849	0.323728
172.288	151.69	131.7669	130.1921	125.7371	134.6619	154.9281
2.592343	1.7716	1.54596	0.140794	1.03544	1.430301	1.731518
0.367195	9.31E-15	0.289632	4.78E-15	0.330278	0.35305	0.536791
170.0663	147.4086	134.1449	120.545	132.2915	135.6108	140.2596
2.121445	2.950074	1.681653	4.68099	4.994919	3.272307	1.762291
0.975647	1.007206	0.56298	0.028355	0.089288	1.00054	0.360064

Table 2 Singular Values Vector for Each Block

Then when applying the equations (3.4) to get the features from these singular value vectors i.e. from the equation (3.4) obtained, 7 features vectors for non-overlapping blocks, from the 50% overlapping blocks taken 6 features vectors and 5 features vectors from 75% overlapping blocks, so the total numbers of vectors that are at our disposal depended upon the w strategy which is 18 features vector, then the average of these features vectors is taken. From the equation (3.5) 18 features are taken directly, here it should be noted that there are no vectors from these equation, likewise in the equation (3.6) 18 features which are gained as well.
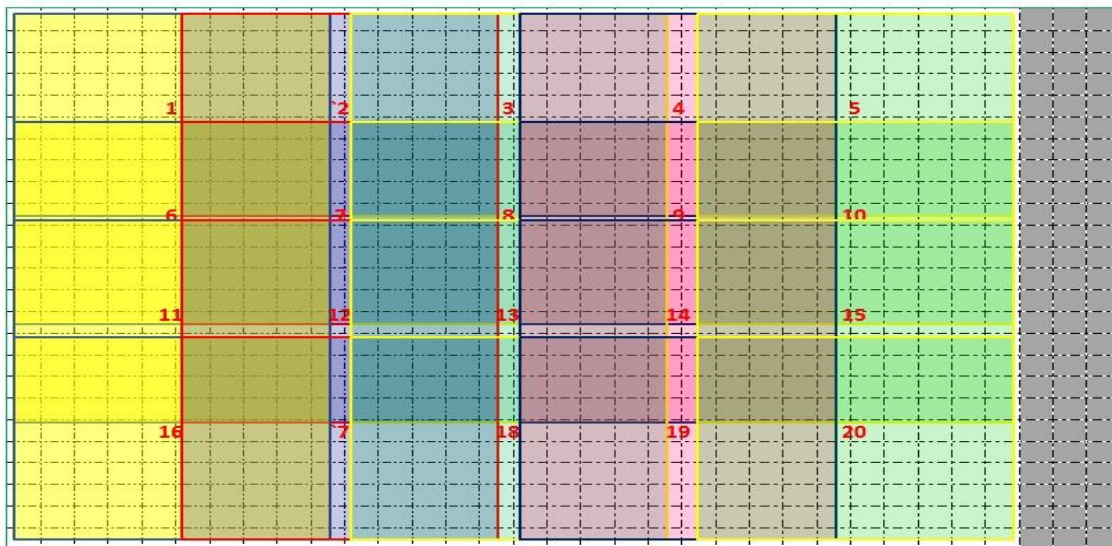
Figure 17 Overlapping blocks (50%)

In the Figure 14, the process of 50% overlapping blocks is shown and done on the image. Likewise, in non-overlapping blocks the same approach is used and applied regarding the remaining pixels.
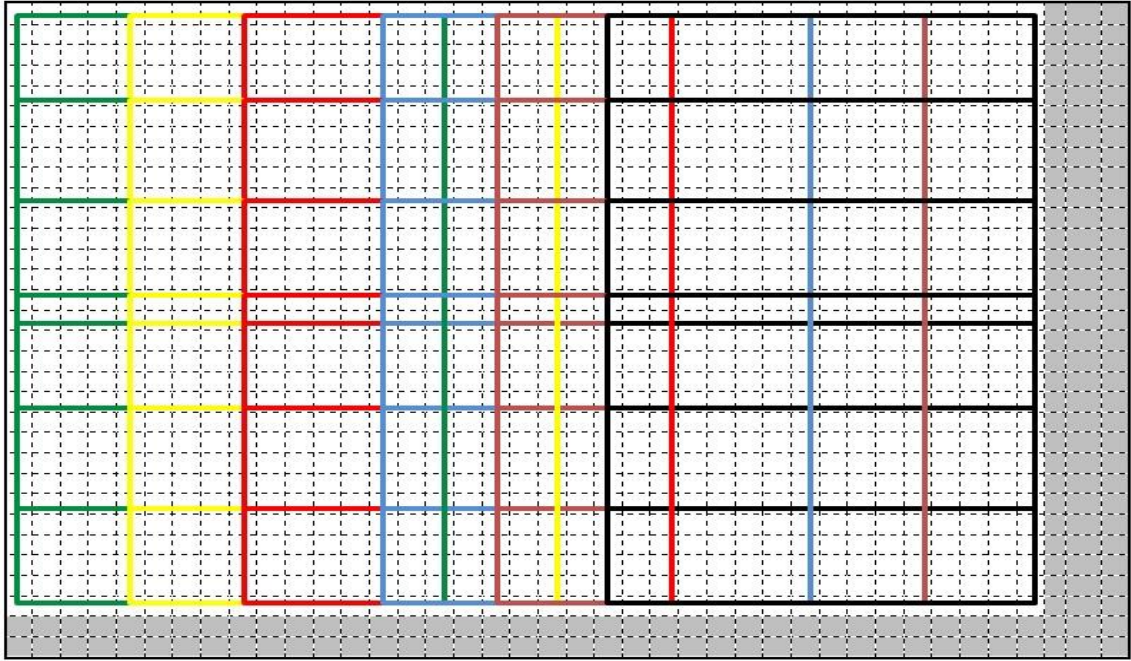
Figure 18 Overlapping blocks (75%)

Figure 15 shows us the 75% overlapping blocks regarding the remaining pixels and same strategy is used as mentioned before.

The same image is then divided into different blocks size according to w schema; the purpose behind that is to supply a rich statistics for the research.

18 features are the total number of features that are extracted from each equation according to w size.

The total numbers of features that are obtained from the image after applying all features equations are 48 features.

$w = 3, 4, ... 20$ respectively																	
0.015126	0.016539	0.004030	0.004444	0.001400	0.008888	0.000316	0.000343	0.000119	0.000155	6.42E-05	0.000140	7.44E-05	0.000109	4.09E-05	2.82E-05	2.42E-05	3.58E-05

Table 3 Average Features Extracted from Equation (3.4)

$w = 3, 4, ... 20$ respectively																	
111.4291	112.5512	114.5146	115.9803	117.6185	118.16	120.7404	122.1578	123.3749	125.0288	126.2342	127.9074	129.3126	130.4545	131.9853	133.2697	134.5337	135.9885

Table 4 Features Extracted From Equation (3.5)

$w = 3, 4, ... 20$ respectively																	
3655373	2731834	1504475	1248527	825680.3	710025.2	525995.8	1872350	1746155	1326040	1249559	993057.2	953780	3072732	2941014	3105588	3015351	2032384

Table 5 Features Extracted From Equation (3.6)

For these 48 features from this one image, same steps are applied onto other original images dataset that are furthermore, have the same process done on the modified images dataset. After extracting features from dataset for original and modified images, fisher LDA will be applied on them.

In tables 6 and 7, one can see the first most features that are obtained from the equation (3.4) for both datasets original and modified images respectively. And then the second features in the tables 8 and 9 that are obtained from equation (3.5) for both datasets,

original and modified images respectively. Tables 10 and 11, the third features that are also obtained from equation (3.6) for both datasets original and modified images respectively.

$w = 3, 4, \dots 20$ respectively				
Image 1	**Image 2**	**Image 3**	**Image 4**	**Image 5**
0.01512605	0.086889819	0.015076415	0.040521079	0.113102653
0.01653907	0.174577557	0.0150605	0.038633809	0.185994421
0.00403069	0.075255763	0.004083276	0.012012195	0.084887223
0.00444444	0.081904762	0.0047109784	0.012187135	0.098545623
0.00140056	0.051056786	0.0011449275	0.007220983	0.050584391
0.00888814	0.123811121	0.008400853	0.019434524	0.155555556
0.00031645	0.050474684	0.000889513	0.003731343	0.038156513
0.00034370	0.052571922	0.000746366	0.003062009	0.043396445
0.00011958	0.037870212	0.000356308	0.002088482	0.026178999
0.00015581	0.045757518	0.000583686	0.002095825	0.034357177
6.42013E-	0.027835968	0.000204162	0.00124282	0.018801965
0.00014029	0.030214054	0.000275233	0.001460446	0.022693099
7.44435E-	0.020499888	0.000189619	0.00102579	0.01210038
0.00010904	0.034971878	0.000318845	0.001155213	0.026707275
4.08942E-	0.014481642	8.13055E-05	0.000636915	0.005823181
2.8225E-05	0.020061115	0.000120196	0.00053302	0.011115204
2.42336E-	0.016573367	9.63837E-05	0.000395854	0.007920764
3.58038E-	0.017235947	6.97947E-05	0.0003719	0.01012582

Table 6 Features Extracted from Equation (3.4) for Original Images

w = 3, 4, ... 20 respectively				
Image 1	**Image 2**	**Image 3**	**Image 4**	**Image 5**
0.02538613	0.10314969	0.01730689	0.03889907	0.12582272
0.03013024	0.20129664	0.01948283	0.03709468	0.20221149
0.01034948	0.08517871	0.00508971	0.01096544	0.09099064
0.01178359	0.09303454	0.00507462	0.01160233	0.11716535
0.00440746	0.06126389	0.00207039	0.00618562	0.06738301
0.02232816	0.14606741	0.00933901	0.01726190	0.16665883
0.00219909	0.05350738	0.00081928	0.00337130	0.05219298
0.00180650	0.05727407	0.00069444	0.00263634	0.05510682
0.00100361	0.04098328	0.00046144	0.00155709	0.03474465
0.00154958	0.04937587	0.00056832	0.00187435	0.04460420
0.00042896	0.02836761	0.00022528	0.00096058	0.02359693
0.00090378	0.03259911	0.00015981	0.00096739	0.03052785
0.00024761	0.02133737	9.89315E-	0.00049261	0.01646090
0.00088985	0.03950011	0.00028313	0.00103558	0.03487659
0.00018538	0.01392744	7.17401E-	0.00032097	0.00798936
0.00027407	0.020079535	0.00012473	0.000037959	0.015516395
0.00022104	0.016442378	6.42558E-	0.00025543	0.010793341
0.00022209	0.01828857	6.34498E-	0.00022492	0.01444267

Table 7 Features Extracted from Equation (3.4) for Modified Images

So one can notice clearly the values which are belonging to the original images are less than the values that belong to the modified images except the values for the fourth original image.

Image 1	Image 2	Image 3	Image 4	Image 5
111.4291	85.48539	147.753	73.63984	118.3034
112.5512	86.58049	149.0483	73.89632	119.8206
114.5146	88.27932	151.286	74.9679	121.2806
115.9803	89.61851	152.798	75.74098	122.9587
117.6185	91.2122	154.6958	76.91455	124.3226
118.16	92.25572	155.3449	76.96649	126.111
120.7404	93.9981	157.1978	78.6866	127.7797
122.1578	95.15593	159.0964	78.89621	129.4279
123.3749	96.44112	160.424	79.78514	130.8482
125.0288	97.94004	161.6951	80.37367	132.7437
126.2342	99.27515	163.0352	81.29503	134.195
127.9074	100.8869	164.613	82.18391	135.6514
129.3126	102.1299	165.8162	83.02864	137.8852
130.4545	103.1982	166.7807	83.05354	139.5361
131.9853	104.6102	168.1659	84.00702	141.0634
133.2697	105.8783	169.881	84.75904	142.4135
134.5337	107.4144	170.8974	85.50805	144.1924
135.9885	108.7872	171.8207	85.81317	145.5181

w = **3**, **4**, ... **20** respectively

Table 8 Features Extracted From Equation (3.5) For Original Images

w = 3, 4, ... 20 respectively				
Image 1	**Image 2**	**Image 3**	**Image 4**	**Image 5**
114.044	68.62765	114.5437	74.26897	119.9768
115.1395	69.50824	115.8572	74.69611	121.3086
116.9669	70.92957	117.8656	75.96664	123.0294
118.1909	72.00233	119.294	76.8991	124.7067
119.65	73.32093	120.927	78.23424	125.9095
120.534	74.05615	121.6685	78.43988	126.8193
122.5863	75.59542	123.4994	80.31442	128.3014
124.2729	76.43738	124.9223	80.74881	130.8424
125.6962	77.46489	126.1396	81.7886	132.1928
126.8453	78.60954	127.394	82.52276	134.0586
128.4992	79.68347	128.6201	83.59526	135.468
129.5556	80.96391	130.0105	84.64953	136.817
131.1063	81.99115	131.1792	85.65127	138.1802
132.2756	82.64279	132.0834	85.8434	140.1558
133.7951	83.78369	133.3404	86.96878	141.6204
134.86	84.73092	134.8883	87.8597	142.8898
136.2011	86.1075	135.8079	88.75163	145.1398
137.5744	87.04613	136.8349	89.23759	146.4302

Table 9 Features Extracted From Equation (3.5) For Modified Images

It is obvious to see there are variances in the values in both tables (8 and 9) some values for original images are greater than values for modified images and one can see these values in the image 2 and image 3. While on the other hand, other values for original images are smaller than the values of modified images.

w = 3, 4, ... 20 respectively				
Image 1	**Image 2**	**Image 3**	**Image 4**	**Image 5**
3655373	3016105	5904576	2534190	3852219
2731834	2249146	4368878	1876367	2865100
1504475	1239935	2405555	1025707	1577912
1248527	1030186	1989534	854008.3	1310083
825680.3	681886.8	1311052	564714.4	865785.4
710025.2	587894.5	1120569	487753.8	740409.7
525995.8	436133.9	825804.7	362397.5	543443.8
1872350	1533094	2933855	1269926	1956200
1746155	1442943	2744651	1193182	1835545
1326040	1087689	2060464	899894.9	1382572
1249559	1036783	1951065	856675.6	1313715
993057.2	815833.5	1532938	676443.7	1038426
953780	783835.5	1463153	649243.4	980945
3072732	2505421	4682287	2078881	3189495
2941014	2427324	4503826	2004516	3081537
3105588	2550921	4721596	2121250	3259806
3015351	2461908	4555870	2058997	3156352
2032384	1661148	3056738	1370311	2121749

Table 10 Features Extracted From Equation (3.6) For Original Images

Image 1	Image 2	Image 3	Image 4	Image 5
3774448	2628689	5019176	2646069	3932123
2803720	1958843	3717333	1959000	2934366
1535574	1080465	2044666	1075658	1598197
1278968	896985.1	1692204	894916.7	1328807
841633.6	594489.2	1114730	593803.5	875351.3
733653.8	512502.1	954594.2	512691.8	761778.7
533512.3	379971.4	702903.5	381791.4	559126.7
1903139	1336048	2493740	1339819	1977065
1787387	1256885	2331290	1262372	1851712
1350085	946971.2	1752274	951775.5	1395618
1276044	902260.3	1657970	908487.8	1324292
1007292	710397.4	1304097	717115.6	1046618
958463.2	682570.4	1244195	689952.9	1001821
3116466	2177887	3982836	2210698	3239079
3011943	2109222	3829366	2137097	3125197
3158337	2223113	4017153	2260749	3306779
3048542	2151033	3874871	2199126	3171825
2048642	1441736	2602549	1464010	2133036

Table 11 Features Extracted From Equation (3.6) For Modified Images

The results in tables 10 and 11 just like other results gained form tables (8 and 9) and also the same situation is seen here regarding the values of second and third images.

One applies Fisher Linear discriminant on these results that are achieved from each equation and for both original and modified images.

Applying Fisher Linear Discriminant on the results, regarding the tables 6 and 7, when applying Fisher LDA, it takes the first cell in the first column from table 6 as a test value and remaining cells in the same column are used as a training values in addition, the cells in the first columns that belong to table 7 are used as a training values too except

the first cell in table 7 which is not used from the first columns. In other words, the total values in the both tables 6 and 7 that belong to first column have 10 values, 8 values are used as a training value and as explained above the first one as a test value and the 6th is not used in the our computation . The same way will be used for the second value in the first column and third value until finishing all value in the first column for original table then move to the next column and applying same methodology then to the third until finishing all columns for the original table. After finishing all columns in the original table, and also using same approach, then one apply it on the values in the modified table.

Figure 19 The process of applying FLD on the obtained features

41

Image	Image	Image	Image	Image 1
1.26436	0.31530	0.13221	0.73499	0.12861
0.93073	0.15974	0.06609	0.84328	0.07108
0.95132	0.10824	0.03844	0.76358	0.03725
1.01114	0.09310	0.03735	0.668	0.03456
0.78260	0.09176	0.01922	0.74507	0.01834
1.04573	0.10006	0.04478	0.68655	0.04615
0.62079	0.05487	0.01344	0.93899	0.00475
0.66281	0.04200	0.01044	0.89269	0.00479
0.55448	0.04196	0.00729	1.03548	0.00244
0.60356	0.03417	0.00966	0.96578	0.00257
0.55631	0.03518	0.00587	1.09096	0.00184
0.60171	0.03560	0.00682	0.93915	0.00345
0.48008	0.03995	0.00750	1.18526	0.00294
0.59456	0.02397	0.00669	0.93831	0.00228
0.33986	0.03846	0.00498	1.74194	0.00250
0.44948	0.02153	0.00489	1.25456	0.00114
0.39616	0.02022	0.00496	1.45577	0.00124
0.46957	0.01694	0.00320	1.14307	0.00163

Table 12 Applying LDA on the Features for Original Images

Image 1	Image 2	Image 3	Image 4	Image 5
0.21585	0.87253	0.15177	0.30268	1.40656
0.12950	0.97234	0.08550	0.15338	1.01188
0.09564	0.86426	0.04791	0.09881	1.01972
0.09165	0.75877	0.04025	0.08864	1.20219
0.05773	0.89402	0.02746	0.07860	1.04250
0.11593	0.80997	0.04978	0.08888	1.12038
0.03306	0.99541	0.01238	0.04957	0.84915
0.02518	0.97253	0.00972	0.03616	0.84167
0.02049	1.12060	0.00945	0.03128	0.73591
0.02557	1.04215	0.00941	0.03056	0.78357
0.01234	1.11180	0.00648	0.02719	0.69818
0.02226	1.01329	0.00396	0.02358	0.80945
0.00978	1.23368	0.00391	0.01918	0.65308
0.01861	1.05980	0.00594	0.02148	0.77643
0.01134	1.67528	0.00439	0.01938	0.46628
0.01116	1.30047	0.00508	0.01533	0.61321
0.01136	1.44263	0.00330	0.01305	0.53984
0.01016	1.21288	0.00291	0.01024	0.66975

Table 13 Applying LDA on the Features for Modifying Image

The tables 12 and 13 show the values that are taken from applying LDA on the extracted features.

Here one continues to apply Fisher LDA on the other features that are extracted from equations also for original and modified images. Then one takes the average of each column individually for the table of original images, the total numbers of the obtained values are 18.

Likewise in the table of the modified images as well as the 18 values obtained, one can notice that it is from one equation, thus for 3 equations (features equations) there are 48 values for the table of original images and same as for the tables of modified images.

A   B

A   B

Figure 20 Samples of images that worked on

Group (A) are the Original images, Group (B) are the Modified images

A   B

A   B

A   B

Figure 21 Samples of images that are worked on

Group (A) are the Original images, Group (B) are the Modified images

The following chapter discusses the results that are taken after applying Fisher LDA on all the images.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Overview

This chapter discusses the results that are taken from the purposed method, secondly it also deals with the results that are achieved from images after focusing just on the tampering area, in other words, it examines a modified part of area taken from the images, finally comparing between the results before and after while concentrating on the tampering area.

4.2 Experimental Results

This research method is applied on 10 images, 5 are original images and others 5 are modified images, these modified images are the same original ones, but after some tampering being made on them. After extracting features from the whole images according to the features equations in sec (3.1) then applying Fisher LDA on these features and taking out the averages of these features. It leads us to get 48 features for original images and likewise for the modified images as mentioned in sec (3.3).

4.2.1 Experimental on Whole Image

In tables 14 and 15 one can see the average values after applying Fisher LDA on the first features that are extracted (f_{sv}^1) from the original and the altered images respectively, it is obvious that the values in table 15 which belong to altered images are greater than the values in the table 14 for the original images.

w	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
values	0.515099	0.414189	0.37977	0.368837	0.331401	0.384658	0.326572	0.322551	0.328334	0.323152	0.338038	0.317351	0.343147	0.313164	0.425551	0.346326	0.375675	0.326886

Table 14 Average Values of Original Images for Feature 1

w	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
values	0.589882	0.470524	0.425274	0.436304	0.420065	0.43699	0.387918	0.377057	0.38355	0.378255	0.371203	0.374513	0.383931	0.376456	0.435339	0.389054	0.402041	0.381194

Table 15 Average Values of Modified Images for Feature 1

For the second features that are extracted (f_{sv}^2) according to the following tables 16 and 17, it is distinctly seen the contrary of the first feature (f_{sv}^1). The average values in table 16 for the genuine images are greater than the average values that belong to the modified images in table 17.

w	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
values	1.644489	1.639202	1.646418	1.650317	1.666008	1.663676	1.687719	1.666452	1.674505	1.676851	1.684437	1.696873	1.702319	1.688296	1.69734	1.700305	1.706234	1.706074

Table 16 Average Values of Original Images for Feature 2

w	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
values	1.492745	1.489289	1.497509	1.502048	1.516111	1.514322	1.53669	1.520983	1.529812	1.532499	1.5416	1.552136	1.55724	1.546577	1.555945	1.5584	1.567221	1.568381

Table 17 Average Values of Modified Images for Feature 2

Regarding the third feature, (f_{sv}^3) tables 18 and 19 show also the average values for the original image in table 18 which is greater than table 19 and has average values for modified images.

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	1.584658	1.582178	1.587684	1.592499	1.606338	1.605838	1.641343	1.60381	1.616493	1.618766	1.636761	1.63557	1.65767	1.632668	1.641803	1.650645	1.667005	1.652106

Table 18 Average Values of Original Images for Feature 3

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	1.468672	1.467584	1.468395	1.47487	1.486452	1.496227	1.523323	1.485769	1.498737	1.501394	1.518108	1.5174	1.538542	1.518888	1.529815	1.538419	1.550458	1.5361

Table 19 Average Values of Modified Images for Feature 3

4.2.2 Experimental on Tampering Area in the Image

Here by taking a part area of the images rather than the whole image and cropping just the altered area from the modified images then applying our proposed method taking into consideration that the original images are cropped, too.

In tables 20 and 21 given below, the averages values are seen of the first feature extracted (f_{sv}^1) from the original cropped images are less than the average values of modified cropped images.

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	0.511968	0.430245	0.412902	0.426633	0.342045	0.431478	0.383846	0.3854	0.386008	0.389108	0.395803	0.412697	0.433782	0.403701	0.340033	0.344646	0.328202	0.339578

Table 20 Average Values of Original Cropped Images for Feature 1

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	0.625155	0.541729	0.521748	0.585044	0.567185	0.527723	0.553062	0.600994	0.628787	0.594072	0.615192	0.712214	0.715307	0.676236	0.570935	0.638335	0.591374	0.650343

Table 21 Average Values of Modified Cropped Images for Feature 1

The tables 22 and 23 show the second feature (f_{sv}^2) that is extracted from the original as well as the modified cropped images. Just the same is also observed of tables 24 and 25 where the third feature (f_{sv}^3) that is extracted from the original and shows the modified

cropped images, too. The average values for original cropped images are greater than the average values of modified cropped images for both features as seen below.

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	2.269096	2.256399	2.260738	2.249913	2.252314	2.238624	2.223248	2.247954	2.238918	2.242073	2.24008	2.244004	2.250904	2.234213	2.240787	2.230657	2.243273	2.239815

Table 22 Average Values of Original Cropped Images for Feature 2

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	2.028745	2.020337	2.024422	2.022692	2.025043	2.011641	2.007539	2.021777	2.018801	2.026255	2.022526	2.030564	2.031874	2.021681	2.027769	2.02083	2.031524	2.032701

Table 23 Average Values of Modified Crop Images for Feature 2

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	1.735769	1.70994	1.71564	1.712879	1.727353	1.703445	1.728707	1.696723	1.69249	1.690099	1.700556	1.700054	1.72329	1.665148	1.667926	1.681525	1.688048	1.655195

Table 24 Average Values of Original Crop Images for Feature 3

W	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Values	1.549393	1.529959	1.532783	1.532518	1.545565	1.528126	1.546565	1.519398	1.513864	1.516318	1.52768	1.527281	1.548488	1.498095	1.500182	1.512413	1.518863	1.491632

Table 25 Average Values of Modified Crop Images for Feature 3

4.3 Conclusion

The proposed method is applied twice, firstly it is applied on the whole images area and secondly on the modified area (after cropping images). From the above shown tables for genuine images and altered images, one can notice clearly there are variance between average values of original images and modified images for all w size and these variance increased when focusing was done just on the modified area of the image rather than the whole image. In other words that is when cropping the images and applying the methods on altered area. Furthermore; the run time is decreased because the size of the area is reduced which leads to the decreasing the number of blocks that entered in the computations for extracting features.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this thesis, the proposed method is used to identify whether the images are genuine or not. By exploiting the soft connection between the rows and columns, using relative linear dependency that is given by the SVD based features. Taking advantage from this capability, any tampering which is done on the genuine image can be disclosed because the soft connection between the rows and columns are devastated. For this very goal in this research, three types of features have been used.

5.2 Future Works

The potential area of future work is to expand the proposed method to use it for determining which part of the area from the genuine image has been modified or altered.

REFERENCES

1. **http://www.hrc.utexas.edu/exhibitions/permanent/firstphotograph, Harry Ransom Center,** (Data Download Date : 05.05.2015)

2. **Mall, V., Shukla, S., Mitra, S. K., & Roy, A. K., (2013, May),** *"Comprehensive Image Index and Detection of Tampering in a Digital Image. In Informatics",* Electronics & Vision (ICIEV), 2013 International Conference, pp. 1-7. IEEE.

3. **http://petapixel.com/2010/11/04/first-digital-photograph-ever-made/,PetaPixe,** (Data Download Date : 05.05.2015)

4. **Neenu, H. U., & Cheriyan, J., (2014, July),** *"Image Forgery Detection Based on Illumination Inconsistencies & Intrinsic Resampling Properties".* In Emerging Research Areas: Magnetics, Machines and Drives (AICERA/iCMMD), 2014 Annual International Conference, pp. 1-6. IEEE.

5. **Bayram, S., Sencar, H. T., & Memon, N., (2009, April).** *"An Efficient and Robust Method for Detecting Copy-Move Forgery".* In Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference, pp. 1053-1056. IEEE.

6. **Swaminathan, A., Wu, M., & Liu, K. R., (2006, October).** *"Image Tampering Identification Using Blind Deconvolution".* In Image Processing, 2006 IEEE International Conference, pp. 2309-2312. IEEE.

7. **Lukáš, J., & Fridrich, J., (2003, August).** *"Estimation of Primary Quantization Matrix in Double Compressed JPEG Images".* In Proc. Digital Forensic Research Workshop, pp. 5-8.

8. **Pevny, T., & Fridrich, J., (2008).** *"Detection of Double-Compression in JPEG Images for Applications in Steganography".* Information Forensics and Security, IEEE Transactions, vol 3, no. 2, pp. 247-258.

9. **Farid, H., (2009).** *"Exposing Digital forgeries from JPEG Ghosts. Information Forensics and Security",* IEEE Transactions, vol 4, no.1, pp.154-160.

10. **Lin, Z., He, J., Tang, X., & Tang, C. K., (2009).** *"Fast, Automatic and Fine-Grained Tampered JPEG Image Detection via DCT Coefficient Analysis".* Pattern Recognition, vol42, no.11, pp. 2492-2501.

11. **Westfeld, A., & Pfitzmann, A., (2001, April).** *"High Capacity Despite Better Steganalysis (F5–a Steganographic Algorithm)".* In Information Hiding, 4th International Workshop vol. 2137, pp. 289-302.

12. **Provos, N., (2001, August).** *"Defending Against Statistical Steganalysis".* InUsenix Security Symposium vol. 10, pp. 323-336.

13. **Hany, F., (2006).** *"Digital Image Ballistics from JPEG Quantization".* Technical Report TR2006-583, Department of Computer Science, Dartmouth College.

14. **Popescu, A. C., & Farid, H., (2005, January).** *"Statistical Tools for Digital Forensics".* In Information Hiding, pp. 128-147.

15. **Galvan, F., Puglisi, G., Bruna, A., & Battiato, S., (2014).** *"First Quantization Matrix Estimation from Double Compressed JPEG Images"*

16. **Huang, F., Huang, J., & Shi, Y. Q., (2010).** "*Detecting Double JPEG Compression with the Same Quantization Matrix".* Information Forensics and Security, IEEE Transactions, vol 5, no.4, pp. 848-856.

17. **Birajdar, G. K., & Mankar, V. H., (2013).** *"Digital Image Forgery Detection using Passive Techniques: A Survey".* Digital Investigation, vol 10, no.3, pp. 226-245

18. **Johnson, M. K., & Farid, H., (2005, August).** *"Exposing Digital Forgeries by Detecting Inconsistencies in Lighting".* In Proceedings of the 7th workshop on Multimedia and security, pp. 1-10. ACM.

19. **Johnson, M. K., & Farid, H., (2005, August).** *"Exposing Digital Forgeries by Detecting Inconsistencies in Lighting".* In Proceedings of the 7th workshop on Multimedia and security, pp. 1-10.

20. **Nillius, P., & Eklundh, J. O., (2001).** *"Automatic Estimation of the Projected Light Source Direction".* In Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference, vol. 1, pp. I-1076.

21. **Lv, Y., Shen, X., & Chen, H., (2009, December).** *"Identifying Image Authenticity by Detecting Inconsistency in Light Source Direction".* In Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference, pp. 1-5.

22. **Hsu, Y. F., & Chang, S. F., (2006, July).** *"Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency".* In Multimedia and Expo, 2006 IEEE International Conference, pp. 549-552.

23. **Ng, T. T., Chang, S. F., Lin, C. Y., & Sun, Q., (2006).** *"Passive-Blind Image Forensics"*. Multimedia Security Technologies for Digital Rights, vol 15, pp. 383-412.

24. **Lin, Z., Wang, R., Tang, X., & Shum, H. Y., (2005, June).** *"Detecting Doctored Images Using Camera Response Normality and Consistency.* In Computer Vision and Pattern Recognition"*, 2005. CVPR 2005. IEEE Computer Society Conference, vol. 1, pp. 1087-1092.

25. **Farid, H., (1999).** *"Detecting Digital Forgeries Using Bispectral Analysis"*

26. **Ng, T. T., Chang, S. F., & Sun, Q., (2004, May).** *"Blind Detection of Photomontage Using Higher Order Statistics"*. In Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium, vol. 5, pp. V-688.

27. **Ng, T. T., Chang, S. F., & Sun, Q., (2004, May).** *"Blind Detection of Photomontage Using Higher Order Statistics"*. In Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium, vol. 5, pp. V-688.

28. **Fridrich, A. J., Soukal, B. D., & Lukáš, A. J., (2003).** *"Detection of Copy-Move Forgery in Digital Images"*. In in Proceedings of Digital Forensic Research Workshop

29. **Popescu, A. C., & Farid, H., (2004).** *"Exposing Digital Forgeries by Detecting Duplicated Image Regions"*. Dept. Compute. Sci., Dartmouth College, Tech. Rep. TR2004-515.

30. **Zhang, Z., Kang, J., & Ren, Y., (2008, December).** *"An Effective Algorithm of Image Splicing Detection"*. In Computer Science and Software Engineering, 2008 International Conference, vol. 1, pp. 1035-1039.

31. **Zhao, X., Wang, S., Li, S., & Li, J., (2014).** *"Passive Image Splicing Detection by 2-D Noncausal Markov Model"*.

32. **He, Z., Sun, W., Lu, W., & Lu, H., (2011).** *"Digital Image Splicing Detection Based on Approximate Run Length"*. Pattern Recognition Letters, vol 32, no.12, pp.1591-1597.

33. **Yan, L. I., ZHOU, Y. J., YUAN, K. G., GUO, Y. C., & NIU, X. X., (2014).** *"Exposing Photo Manipulation with Inconsistent Perspective Geometry"*. The Journal of China Universities of Posts and Telecommunications, vol 21, no.4, pp.83-10.

34. **Denis, P., Elder, J. H., & Estrada, F. J., (2008).** *"Efficient Edge-Based Methods for Estimating Manhattan Frames in Urban Imagery"*, pp. 197-210.

35. **San Choi, K., Lam, E. Y., & Wong, K. K., (2006, February).** *"Source Camera Identification Using Footprints from Lens Aberration".* In Electronic Imaging 2006, pp. 60690J-60690J.

36. **Bayram, S., Sencar, H., Memon, N., & Avcibas, I., (2005, September).** *"Source Camera Identification Based on CFA Interpolation".* In Image Processing, 2005. ICIP 2005. IEEE International Conference on vol. 3, pp. III-69.

37. **Van Lanh, T., Chong, K. S., Emmanuel, S., & Kankanhalli, M. S., (2007, July).** *"A survey on Digital Camera Image Forensic Methods".* In Multimedia and Expo, 2007 IEEE International Conference, pp. 16-19.

38. **Kharrazi, M., Sencar, H. T., & Memon, N., (2004, October).** *"Blind Source Camera Identification".* In Image Processing, 2004. ICIP'04. 2004 International Conference, vol. 1, pp. 709-712

39. **Gul, G., & Kurugollu, F., (2008, March).** *"Detection of Watermarking Methods Using Steganalysis".* In Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference, pp. 1725-1728.

40. **Gul, G., Avcibas, I., & Kurugollu, F., (2010, September).** *"SVD Based Image Manipulation Detection".* In Image Processing (ICIP), 2010 17th IEEE International Conference, pp. 1765-1768

41. **Theodoridis, S., Pikrakis, A., Koutroumbas, K., & Cavouras, D., (2010**). *"Introduction to Pattern Recognition: A Matlab Approach".* Academic Press.first published 2010.chapter Three, pp. 87-88.

42. **http:// www.youtube.com/watch?v=dS5vKUAC3Sc,** (Data Download Date : 15.07.2015)

43. **http:// www.dpreview.com/glossary/camera-system/color-filter-array,** (Data Download Date : 15.07.2015)

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Sinan, Majeed

Date and Place of Birth: 12 March 1983, Iraq / Nineveh / Mosul

Marital Status: Single

Phone: +90 534 611 65 19

Email: sinan_alkhayaat@yahoo.com

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya University Mathematics and Computer Science	2015
B.Sc.	College of computer and mathematical science	2005
High School	Al Risalah Secondary School	2001

WORK EXPERIENCE

Year	Place	Enrollment
2007- Present	The Ministry of Education / General – Directorate of Education in Nineveh	Specialist

FOREIN LANGUAGES

Advanced English, Beginner Turkish

HOBBIES

Reading Books, Chess, Volleyball, Swimming, Watching Movies and Traveling.