M.Tech Dissertation Report on

"SVD Based Improved Fragile Watermarking Scheme for Image Tamper Detection and Self-Recovery for Color Images"

In the partial fulfillment of the Master of Technology in Electronics and Communication Engineering

Submitted by

AMAN YADAV

2017PEC5250

Under the supervision of

Mr. Rakesh Bairathi

Associate Professor,

Department of Electronics and Communication Engineering,

Malaviya National Institute of Technology, Jaipur

June, 2019

CERTIFICATE

This is to certify that the project report entitled "*SVD Based Improved Fragile Watermarking Scheme for Image Tamper Detection and Self-Recovery for Color Images*" done by Aman Yadav, Enrollment No. 2017PEC5250 is an authentic work carried out by him at Malaviya National Institute of Technology, Jaipur under my guidance during the session 2017-2019.

Date:

(Rakesh Bairathi)
Associate Professor,
ECE Department,
MNIT, Jaipur

Declaration

This is to certify that the dissertation report entitled "*SVD Based Improved Fragile Watermarking Scheme for Image Tamper Detection and Self-Recovery for Color Images*" is being submitted by me in partial fulfillment of degree of Master of Technology in Electronics & Communication Engineering during 2017-19. This work is carried out by me under the supervision of Mr. Rakesh Bairathi, Associate Prof., Department of ECE, MNIT, Jaipur.

I am fully responsible for the material used in this report in case if any discrepancies arises. The report (fully/partly) is not submitted for the award of any other degree. Wherever I have consulted the published work of others, it is clearly attributed. Where I have quoted from the work of others, the source is always given. To best of my knowledge, I have acknowledge all the relevant sources in the report. With the exception of above, this report is entirely my own work.

Date:

Aman Yadav
2017PEC5250

Acknowledgement

I would like to express my gratitude towards **Mr. Rakesh Bairathi**, Associate Professor, ECE department MNIT, Jaipur for his guidance, motivating support and valuable suggestions. I am grateful to him for giving me the freedom to explore many opportunities and guidance when I was overwhelmed.

I would also like to thank **Dr. D. Boolchandani**, Head of department of Electronics and Communication Engineering, MNIT Jaipur for his valuable support and suggestions.

I would also like to thank Department of Electronics and communication of Malaviya National Institute of Technology, Jaipur for providing me with the resources needed for the completion of this project.

I would also like to thank my friends and all my colleague in developing the project and people who have willingly helped me out with their abilities.

I would like to express my gratitude towards my parents for their kind co-operation and encouragement which help me in completion of this project.

Table of Content

Abstract

An image content modification became easy in past few decades as computer based applications have been increased a lot. Image authentication becomes a necessity must for further use of it. In this concern a SVD based semi fragile watermarking scheme for image authentication is proposed here. The proposed schemes detects the tampered blocks in an image as well as recover the original image back. In proposed scheme, a host image is broken into 4x4 non overlapping blocks and SVD is applied on each block. Traces of SVD is calculated for each block and its binary equivalent is calculated. This binary equivalent work as block authentication bits for image tampering detection. Alongside of block authentication bits, self-recovery bits are also calculated. A 4x4 image block is further divided into 2x2 block and average value for each 2x2 block is calculated. Binary equivalent of these average values are self-recovery bits. Both block authentication and self-recovery bits are watermarked in LSBs of original image. The watermarked information is extracted at receiver's end block authentication is performed for each image block. If the block is found tampered, the actual information of tampered block is recovered back with the help of self-recovery bits.

List of Figures

List of Tables

Chapter-1:

Introduction

1.1 Introduction

Since the first camera was developed, from the day technology has been improved a lot now a days. After the embedding of cameras along with smartphones people are addicted towards the use of it. Images are now becoming a part of everyone's life. Some of them are storing images as their memories of past and some are using images as data transmission.

Due to the advances in the technologies and a huge development of computer based communication it became very easy to manipulate the original data in any field. So image processing is no more an exception. Now a days there are a lot of image processing toolbox like paint, Photoshop and many more which can easily manipulate the image and that can be a serious concern. So the image security as well as image recovery becomes important. In this regards a watermarking scheme is proposed for tamper detection in an image as well as the self-recovery scheme is also proposed to recover the tampered region.

1.2 Objective of the study

Photography lost its innocent years ago. Image manipulation is becoming easier every day. When Niepce created first image in 1814, after a few decades of it images are already being manipulated. Tampering of an image can be innocent or destructive in many ways [1]. There are two ways of image tampering. One, if image quality is changed but the content of an image is unchanged is named as innocent tampering such as image contrast brightness, image zooming, image rotation, image adjustment and many more. On the other hand if the intent of tampering is to change the content of image can be named as evil tampering such as copy and paste attack, image content removal, image text addition or deletion and so on.

Innocent tampering is less destructive and easy to detect while evil tampering can be a serious concern as it modifies the original image. Evil tampering can be a serious concern in many fields such as medical imaging, military operations, evidence manipulation etc. So the forensic of image is needed in this context. In medical field a hair line structure addition in x-ray or ultrasonography, can results as a complete change in the actual information and will results as a wrong medical report. Same for crime spot images, if the crime spot images are manipulated will result as evidence manipulation. In such aspects authenticity of image becomes a serious concern. Hence the credibility and respectability of an image needs to be protected [2], [3]. Watermarking schemes and cryptography schemes are used to authenticate the image. In this concern a lot of watermarking schemes have been proposed.

1.3 Overview of the problem

Image tampering became common now a days so the image authentication is required. There has been a lot of research in field of image authentication where most of the previously proposed schemes are able to detect the tampering in an image and some of them are even able to detect tampered region. But only a few of them are able to recover the detected tampered region. Even though some previously proposed schemes are able to recover the tampered region but there image quality is not up to the mark. Quality of recovered image decreases as the tampered region in image increases. If the quality of an image decreases below a certain mark, the recovered image is nor more of use. The problem of image quality need to be solved and I am proposing an addition to the previously done work by Shehab and Elhoseny [4]. Shehab and Elhoseny proposed a robust and fragile watermarking scheme in spatial domain. The scheme they used is able to detect almost all the tampered regions in an image and recovery of all the detected region. The image quality of my proposed scheme is found sufficiently better than the previous scheme. A comparison between both the schemes is given upcoming section.

1.4 Thesis organization

Chapter-2 provides a literature review for previously reported schemes.

Chapter-3 covers the basics of digital watermarking schemes and its properties. Chapter also includes a brief review on some special algorithms such as SVD and Arnold transform.

Chater-4 comprises the proposed scheme and improvement to the previous proposed scheme. This chapter also includes watermark generation, embedding and extraction for proposed scheme.

Chapter-5 covers a detailed performance analysis for and improved result comparison of proposed scheme over previously proposed scheme.

Chapter-6 represents the performance of proposed scheme over color images for some standard color images followed by random color images.

Chapter-2:

Literature Review

In field of image processing, a lot of watermarking and de-watermarking schemes have been proposed in last few decades. Many of them were able to detect the altered images and some of them were able to recover that altered region. Some of the previous schemes are as follows:

S Rawat, B Raman [5], proposed a chaotic system based fragile watermarking scheme. A chaotic sequence is generated using a logistic map and added with a binary watermark image. The result is watermarked into Arnold catmap based scrambled host image. Anti-Arnold catmap is used on scrambled image to forge a watermarked image. Image tamper detection is performed based on the extracted watermark at other end. Unfortunately, this scheme can only detect the altered regions in a watermarked image but not able to reconstruct the original image back.

X Zhang, S Wang [6], proposed a novel statistical fragile watermarking scheme for location detection of tampered pixels. Authentication bits are generated from pixel values and watermarked into the host image. Based on the watermarked information tampered pixels are detected. In some cases generated information may coincide which can result in false declaration. And more of this scheme is able to detect the tampered pixels but cannot reconstruct the original information.

V Dhole, N Patil [7], provided a self-embedding watermarking scheme for tamper detection and recovery of tampered blocks. This scheme was well enough to detect the altered areas in an image and recovery of altered regions. But is unable to handle the Vector Quantization (VQ) attack.

B Patra, J Patra [8], gave a Chinese Remainder Theorem (CRT) based watermarking scheme for image authentication and recovery of altered regions. This scheme had an improved computational complexity. They proposed bigger size (8x8) block based watermarking scheme. The disadvantage with such big size block based scheme are poor tamper detection.

M. Elarbi, C. Amar[9], provided a neural network based recovery of tampered images. A host image is divided into 8x8 blocks and average value is computed for each block. Generated watermark information of a host block is hidden in another block sufficiently far from host block. A neural network is trained against average value computed for recovery of tampered region. Even after decent results the bigger block results in less tamper localization detection.

In a matrix Singular Value Decomposition (SVD) demonstrates its basic building structure. Any change in the matrix changes its corresponding singular matrix. This property of SVD can be used for tamper detection in an image. A lot of SVD based watermarking have been proposed in past few years. Some of them are demonstrated below.

R. Liu, T. Tan [10], gave a SVD based watermarking scheme to identify the ownership of digital media. The problem the scheme is it only provides the rightful ownership of image but cannot sustain against any kind of attacks.

R. Sun, H. Sun, T. Yao [11], came up with a SVD based watermarking scheme for image authentication. SVD based watermark is generated & watermark is quantized and embedded into host image for image authentication. Again the problem with this approach is no recovery for altered regions.

A. Shehab, M. Elhonesy [4], proposed a SVD based image tamper localization detection and self-recovery of the altered image blocks. Proposed scheme uses SVD calculation on each 4x4 image block of host image. 4x4 block based recovery provides a major advantage of higher tamper localization detection.

The scheme provided by Shehab and Elhonesy [4] provides a better tamper detection localization due to small block size and recovery of altered blocks. The scheme uses a 32 bit watermark generation for each block consist of 12 authentication bits and remaining 20 as

self-recovery bits. Even though the results were pretty decent but still they could have been improved.

I am proposing some improvements to the scheme to improve the quality of recovered image for all tampered blocks. In this concern I am denoting it as my major reference scheme.

Chapter-3:

Digital Watermarking and Its Significance

Image processing is one of the techniques where we can perform some operations on an image to get an enhanced image or extraction of some useful data out of an image. Image processing normally includes three steps:

- Importing an image via different image acquisition tools
- Analysis and manipulation of an image
- Output result as modified image

Analogue and digital image processing are two main types of image processing. Analogue image processing is used for hard copies and digital image processing is used for digital image manipulation. Major applications of a digital image processing are image resizing, image enhancement, contrast enhancement, filtering etc. [12].

Image processing has a lot of applications in different field such as moving object tracker, biomedical imaging, defense services etc. [13].

3.1 Significance

Digital Multimedia plays an important role in a lot of application such as intelligent information gathering, news reporting, criminal investigation, surveillance, health care etc. But in last few decades technology has been improved a lot and unauthorized personals can easily manipulate or modify the information using different digital multimedia editing tools. So the authenticity of such information is no longer trustworthy. Such authenticity problem can be resolved using watermarking schemes.

Different digital watermarking schemes have been proposed in years which have been considered as one of the most promising techniques for digital information authentication. General idea of watermarking is to embed a secrete watermark in original information which is used to identify the authenticity of information. If the watermark is extracted successfully the information is authentic else the information has been modified.

A lot of watermarking schemes has already being proposed, among all of them semi fragile watermarking schemes are commonly used for copyright protection and information tampering detection.

I am here presenting a color image tamper localization detection scheme which identifies the authenticity of the image. Using this schemes one can also find the localization of tampered region if the watermarked image has been tampered. Along with the tamper localization detection presented scheme can also recover the original image back if tampered.

3.2 Background

Before moving forward to the presented scheme, a brief review of digital watermarking schemes along with its important properties in the next section followed by basic algorithms which I have used in my work.

3.2.1 Digital watermarking and its properties

Watermarking is not a new technique, according to Weiss and Historische [14], it started back in 13th century in Europe where a visible mark was superimposed on an image as one's signature. It has been used for years for digital information security. The basic idea behind a digital watermarking technique is to embed a secrete mark which can later be used to authenticate the digital information.

During the early years of digital watermarking history except the visibility of watermark watermarking was well and good. Clearly, visible watermark is not suitable as it is superimposed that can bring distortions which may lead to reduced visual quality of an

image. So an efficient watermarking technique must follow the following properties [15]:

1.1. Invisibility of watermark: The watermark embedded into any digital multimedia such as image, video, audio should not be visible to the user else watermarking scheme may result to some distortions. A lot of search has done to find the minimum requirements of invisibility for distortion free watermarking. The distortion introduced by the watermark should not be more than the just-noticeable distortion (JND) of the image. Some researchers calculated the JND for contrast sensitivity function (CSF) and Watson model [16, 17].

1.2. Tamper Detection: Tamper detection should be reliable. Watermark detection authenticity depends on two concepts, one is false positive error and the other is false negative error. False positive error occurs when there is no watermark in host media despite of it the detector still declares the error. A false negative error occurs when watermark is available in host media but still detector declares that there is no watermark in it.

1.3. Altered region identification: Tamper detection is one aspect of digital watermarking schemes. Alongside of tamper detection the location of altered regions should be highly disposed to verification as authenticated.

1.4. Incidental and malicious tamper Discrimination: One of the most difficult issue in digital watermarking is to discriminate between incidental distortion and intentional tampering. This discrimination includes a tolerance level to common image processing (image enhancement) and image compression. Any digital watermarking scheme is supposed to survive against such distortions but it should still be able to detect malicious tampering attacks such as add and removal of content, text addition etc.

1.5. Security: The embedded watermark should be impervious to forgery and manipulation of digital information.

1.6. Unaware of transmission of information: The host image and explicit information obtained from the host image should not be used in authentication process.

3.2.2 Semi fragile watermarking scheme

Any fragile digital watermarking scheme consists of two major components, embedding of watermark and extraction of embedded watermark. Figure 3.1 shows the basic block diagram of any digital watermarking scheme. Here I am briefing about both embedding and extraction of watermarking schemes.

Watermark embedding process: Part-1 of figure 3.1 shows the embedding scheme. The embedding scheme consists two major parts, generation of watermark and embedding of generated watermark. In general the watermark can be a randomly generated sequence or a binary image or a content based signature. After generation of watermark, using different proposed schemes watermark is embedded in the host image.

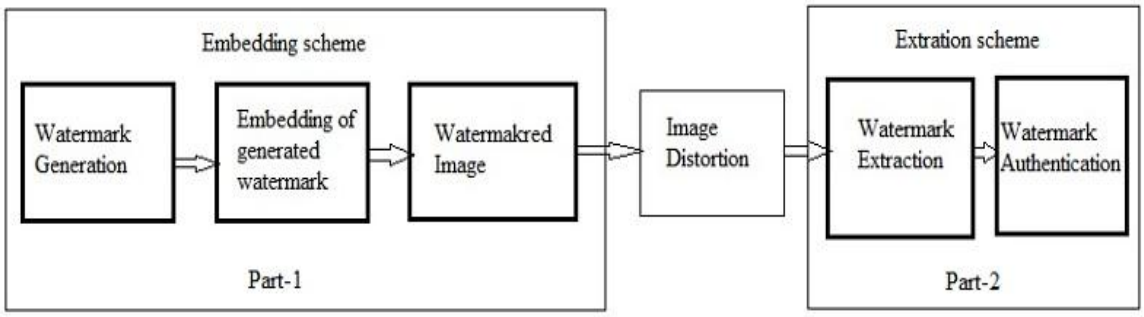

Figure-3.1: Typical semi fragile watermarking scheme

Watermark extraction process: Part-2 of figure 3.1 shows the watermark extraction process. The same algorithm is applied at the receiver's end for watermark extraction. For image authentication, extracted watermark is compared with actual watermark. If the original and extracted watermark are different then the image is marked as tampered one.

3.3 Singular Value Decomposition

Matrix decomposition or matrix factorization includes the description of a particular matrix using its constituents. SVD is matrix decomposition method used for reduction of a matrix to its constituent parts to make the matrix calculations simple. SVD can be applied for both real valued matrixes as well as complex matrixes. SVD is applied on a host image results in three matrixes. Basic expression for SVD is as follows:

$$A = PSQ^T \quad (1)$$

Where P, S and Q are left singular matrix, singular matrix and right singular matrix respectively and A is the host image. SVD is applied to obtain three new matrixes as P, S, and Q. Left and right singular matrixes are vector matrixes and follows a property as $PP^T = I_n$ and s $QQ^T = I_n$, where I_n is an identity matrix. [18], [19].

Singular matrix S follows a few properties. S-matrix is a diagonal matrix where all the diagonal elements are in descending order starting from the first. Each diagonal element for S-matrix is known as singular values. An NxN square matrix results in N singular values. These singular values shows a robust nature against intentional or un-intentional attacks on host image. This property of robustness towards different attacks can be used for authenticity of an image.

3.4 Arnold and Anti Arnold Transform:

Image scrambling techniques are used in digital image processing to disorder the original image. Due to its periodicity, Arnold transform is widely used in image scrambling algorithms. Arnold transform is a process of realignment of pixels in an image. One pixel is realigned to the other pixel location. A two dimensional Arnold transform is as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \quad (2)$$

Where x and y are pixel coordinates of host image, N is square image size and x' and y' are scrambled image coordinates. If this transform is performed several times, it results as well shuffled scrambled image [20]. Periodicity of Arnold transform varies with different image sizes.

Due to the periodicity property of Arnold transform recovery of scrambled image is easy. To find Anti-Arnold algorithm, let T being total iterations for a host image. And Arnold transform is performed i times then performing the same algotithms $(T - i)$ times more, one can get the original host image back.

For $P = Q.R$ where P, Q and R being matrixes, using the property of inverse matrix $R = Q^{-1}.P$. Using the same property, inverse of a Arnold matrix can be calculated as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} mod\ N \quad (3)$$

3.5 Reference Scheme

Shehab and Elhoseny [4], proposed a watermarking scheme for medical image tamper detection and self-recovery of tampered blocks. A host image is divided into 4x4 non overlapping blocks and SVD is performed over each such block and traces for block wise SVD is also calculated which is used as authentication bits mapped in between 1 to 2048. Arnold algorithm is also performed for each 4x4 block and 4x4 block is further divided into 2x2 sub-blocks. Average value is computed for each sub-block which are used as self recovery bits for tampered regions.

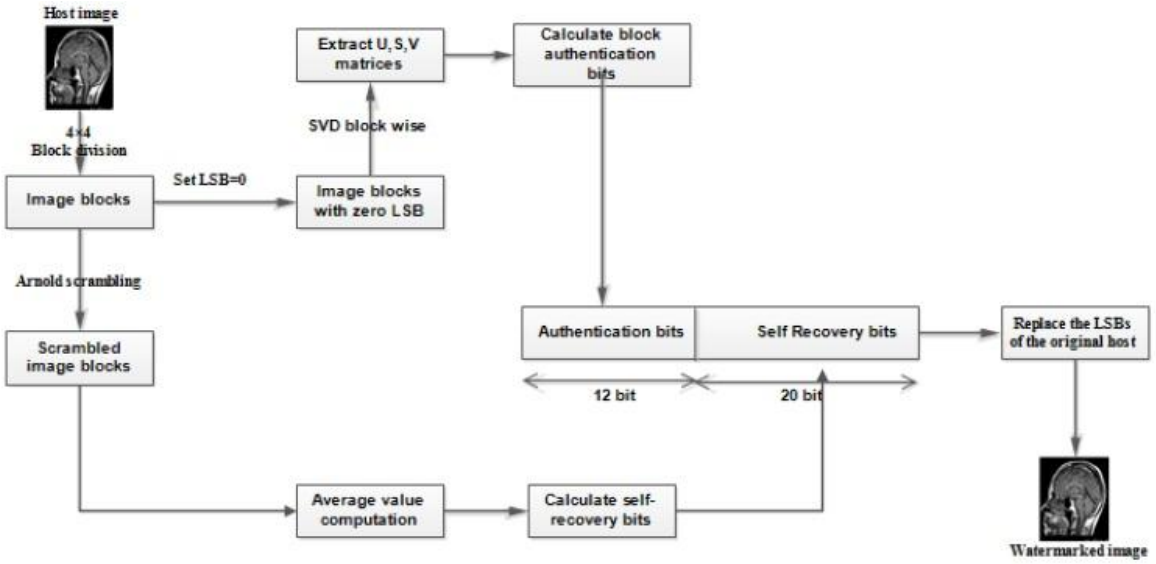

Figure-3.2: Watermarking process for reference scheme [4]

Figure 3.2 shows the watermarking scheme proposed by Shehab and Elhoseny [4] where they used combination of 12 authentication bits and 20 self-recovery bits for each 4x4 block. Complete 32 bit watermark is embedded in 4x4 block by replacing the last 2 LSB bits of that block. And all such blocks are recombined to form a watermarked image f

Figure-3.2 shows a de-watermarking process for reference scheme [4]. Where each watermarked image is again divided into 4x4 non overlapping blocks and last two LSB bit information is extracted. And again SVD and Arnold algorithms are performed.

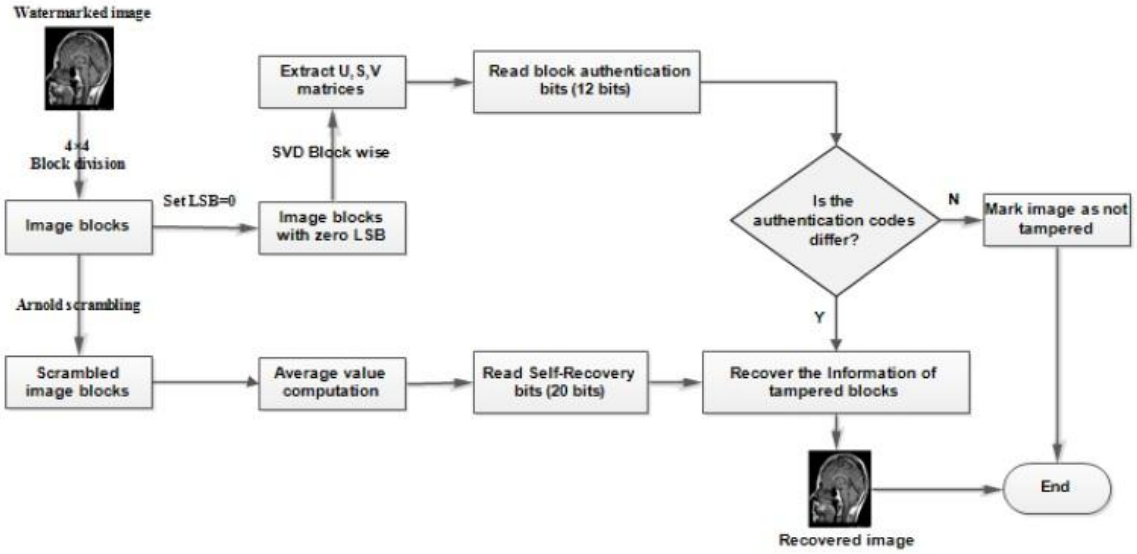

Figure-3.3: De-watermarking process for reference scheme [4]

Block authentication bits are calculated same as watermarking process and compared with extracted attention bits. If both are equal image is not tampered and if authentication bits differs then information of the tampered image block is recovered with the help of self-recovery bits.

The reference scheme [4] uses a 12 bits for authentication of an image which can provide a better image authentication but at the same time it uses only 20 bits for self-recovery of tampered block, 5 MSB bits for each 2x2 sub block which can result in high loss of information.

Here I am proposing an improvement in the above watermarking scheme by using 6 MSB bits for tampered image recovery and only 8 bit for image for image authentication. More self-recovery bit provides a better recovery of tampered region. At the same time reducing the authentication bits may result as wrong tampered detection for some block but the issue

can be resolved by selecting a proper mapping for SVD traces. Improved flow charts for watermarking and de-watermarking process for proposed schemes are shown in upcoming chapter.

Chapter-4:

Proposed Scheme

The proposed semi-fragile watermarking scheme consists of four major components: watermark generation, watermark embedding into host image, watermark extraction and authentication of received image. Before starting the chapter, I am briefing some important notations and concepts which are later used in my thesis.

Important notations:

Table-4.1: Watermark terminology

Host image	The original image which has to be watermarked
BAN (Block Authentication Number)	used for authentication of image at receivers end
PB (Protected Block)	Block for which watermark is generated
SB (Supporting Block)	Block in which generated watermark of PB block is embedded

Various researches such as image processing, cryptography are may be slightly different terminology from each other, but most of these terminology share some common standards. Table 4.1 provides a quick guide to the most frequently used terminology.

4.1 Watermark Generation

Using the SVD algorithm we are generating a content based watermark which is later embedded in host image. Figure 4.1 shows flow chart of improved watermark generation and embedding process for proposed scheme.

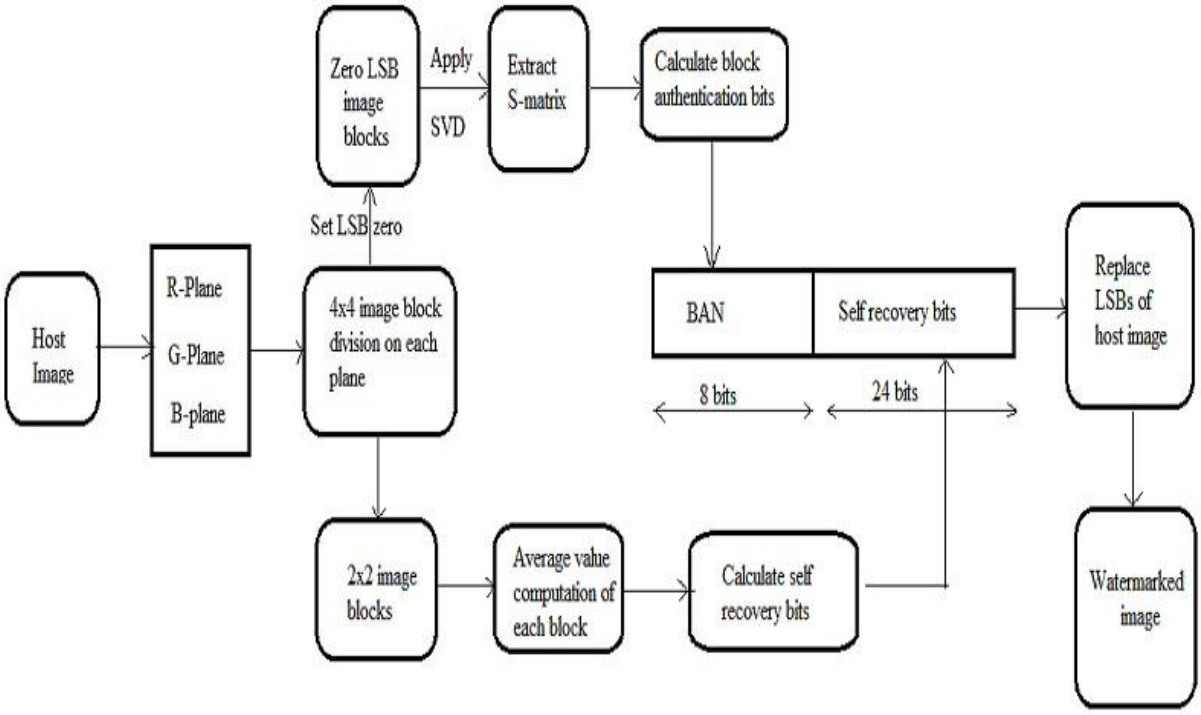

Figure-4.1: Improved watermark generation and embedding process

Detailed steps for generating the content based watermark are as follows:

1. At the very beginning of watermark generation, the host color image is divided into its corresponding three planes that are Red, Green and Blue planes.
2. First, the actual image is divided into four equal size rectangular blocks and named as major blocks. Which are used later during watermark embedding.
3. Red plane is selected at first, and it is divided into 4x4 non overlapping blocks.
4. One 4x4 block is selected at once and SVD algorithm is applied on it.
5. Last two LSBs of each pixel n a 4x4 block is set to zero and SVD algorithm is performed on it.
6. SVD generates three matrixes U, S, and V. Now trace of S matrix is calculated for each block which is used as block authentication in my work.
7. The calculated trace is mapped in range of 0-255 and 8 bit binary equivalent of this mapped trace is also calculated and named as block authentication number (BAN).
8. Each 4x4 block is further divided into a four 2x2 non overlapping blocks.
9. An average value is being computed for each 2x2 block.

10. Binary equivalent of each of computed value is also being computed.
11. Six MSB bits of each computed average value is taken out to for self-recovery bits. 6*4 makes it 24 self-recovery bits, 6 bits for each 2x2 block.
12. Both BAN and self-recovery bits are combined to for a 32 bit watermark. 8 bits for image authentication and remaining 24 bits for recovery of tampered block if authentication of image fails for any block.
13. For green and blue planes, step 7-9 are repeated.
14. Once the average value of 2x2 block is obtained, the complete 8 bit is used as self-recovery. 8*4 makes it 32 self-recovery bits, 8 bits for each 2x2 block.
15. Later this 32 bit watermark for all three plane is being embedded in host image which is discussed in the upcoming section.

4.2. Watermark Embedding

In order to be able to recover the altered content Generated watermark needs to be embedded in the host image. In order to embed the watermark into host image PB (protected Block) and SB (supporting block) comes into play. This PB and SB block division provides us the better self-recovery if any corruption occurs to PB. Selecting SB for a PB in a random manner might be closer to each other and may result as both block tampering. In such case self-recovery information may lost. To do so, PB and SB must be well distant from each other. A basic diagram of PB and SB selection is shown in figure 4.2. As it can be seen in the figure, for PB-1 its corresponding SB-1 is well and distant from each other and similar to remaining blocks also.

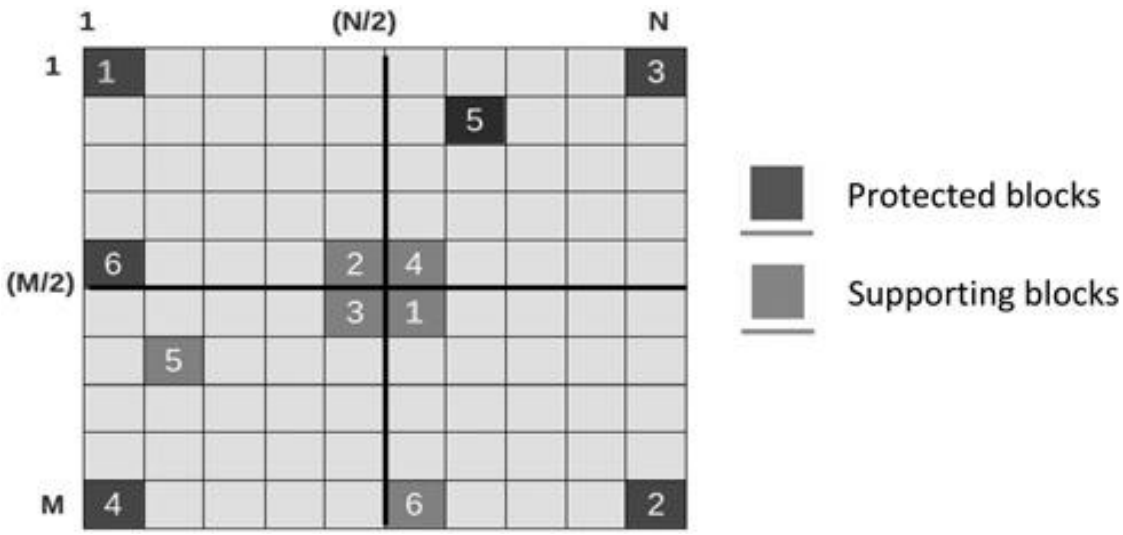

Figure 4.2: PBs and corresponding SBs [9]

Detailed steps for generated watermark embedding in host image are as follows:

1. Last two LSBs of each pixel are being used as watermark embedding process.
2. There are a total of 16 pixels in 4x4 image blocks. Set last two LSBs from each pixel as zero will results as 32 vacant space (2*16).
3. First, the each plane of actual image is divided into four equal size rectangular blocks and named as major blocks.
4. Smaller 4x4 blocks of major Block-1 and Block-4 are PBs and SBs for each other.
5. Each major block is then divided into 4x4 non overlapping blocks (similar block used during watermark generation)
6. For each 4x4 PB its corresponding SB is selected.
7. Watermark embedding for red plane is performed at first. The two LSBs of first four blocks of PB are set as initial 8 bits of 32 watermarks bits.
8. Step-7 is repeated for corresponding SB block where initial 8 bits are entered from its own 32 watermark bits.
9. Remaining 24 bits of each PB and SB are watermarked into each other. And red plane is watermarked
10. To watermark blue and green planes, one 4x4 block is selected as PB and its 32 bit watermark is embedded into last two LSBs of each pixel of its corresponding SB block.

11. Once the watermark is embedded, all the three planes are recombined to for a watermarked color image. And image is ready to use.

4.3. Watermark Extraction:

Watermark extraction is must for any watermarking scheme. If one cannot extract the watermark from its watermarked image, the watermarking scheme s of no use. To extract the watermark from watermarked image a similar process is performed as it was done in during watermarking. Figure 4.3 shows a flow chart of improved watermark extraction process.

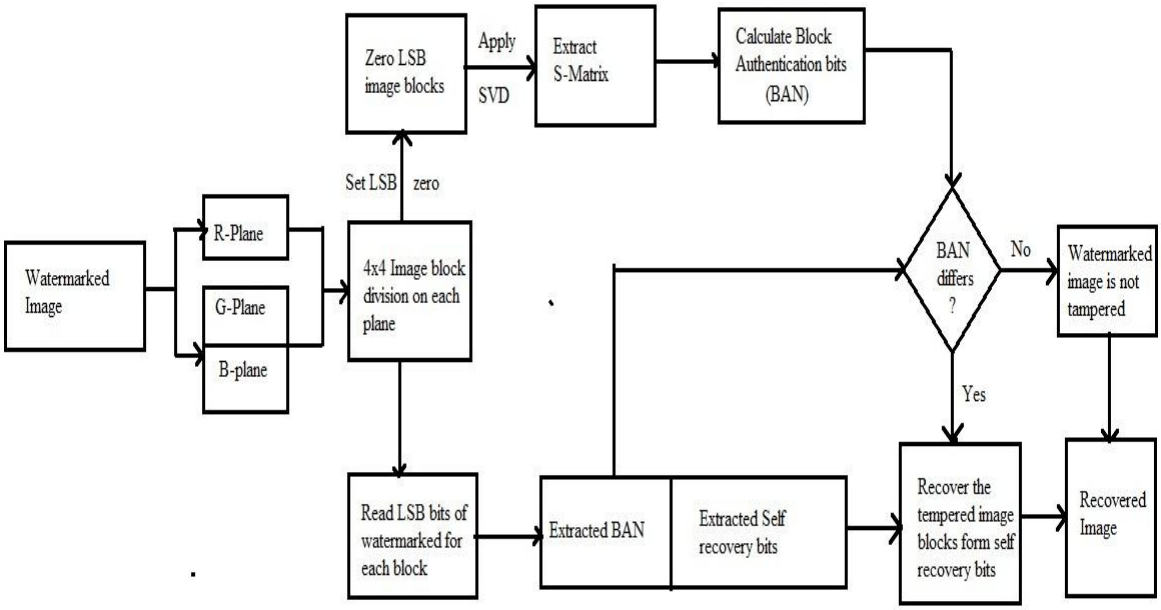

Figure 4.3 Improved watermark extraction & recovery process

Detailed steps for watermark extraction process are as follows:

1. First the received watermarked image is divided into its corresponding Red, Green and Blue planes.
2. Each plane is then divided into four equal size major blocks.

3. Red plane is watermarked with block authentication bits so only red plane is divided into 4x4 non overlapping blocks.
4. Last two LSBs of each pixel of a 4x4 block is extracted out of it.
5. This extracted value consists of two parts as extracted BAN and self-recovery bits of corresponding SB of 4x4 block.
6. Once the watermarked BAN is extracted, set last two LSBs of each pixel to zero.
7. SVD algorithm is performed on zero LSB blocks and S-matrix is generated.
8. Find the trace of generated S-matrix and map it in range 0-255.
9. Binary equivalent of this mapped trace is also calculated and is compared with the extracted BAN from step-5.
10. If the re-calculated BAN and extracted BAN are equal the image block is marked as not tampered else it is marked as tampered.
11. If none of watermarked image blocks is tampered, the image is marked as un-tampered image.

4.4. Recovery of tampered blocks:

If a watermarked image is found as tampered image, then it needs to be recovered. I am proposing a block tamper detection method and it recovery if found tampered. In order to reconstruct the image block self-recovery bits are extracted out of watermarked image. Detailed steps for self-recovery of tampered image block are as follows:

1. Self-recovery bits are extracted out of corresponding SB of tampered PB.
2. For red plane, there are 24 bits of self-recovery information, 6 MSB bits of each 2x2 block.
3. All 6 bits are MSB of tampered 2x2 block, so there can be an error of 2 bits or 4 pixel values. To minimize the error, 2 additional bits are added as [1 0] to compensate the error from 4 pixel values to 2 pixel values.
4. Such 2x2 blocks are recombined to form a 4x4 recovered image block.
5. For green and blue planes, there are 32 bits of self-recovery information, 8 bits for each 2x2 tampered blocks.

6. All 8 bits are converted back to decimal equivalent of self-recovery bits to form a recovered 2x2 block.
7. Such 2x2 blocks are recombined to form a recovered 4x4 block for blue and green plane.
8. When all the 4x4 tampered blocks are recovered, they are recombined to form a reconstructed image for each plane.
9. At last all the three planes are recombined to for the original reconstructed color image.

The reference scheme [4] uses a 12 bit authentication information and less recovery bits while proposed scheme uses 8 bit authentication information and more recovery bits then the reference scheme [4]. A complete performance analysis along with test image results are presented in the upcoming section. Later the proposed scheme is also performed over different size color images.

Chapter-5:

Performance Analysis

5.1 Comparison with previous work

The proposed scheme is applied to some of the standard MATLAB images with different types of attacks such as copy and paste attack, text edition, content removal and VQ attack. The reference scheme is also performed on all of the above attacks. The images are recovered successfully and the results are compared for both schemes. PSNR of the recovered image for both schemes are compared. Table 5.1 shows a comparative study of the proposed scheme and previous work.

Table-5.1: Comparison of reference scheme [4] and proposed scheme against different types of attacks

Type of attacks	Host Images	Shehab et al [4]		Proposed Scheme	
		Water-marked Image PSNR (dB)	Recovered Image PSNR (dB)	Water-marked Image PSNR (dB)	Recovered Image PSNR (dB)
Copy and paste attack1	Lena	44.22	37.35	44.43	40.76
	Barbara	44.20	40.70	44.44	43.60
Text Addition	Airplane	44.12	41.32	44.22	40.45
	Barbara	44.20	35.23	44.44	36.68
	Lena	44.22	35.08	44.43	37.95

Content removal	Barbara	44.20	38.41	44.44	41.98
VQ attack	Lena + Barbara	44.22	38.81	44.43	40.16

5.1.1. Copy and paste attack

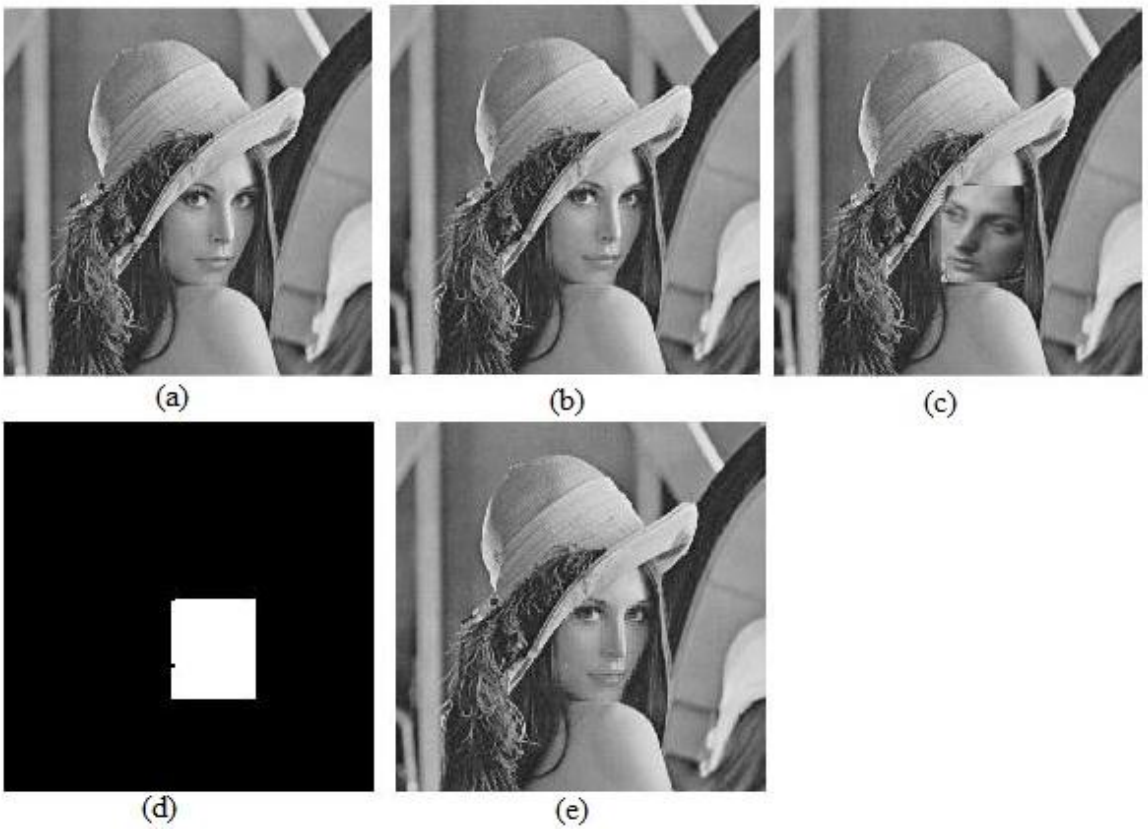

Figure-5.1: Copy-paste attack Lena for reference scheme [4] (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization, (e) recovered image

In a copy and paste attack, a small part of some image is copied and pasted on the watermarked image. A copy & paste attack is performed on a 512*512 Lena and Barbara image. Same content is copied and pasted at same location in watermarked image.

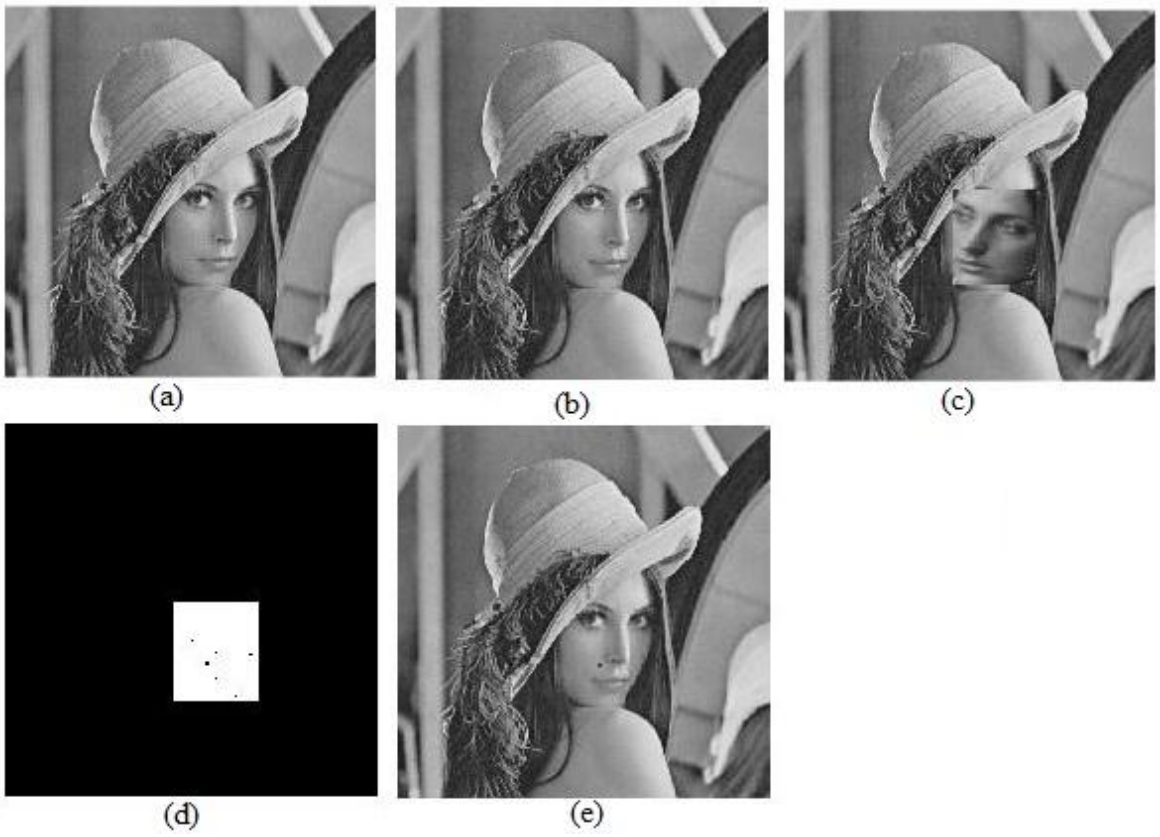

Figure-5.2: Copy-paste attack Lena for proposed scheme (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization detection, (e) recovered image

Figure 5.1 shows the recovery of Lena image against copy paste attack for reference scheme [4]. The scheme detects almost all the tampered blocks with an accuracy of 99.98%. Even after a high tamper detection rate the scheme results average reconstruction of tampered blocks with a PSNR of 37.35 dB. The recovered blocks appears to be a bit noisy and blur.

On the other hand, the proposed scheme detects the tampered region with an accuracy of 99.96%. Figure 5.2 shows the proposed scheme for Lena image. The reconstructed image PSNR for proposed scheme is 40.76 dB. The recovered blocks for proposed scheme appears better than the previously proposed scheme [4].

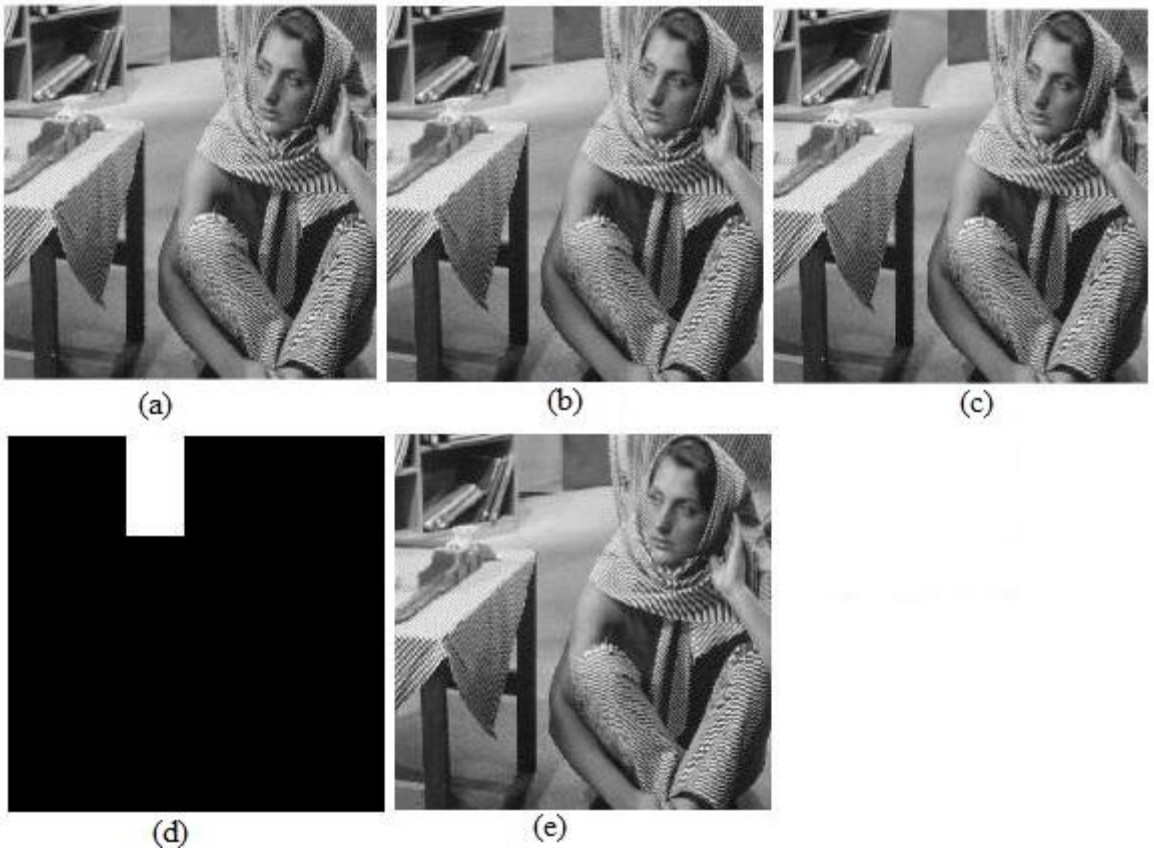

Figure-5.3: Copy-paste attack Barbara for reference scheme [4], (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization, (e) recovered image

Alongside of Lena image, copy and paste attack is also tested against Barbara image for better results comparison. Both the scheme performed image tampered detection efficiently with zero false detection. Results for previous scheme [4] are shown in figure 5.3. Again even after a high tampered detection accuracy, the recovered PSNR was found to be 40.70 dB.

Figure 5.4 shows the proposed scheme against copy and paste attack. The recovered PSNR was found to be 43.60 dB which is very close to its watermarked image PSNR of 44.44 dB.

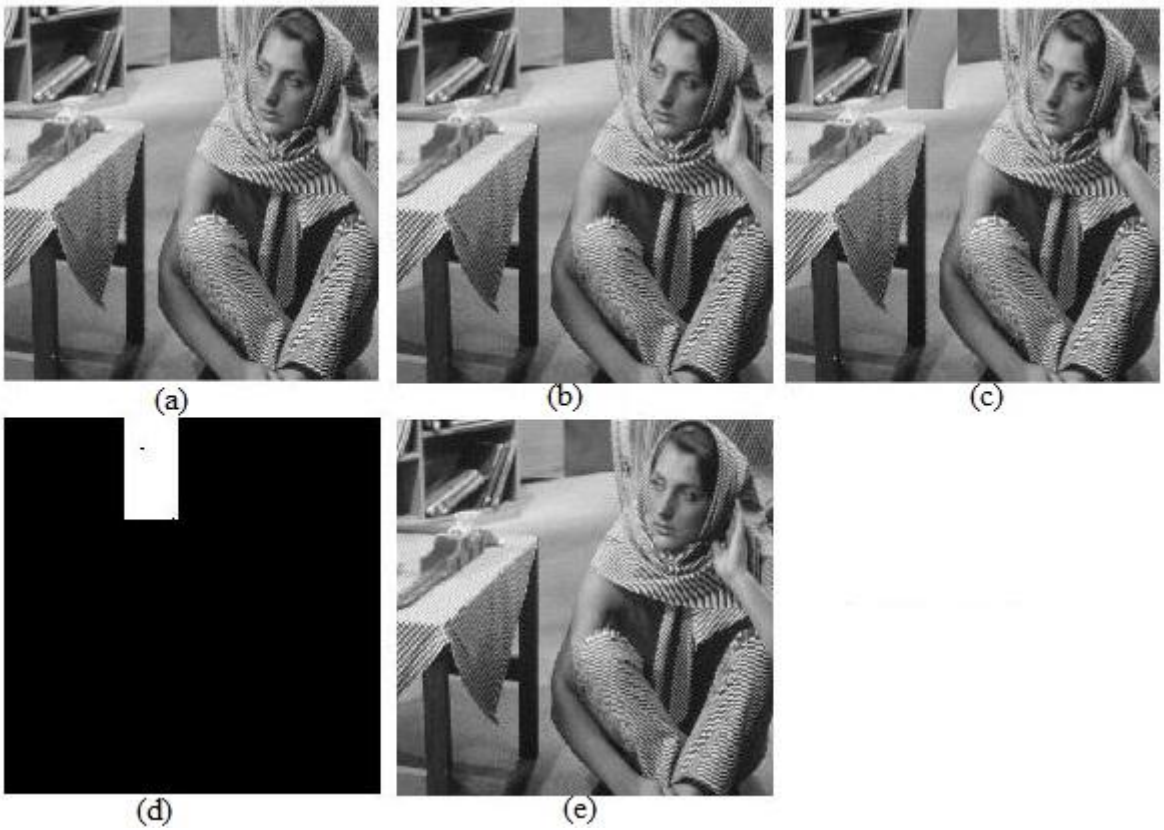

Figure-5.4: Copy-paste attack Barbara for proposed scheme (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization, (e) recovered image

At the End, the results shows that tamper localization detection for reference scheme [4] is good enough but its self-recovery of tampered image is not up to the mark.

5.1.2 Text Addition Attack

Standard MATLAB images Airplane and Barbara are used for text addition attack. A text message “Airplane F-16” is added to watermarked Airplane image and text message “Barbara” is added to watermarked Barbara image.

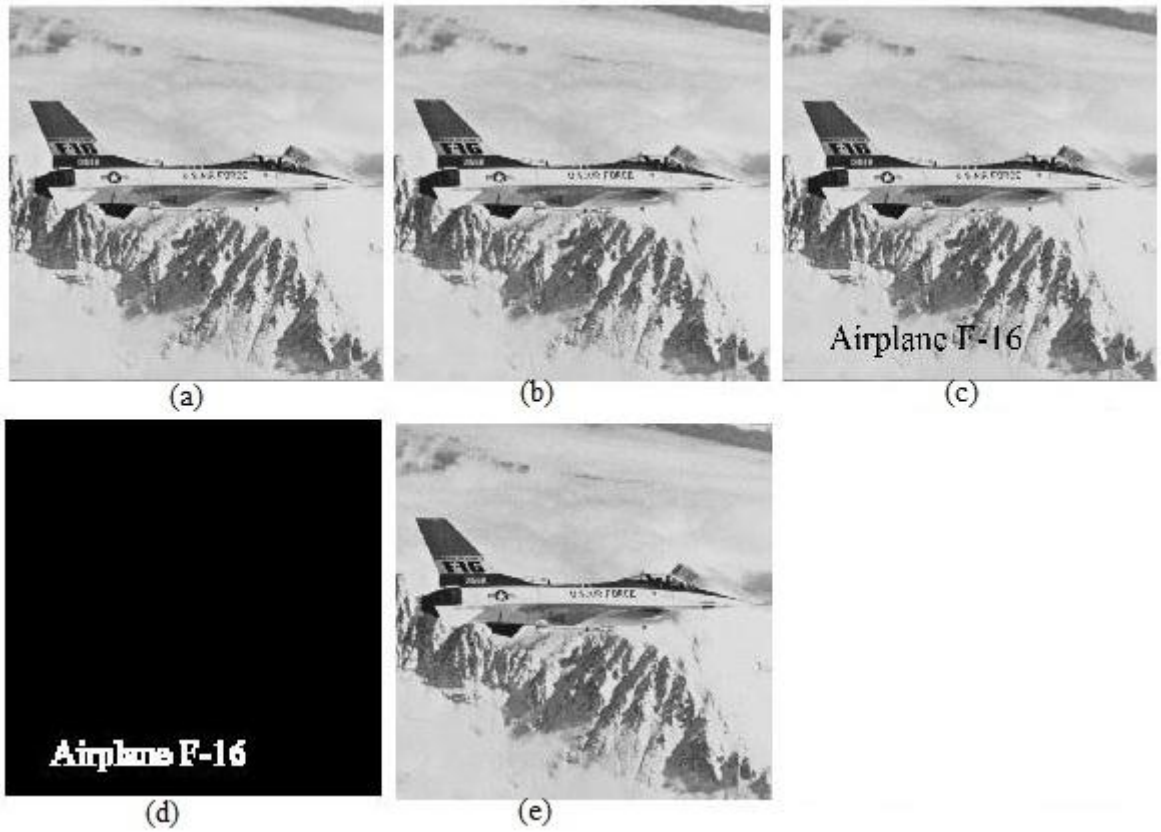

Figure-5.5: Test addition attack Airplane on reference scheme [4], (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization, (e) recovered image

Results for text addition attack on Airplane image for previous scheme [4] are shown into figure 5.5. The recovered PSNR is 41.32 dB.

Figure 5.6 shows the proposed scheme against the text addition attack. The recovered PSNR for extracted image is 40.44 dB. Surprisingly, the recovered PSNR of previously proposed scheme [4] is found better the proposed scheme which was not expected.

For further comparison, text addition attack is performed on Barbara image. And the recovered PSNR of proposed scheme is found to be 36.68 dB where the recovered PSNR of previous scheme [4] is found to be 35.23 dB.

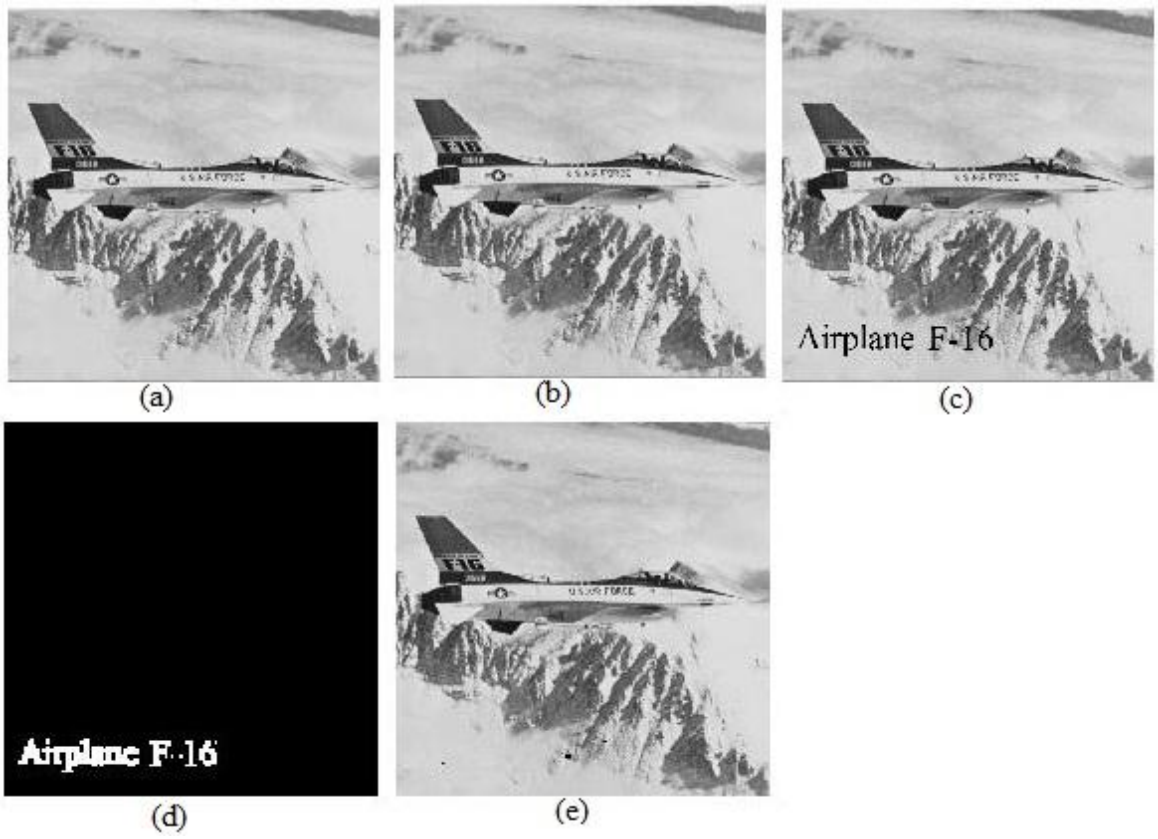

Figure-5.6 Text addition attack Airplane on proposed scheme (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization, (e) recovered image

5.1.3 Content Removal Attack

For content removal attack, a slight part of watermarked image is removed from it. MATLAB standard images Lena and Barbara are our test images for content removal attack.

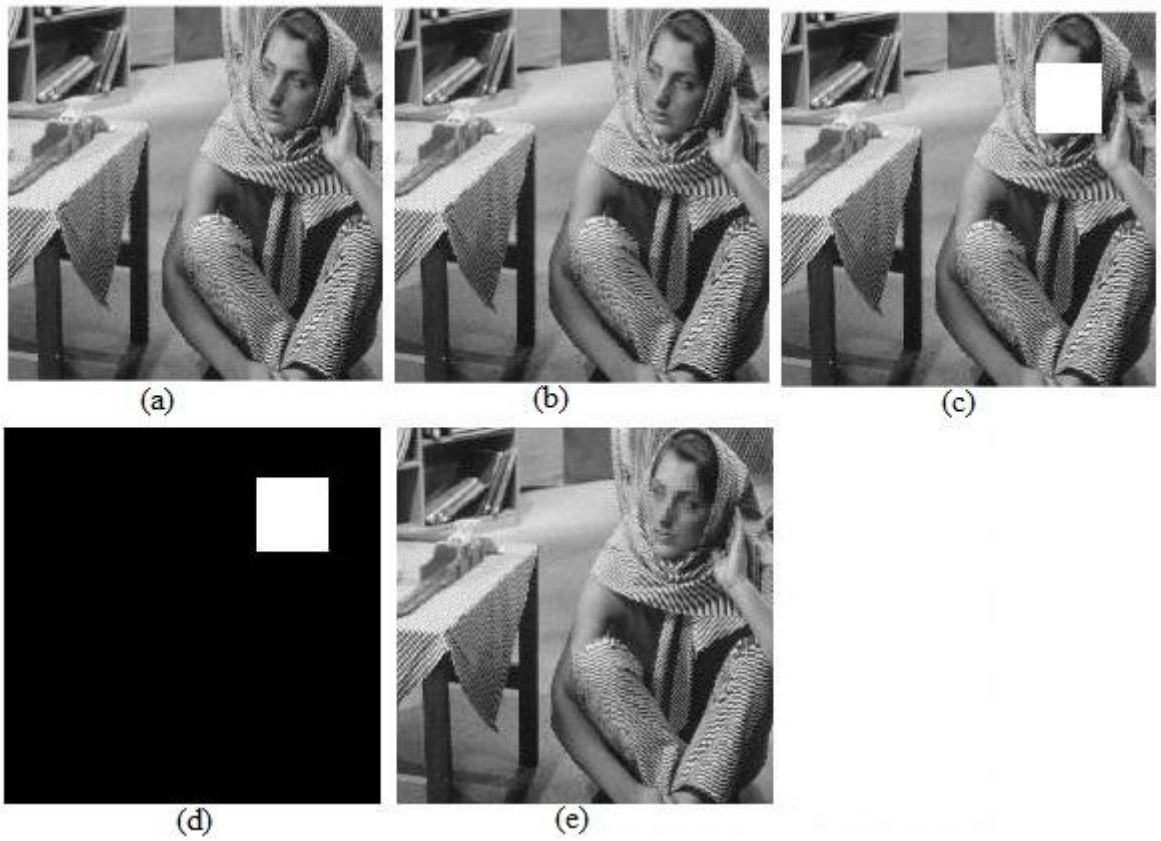

Figure-5.7: Content removal attack Barbara reference scheme [4] (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization, (e) recovered image

Figure 5.7 shows a content removal attack for reference scheme [4]. Tamper localization detection is good enough but still a little blur-ness can be seen in recovered image at tampered regions. A PSNR of 38.41 dB is found for the recovered tampered regions.

Figure 5.8 shows a content removal attack for proposed scheme. Tamper localization detection for proposed scheme is exceptionally good and a better recovery of tampered regions is found for proposed scheme. A PSNR of 41.98 dB is found for the recovered tampered regions.

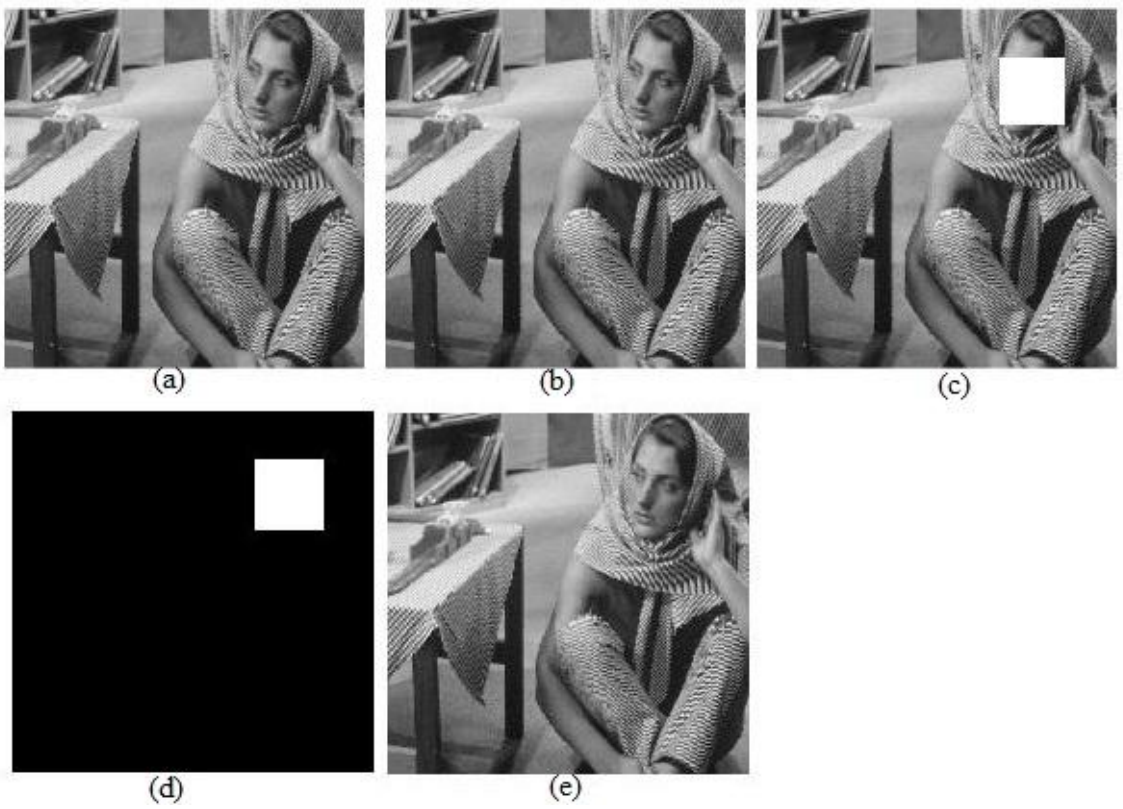

Figure-5.8: Content removal Barbara on proposed scheme, (a) host image, (b) watermarked image, (c) tampered image, (d) tamper localization detection, (e) recovered image

Content removal attack is also performed for Lena image where a PSNR of 35.08 dB and 37.95 dB is found for previous scheme [4] and proposed scheme respectively.

5.1.4 VQ attack

A VQ attack is also performed for test image Lena which is tampered with copy and paste attack with another image content watermarked using the same scheme. Recovered PSNR of 38.81 dB and 40.16 dB is found for previous scheme [4] and proposed scheme respectively.

5.2 Comparison with different level of tampering

In addition to the previous results a more descriptive results are presented in this section. A total of four 256*256 standard images are used for comparison of both scheme. A detailed comparative results against copy and paste attack and text addition attack are shown in to the table 5.2 and table 5.3 respectively.

5.2.1. Copy and paste attack

Table- 5.2: Comparison against copy and paste attack

Test Images/ Tampered regions	Reference Scheme [4] recovered PSNR (dB)			Proposed Scheme recovered PSNR (dB)		
	10%	25%	50%	10%	20%	50%
Airplane	40.63	35.94	24.31	41.21	39.41	28.75
Boat	32.32	26.34	24.59	35.59	31.28	29.17
Baboon	30.44	28.78	25.58	33.81	31.50	28.87
Zelda	36.54	34.08	30.88	41.28	38.35	33.75

Table 5.2 is comparative result for both the schemes at three different tampering level i.e. 10%, 20% and 50%. At low tampering level both schemes are equally good enough but as the tampering level increases proposed scheme starts dominating.

A visual comparative result for ‘Zelda’ test image at 50% copy and paste attack for both schemes is shown in figure 5.8 and figure 5.9, where figure 5.8 shows tamper localization detection and figure 5.9 shows recovered images for both scheme.

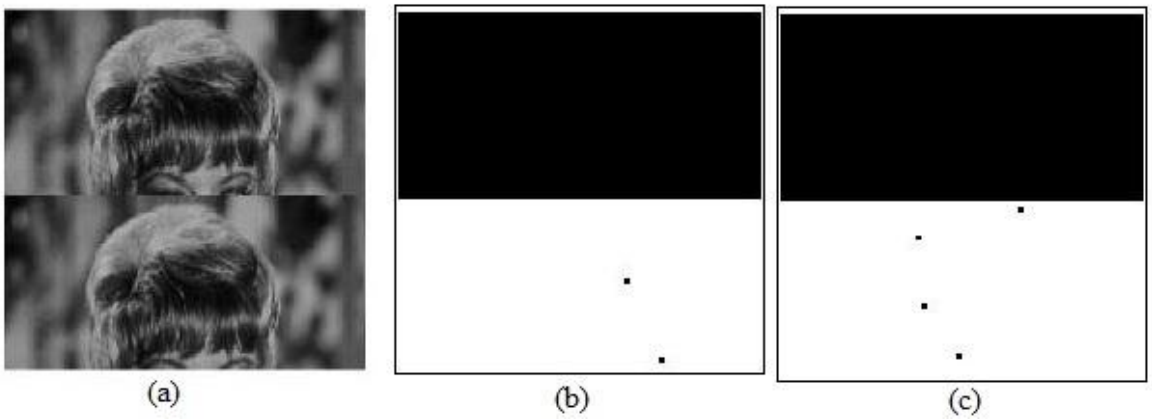

Figure-5.9: Tamper localization Zelda at 50% tampering (a) Tampered image, (b) reference scheme [4], (c) proposed scheme.

Figure-5.10: Recovered image Zelda at 50% tampering (a) host image, (b) reference scheme [4], (c) proposed scheme

Difference between recovered images for both the schemes can be clearly seen in figure 5.9. But a better tamper detection is found for reference scheme [4]. The problem for better tamper detection can be resolved further with a better mapping of SVD generated trace.

5.2.2. Text addition attack

Table 5.3 is a comparative result for different font size texts. Similar to the copy and paste attack proposed schemes provided more dominating results over regular scheme.

Table-5.3: Comparison against text addition attack

Test Images/ Text Font Size	Reference scheme [4] recovered PSNR (dB)			Proposed scheme recovered PSNR (dB)		
	16	24	28	16	24	28
Airplane	40.38	36.79	35.26	41.60	37.81	40.01
Boat	43.03	41.30	41.00	43.02	43.47	43.19
Baboon	38.86	36.07	34.48	41.10	39.08	38.36
Zelda	43.58	43.17	42.71	44.30	44.18	42.28

5.3 Chapter Summary

The results for proposed scheme are better than the reference scheme [4]. Due to the 12 bit of authentication information in reference scheme [4] it provides a range in between 1 to 2048 for authentication information so chances of overlapping are less and scheme has a better tamper detection. While the proposed scheme has 8 bit of authentication bit information where closer data may overlap.

Despite of a higher tamper detection for the reference scheme [4], proposed scheme provides a better self-recovery over reference scheme [4]. In addition to it, with a proper mapping of authentication information can reduce the chances of overlapping and will provide a better tamper detection.

Chapter-6:

Proposed Scheme over Color Images

Performance analysis for both schemes shows that the proposed scheme provides a better self-recovery than the reference scheme. Moving forward for self-recovery of images, the proposed scheme is being tested against color images. The scheme is tested against different copy-paste attack, text attack and VQ attack. Later the scheme is also tested against some bigger size random images.

6.1 Color images against Different types of attacks

To perform the proposed scheme over color images three 256*256 color images are selected. The PSNR based results against different type of attacks for all test images are shown in table 6.1.

Table-6.1: Recovery of tampered color image against different types of attacks

	Test images	PSNR of watermarked image (dB)	PSNR of recovered image (dB)
Copy-paste attack	Lena	44.28	33.66
	Baboon	44.43	35.85
	Airplane	43.79	42.79
Text addition	Baboon	44.43	37.18
VQ attack	Lena + Baboon	41.28	37.20

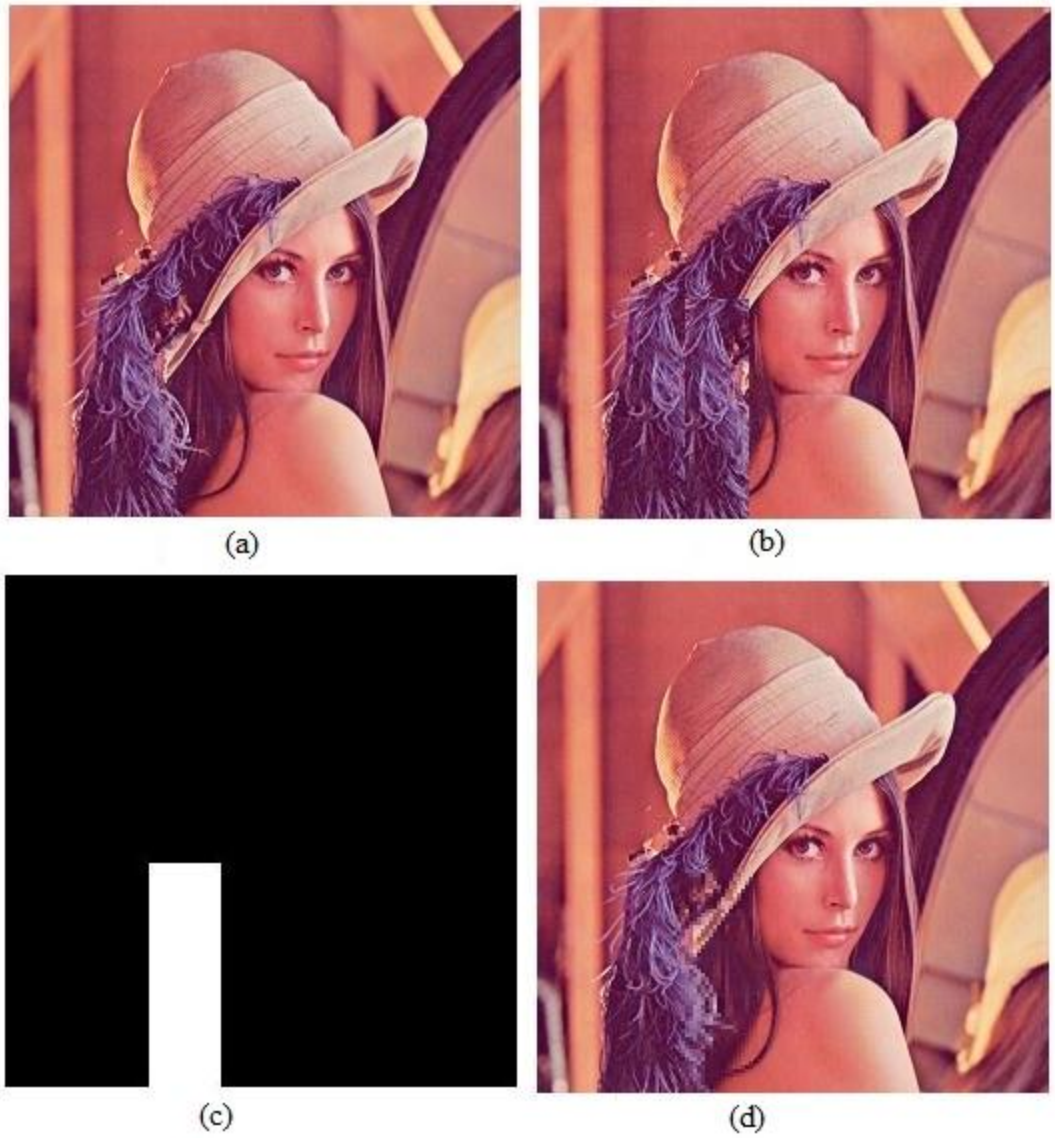

Figure-6.1: Copy-paste Lena color image (a) host, (b) tampered image, (c) tamper localization, (d) recovered image

Test results for Lena color image are shown in figure 6.1 where extra hair has been added in watermarked image. The image is successfully recovered with 100% tamper localization.

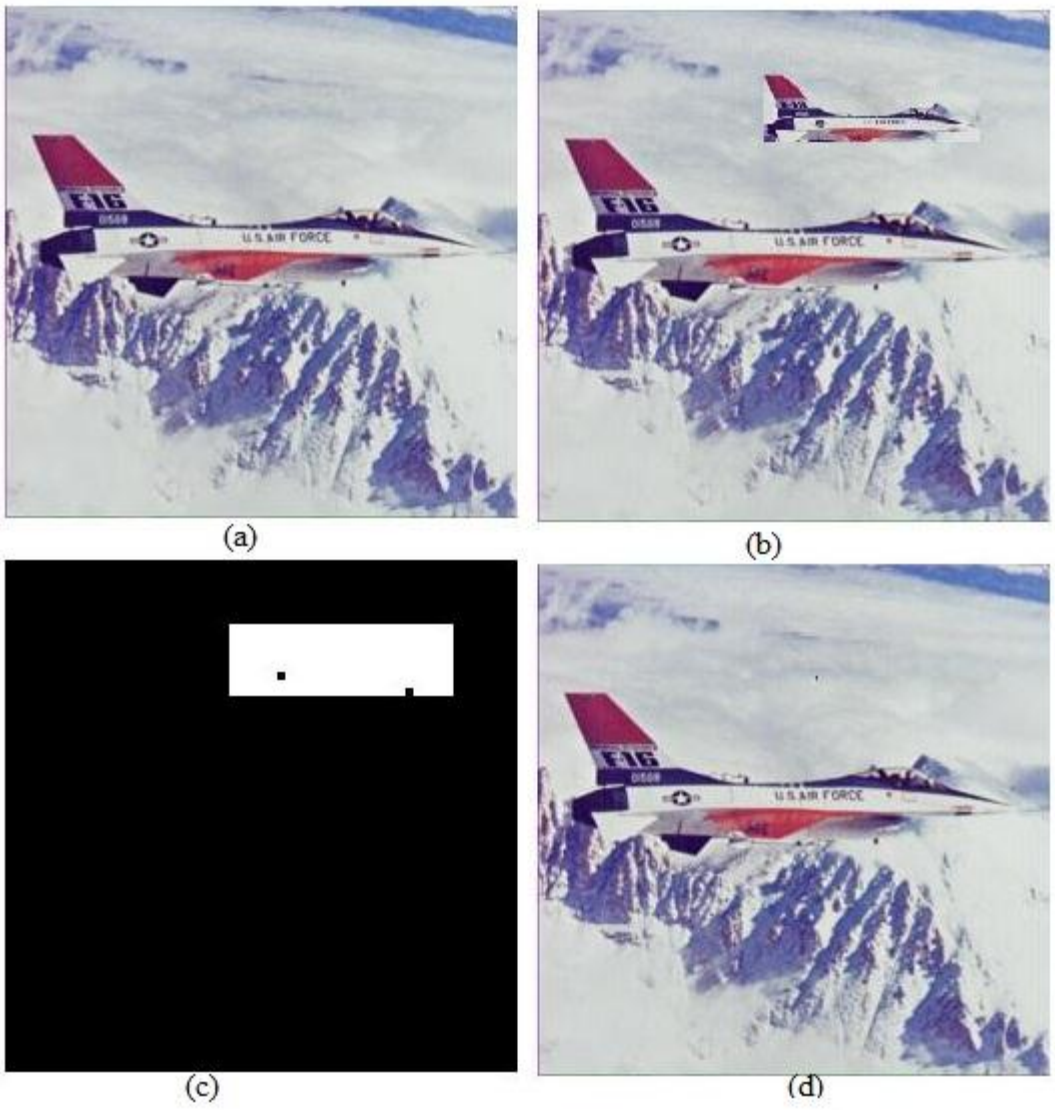

Figure-6.2: Copy-paste attack Airplane color image, (a) host, (b) tampered, (c) tamper localization, (d) recovered image

Figure 6.2 shows a copy paste attack over Airplane image. For this an additional plane is copy pasted in watermarked image. Tamper localization and its corresponding recovered image are shown in figure 6.2 (c) & (d). Recovered image is having high tamper detection where only two blocks were wrongly marked.

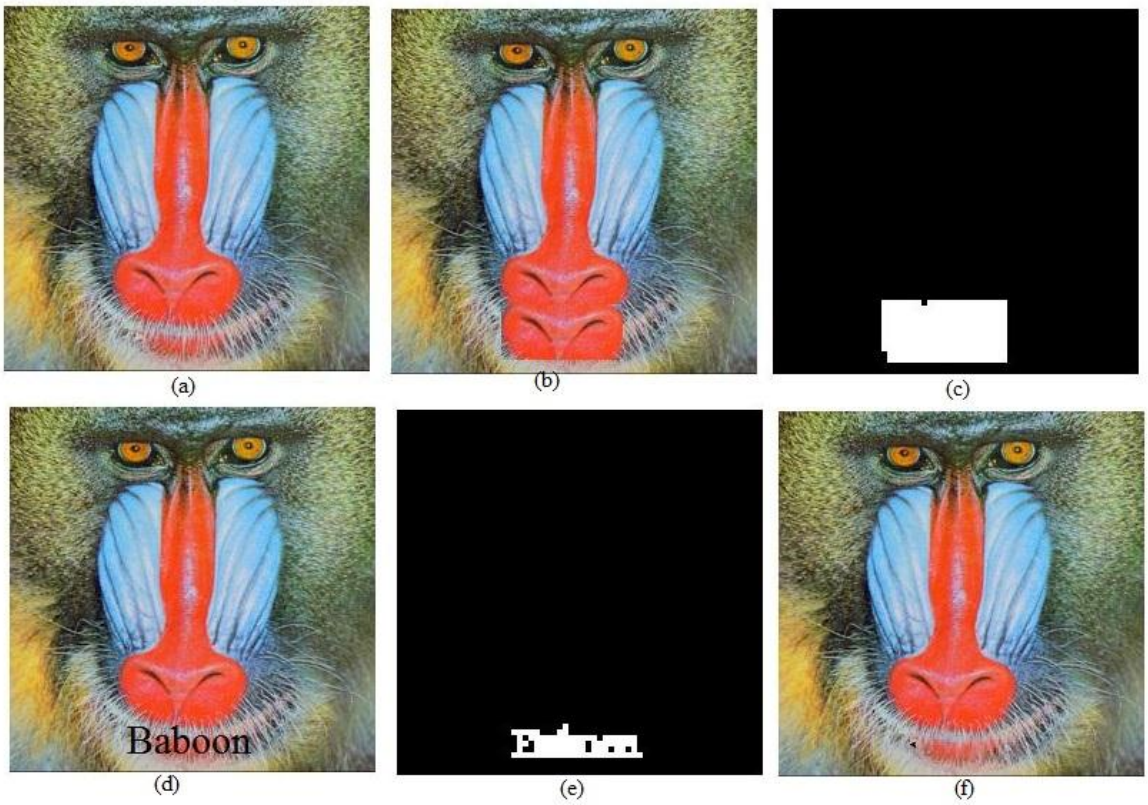

Figure-6.3: Different attacks Baboon color image, (a) host, (b) copy attack, (c) tamper localization copy attack, (d) text addition, (e) tamper localization text addition attack, (f) recovered image

Both copy-paste and text addition attacks are performed on Baboon image. A nose is copy-pasted to form a false image. Similar a text ‘Baboon’ is added to watermarked image.

Tamper localization and recovery of tampered regions for both attack are shown in figure 6.3. Again the tamper localization detection was good with only two wrongly marked blocks.

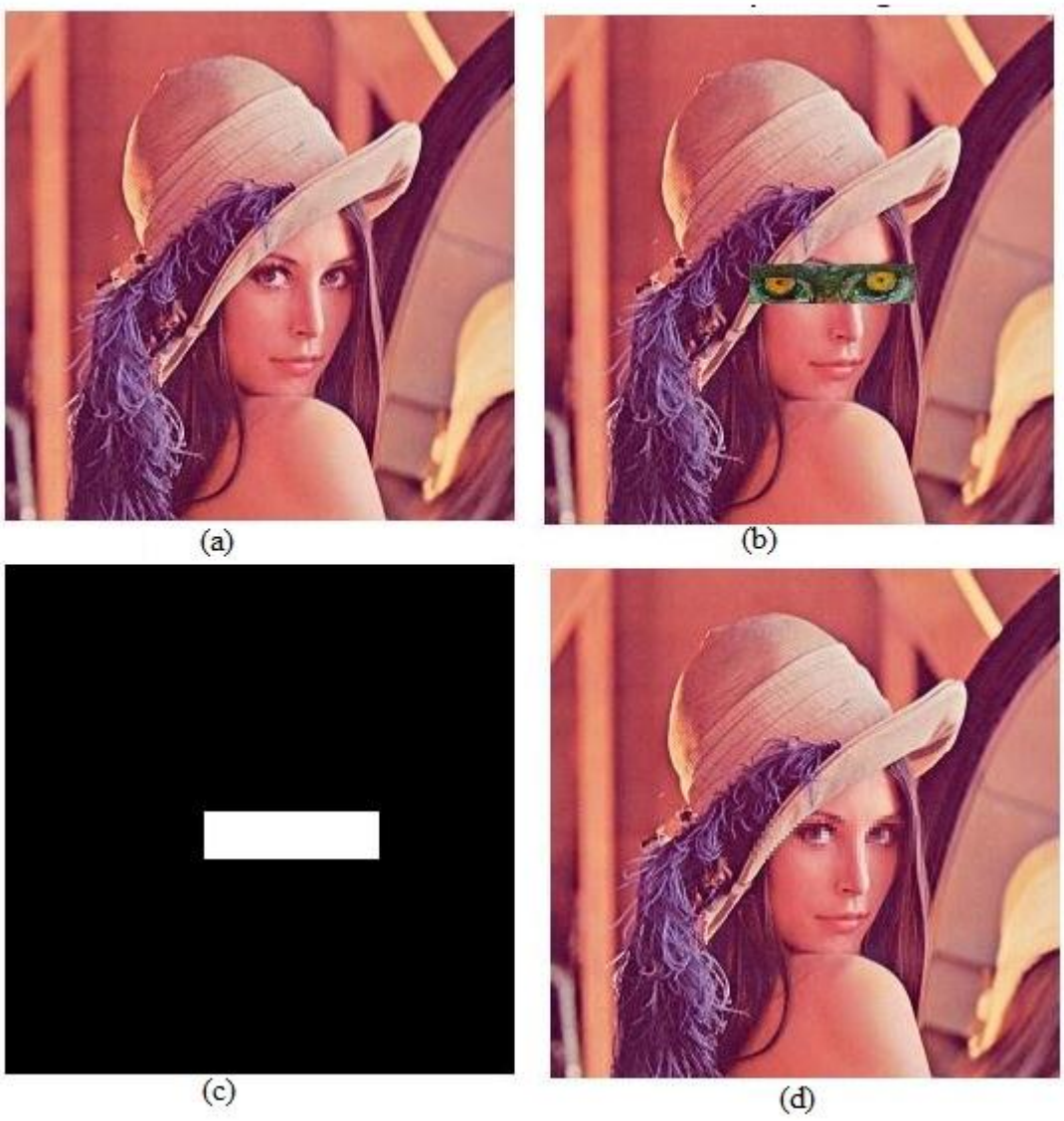

Figure-6.4: VQ attack on Lena, (a) host, (b) tampered, (c) tamper localization, (d) recovered image

To perform VQ attack is part of watermarked Baboon is taken out and is pasted over Lena image. Then the proposed scheme is performed over it.

The tamper localization detection and recovered image are shown in figure 6.4. None of the altered image was wrongly marked.

6.2 Different attacks against random size color images

The proposed scheme has a limitation i.e. the host image size should be a multiple of 8. In such case if a host image is not multiple of 8 then the image is increased to its nearest multiple of 8. The proposed scheme is performed on three test images and there corresponding results are shown in table 6.2.

Table-6.2: Effect of proposed scheme on random image size

Types of attack	Test images (row*col)	PSNR of watermarked image	PSNR of recovered image
Copy and paste attack	Peppers (384*512)	44.05	41.54
	Dog (250*311)	44.39	38.71
	Apple (313*507)	44.35	33.81
Text addition attack	Peppers (384*512)	44.05	44.04
	Dog (250*311)	44.39	40.51
	Apple (313*507)	44.35	40.71

Results for all three test images i.e. Peppers, Dog, Apple are shown in figure 6.5 to figure 6.7 respectively. Recovered image quality is good enough for all three images as shown in figure 6.5 to 6.7.

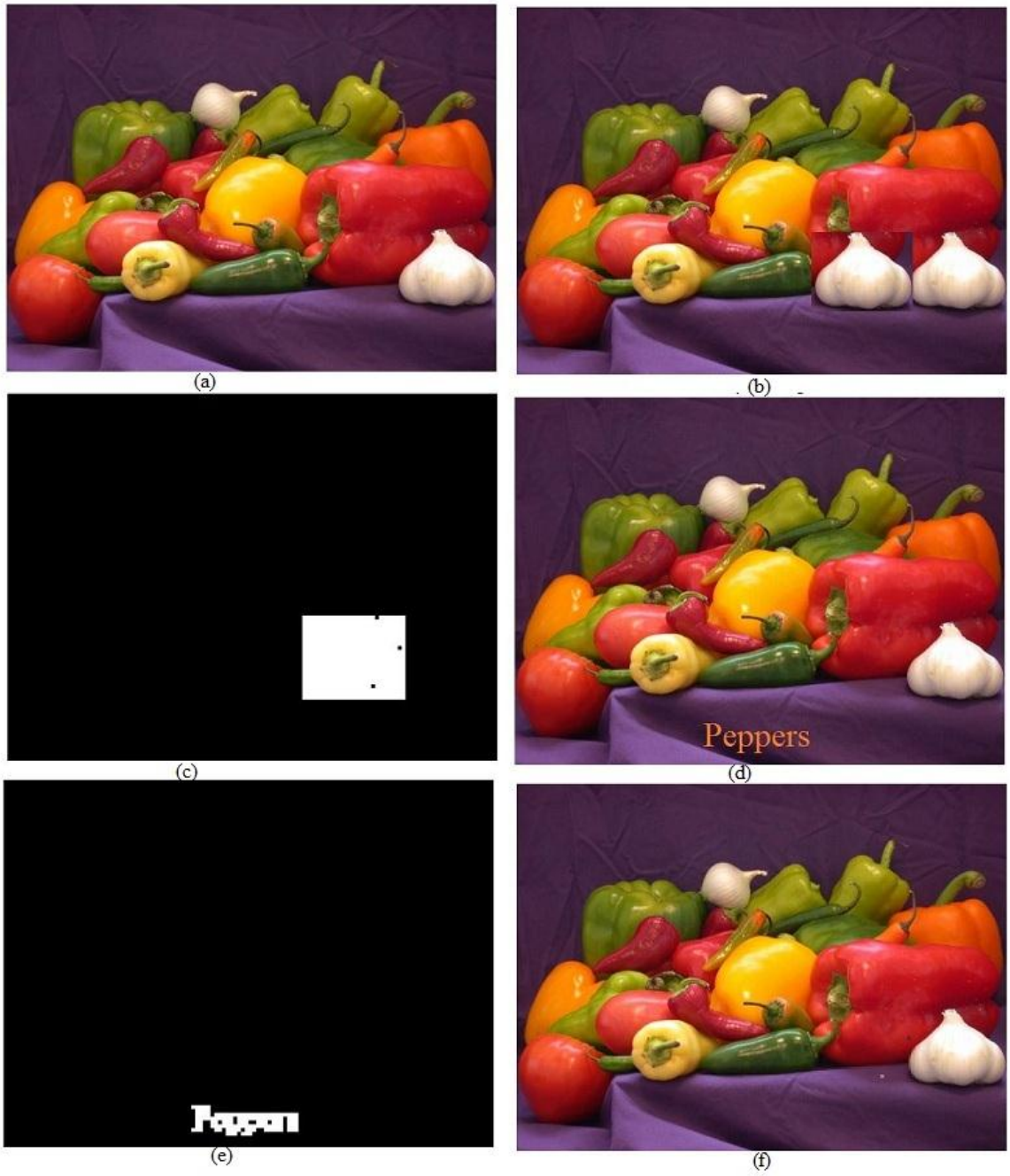

Figure-6.5: Copy-paste and text addition attack on Peppers, (a) host, (b) copy-paste attack, (c) temper localization copy-paste attack, (d) text addition attack, (e) tamper localization text addition attack, (f) recovered image

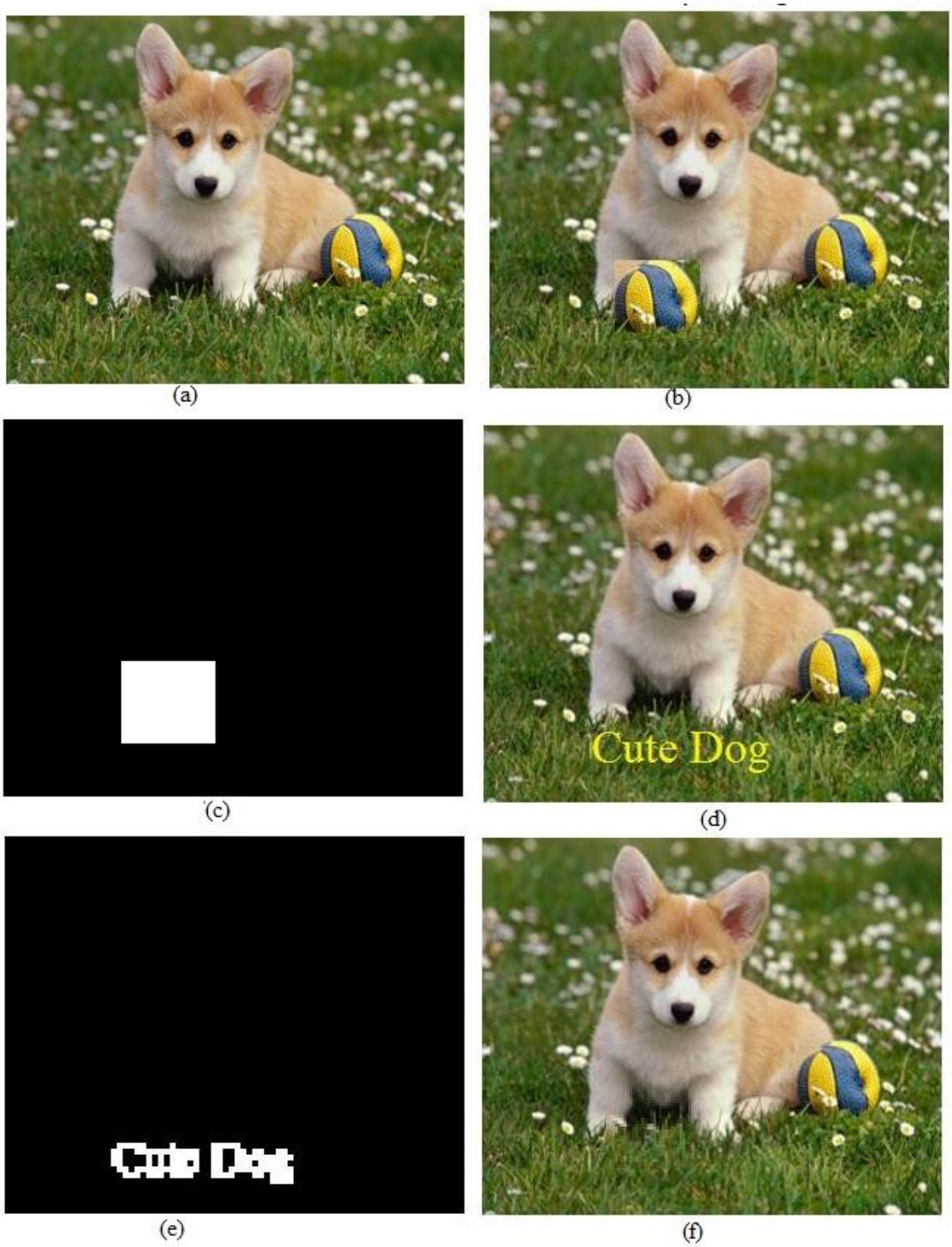

Figure-6.6: Copy-paste and text addition attack on Dog, (a) host, (b) copy-paste attack, (c) temper localization copy-paste attack, (d) text addition attack, (e) tamper localization text addition attack, (f) recovered image

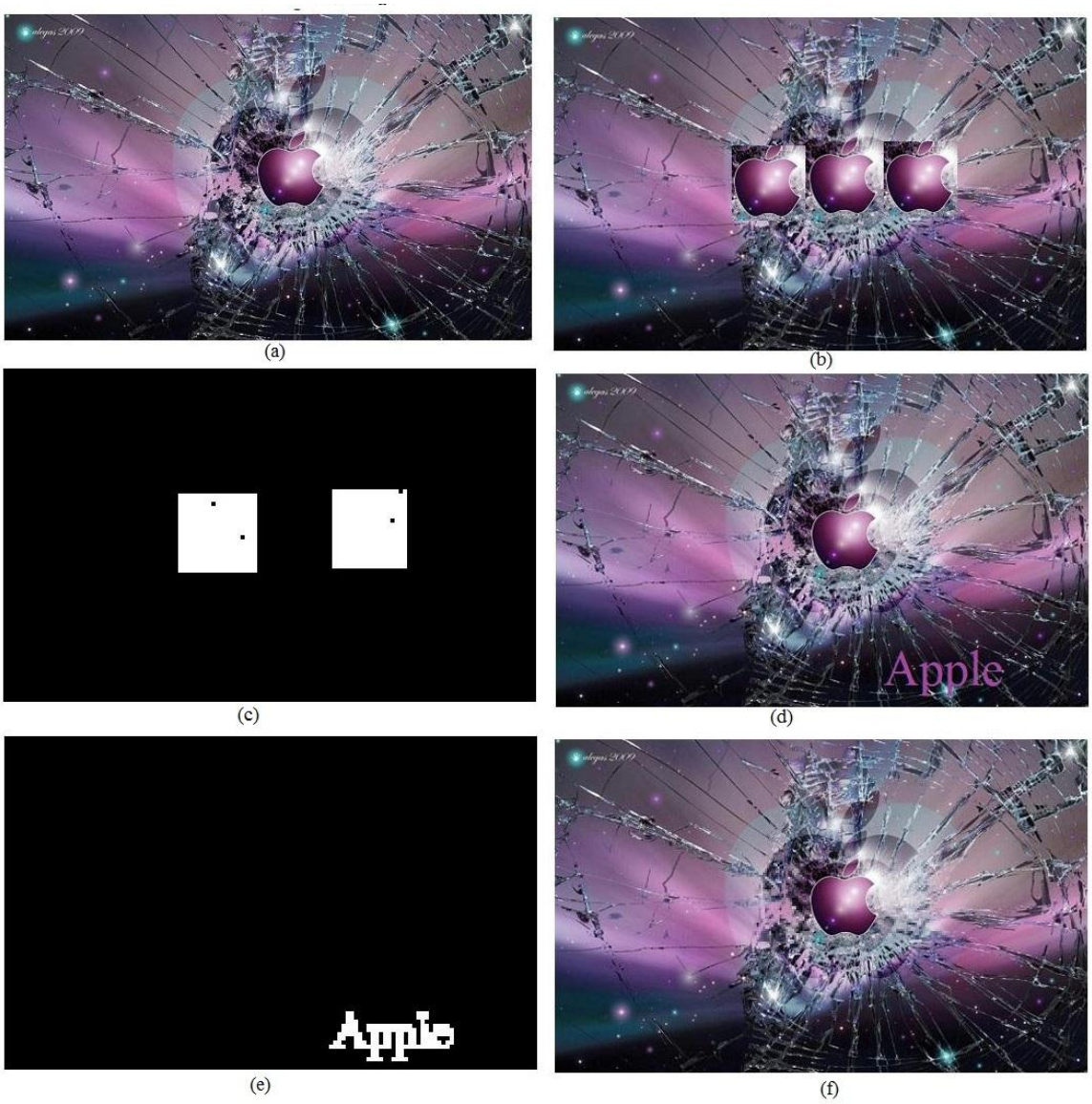

Figure-6.7: Copy-paste and text addition attack on Apple, (a) host, (b) copy-paste attack, (c) temper localization copy-paste attack, (d) text addition attack, (e) tamper localization text addition attack, (f) recovered image

Chapter-7:

Conclusion & Future Work

This thesis presents a SVD based semi fragile watermarking scheme for image tamper localization detection and self-recovery of the tampered regions as an improvement to my reference. For the above context the proposed scheme uses a combination of Block authentication bits to check altered regions and self-recovery bits to recover the tampered region. Block authentication bits are calculated with the help of SVD for each 4x4 block while self-recovery bits are calculated by average value computation for each 2x2 sub-block.

Chapter 5 gives a complete performance analysis for both reference scheme [4] and suggestions for improvement. Where the proposed scheme clearly wins with more self-recovery bits. Although the proposed scheme is found to be a bit lazy in tamper detection because of less authentication bit information (only 8 bits). But the results are improved by proper mapping of authentication information generated by SVD algorithm. Later the proposed scheme is also performed against color images and results were quite acceptable.

Even though the proposed scheme gives a better results compare to the reference scheme [4] but still a lot can be improved. Image resizing and image rotation are such problems which need to be solved. This is going to be my future work.

References

1. C.Rajalakshmi, Dr.M.Germanus Alex, Dr.R.Balasubramanian, "Study of image tampering and review of tampering detection techniques", International Journal of Advanced Research in Computer Science, Volume 8, No. 7, July – August 2017.
2. R. Hamza, K Muhammad, Z. Lv, "Secure video summarization framework for personalized wireless capsule endoscopy", Pervasive Mobile Comput. Vol 41, pp. 436-450, Oct 2017.
3. R. Hamza, K Muhammad, A. Nachiappan, "Hasn Based encryption for keyframes of diagnostic hysteroscopy", IEEE Access, 2017.
4. A Shehab, M Elhoseny, K Muhammad, "Secure and robust ragile watermarking scheme for medical images", IEEE Access, Feb 2018.
5. S Rawat, B Raman, "A chaotic based fragile watermarking scheme for image tamper detection", AEU Int. J. Electron. Commun, 2011.
6. X. Zhang, S. Wang, "Statistical fragile watermarking capable of locating individual tampered blocks", IEEE Signal Process., Oct. 2007.
7. V. Dhole, N. Patil, "Self embedding fragile watermarking for image tampering detection and image recovery using self-recovery blocks", ICCUBEA, Feb. 2015.
8. B.Patra, J. Patra, "Crt- based fragile self-recovery watermarking scheme for image authentication and recovery", ISPACS, Nov. 2012.
9. M. Elarbi, C. Amar, "Image authentication algorithm with recovery capabilities based on neural networks in DCT domain", IET Image Processing, 2011.
10. R. Liu, T. Tan, "An SVD based watermarking scheme for protecting rightful ownership", IEEE Trans. Multimedia, 2002.
11. R.Sun, H. Sun, A. Yao, "A SVD and quantization based semi fragile watermarking technique for image authentication", Int. Conf. Signal Process., Aug. 2002.
12. [Online] https://sisu.ut.ee/imageprocessing/book/3

13. [Online] https://www.engineersgarage.com/articles/image-processing-tutorial-applications.

14. Weiss, W. Historische Wasserzerchen. Saur, 1987.

15. Liu, T. and Qiu, Z. The survey of digital watermarking-based image authentication techniques. In Proc. of the 6th Int. Conf. on Signal Processing, 2002, 1556-1559.

16. Watermarker.com. 2004. http://www.watermarker.com/watermark-protector/watermark-examples.aspx, Sep.2005.

17. Hartung, F. and Kutter, M. Multimedia watermarking techniques. IEEE Special Issue on Identification and Protection of Multimedia Information, 87, 7 (1999), 1079-1107.

18. [Online] https://machinelearningmastery.com/singular-value-decomposition-for-machine-learning/

19. [Online] https://en.wikipedia.org/wiki/Singular_value_decomposition

20. L. Wu, J. Zhang, W. Deng, D. He, "Arnold transform algorithm asnd anti-Arnold transform algorithm", IEEE Int. Conf., Dec. 2009.