Thesis- A Noble Authentication Model Using SHA3-512 Hash Function and 8-Directional Pixel Selection Technique of LSB Based Image Steganography

By

Thanbir Alam Sk.
(161-35-1451)

Supervised By

Md. Maruf Hassan

Assistant Professor

Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall – 2019

APPROVAL

This thesis titled on "**A Noble Authentication Model Using SHA3-512 Hash Function and 8-Directional Pixel Selection Technique of LSB Based Image Steganography**", submitted by **Thanbir Alam Sk.**, **161-35-1451** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

-- **Chairman**
Prof. Dr. Touhid Bhuiyan
Professor and Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

-- **Internal Reviewer**
Dr. Md. Mostafijur Rahman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

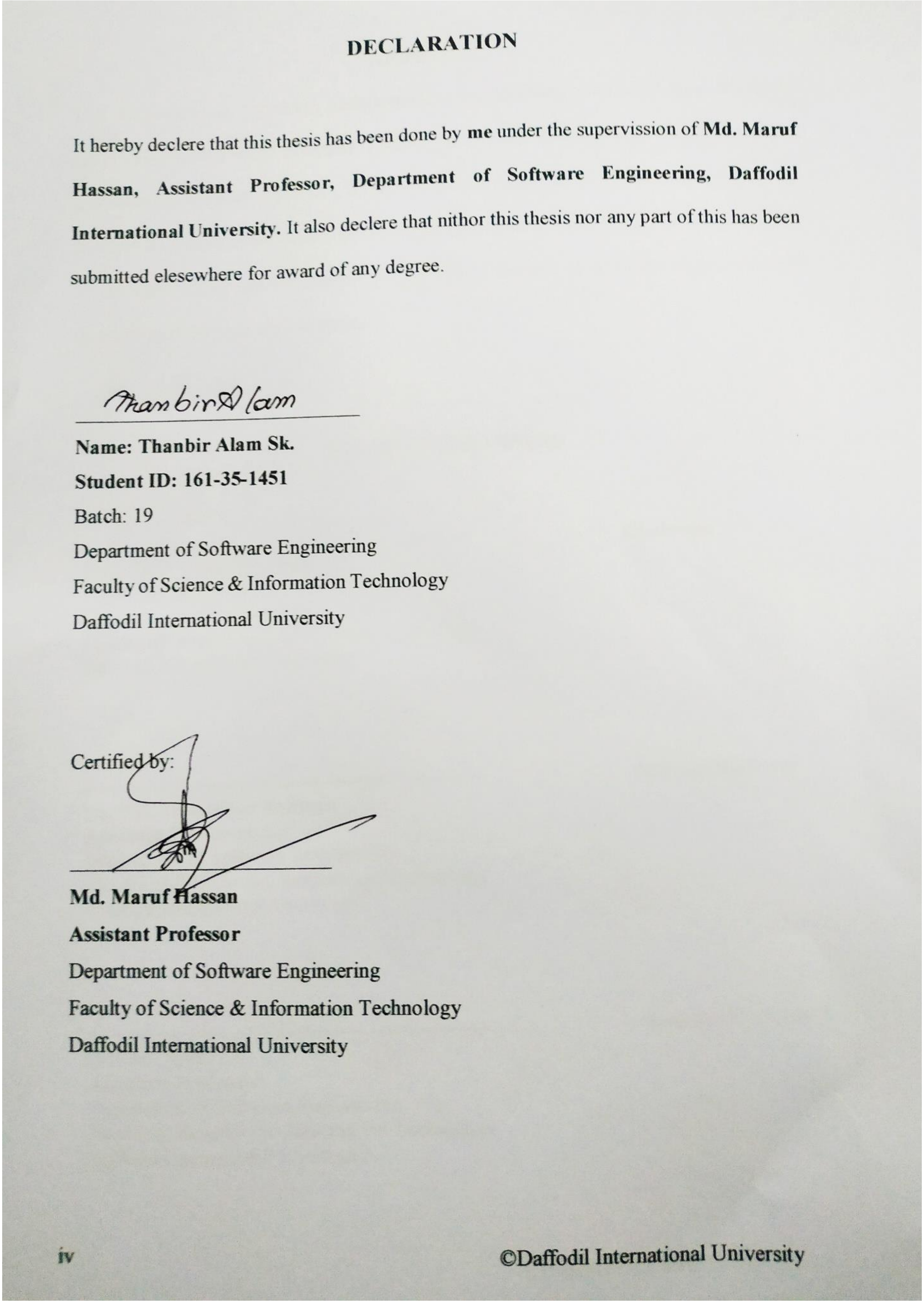
-- **Internal Examiner 1**
Dr. Md. Asraf Ali
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

-- **Internal Examiner 2**

Asif Khan Shakir
Lecturer
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

-- **External Examiner**

Dr. Md. Nasim Akhtar
Professor
Department of Computer Science and Engineering
Faculty of Electrical and Electronic Engineering
Dhaka University of Engineering & Technology, Gazipur



DECLARATION

It hereby declere that this thesis has been done by **me** under the supervission of **Md. Maruf Hassan, Assistant Professor, Department of Software Engineering, Daffodil International University.** It also declere that nithor this thesis nor any part of this has been submitted elesewhere for award of any degree.

Thanbir Alam

Name: Thanbir Alam Sk.
Student ID: 161-35-1451
Batch: 19
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Certified by:

Md. Maruf Hassan
Assistant Professor
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

ACKNOWLEDGEMENT

I have taken endeavors in this thesis. Be that as it may, it would not have been conceivable without the kind help and help of numerous people. I might want to stretch out my earnest because of every one of them. I am exceptionally obligated to Daffodil International University for their direction and steady supervision by **Md. Maruf Hassan** and in addition for giving necessary information with respect to the venture and additionally for their help in finishing the task. I would like to express my gratitude towards our parents, our batch mate, member of DIU for their kind co-operation and consolation which help us in finishing of this task. I might want to offer my exceptional thanks and on account of industry people for giving me such consideration and time. My thanks and thanks likewise go to my associate in building up the venture and individuals who have energetically bailed us out with their capacities.

TABLE OF CONTANT

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

In this paper we represent the web-based authentication security system which uses Image Steganography and SHA3-512 hashing function. Our developed web authentication system encrypts user's password with SHA3-512 hashing function which hides into a cover image is called image steganography. Pixel selection for data hiding becomes crucial for the solutions in spatial domain of image steganography to ensure imperceptibility. This paper also presents an efficient approach of pixel selection technique for hiding secret data in cover object of image steganography. After reviewing recent literature, it has been observed that most of the works on pixel selection uses zig-zag technique for their solution. However, it becomes very prone to steganalysis based attacks by the intruders. In this study, 8-directions pixel selection technique is proposed to embed data in the cover image where Least Significant Bit (LSB) method has been used on Red, Green and Blue (RGB) color image especially focused on JPG, JPEG, and PNG. Since this projected procedure avoids the known steganalysis techniques, it will be challenging for the attacker to recognize the presence of secret information from the stego image. To measure the quality, statistical analysis has been performed where the value of the quality measurement matrices has provided better results. We endorse this security for forthcoming web applications of the future that will be handling subtle user information.

Keywords: Authentication, Image Steganography, SHA3-512, Pixel selection technique, LSB

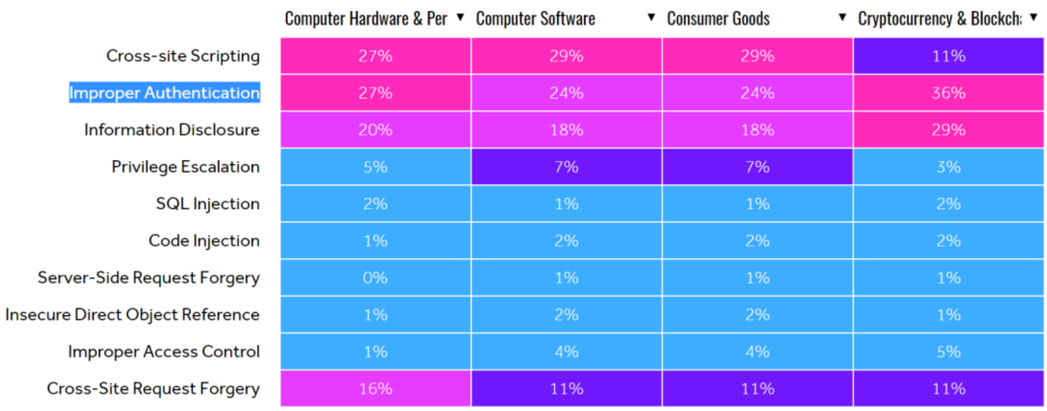
CHAPTER 1

INTRODUCTION

1.1 Background

With rapid advancement in technologies a lot of secret data is transmitted over the internet but at the same time security is a major issue of today's world. The information which is transacted between sender and receiver through over internet need to secure from attacks caused by intruders. Without proper security sustained, data transfer and all kinds of secret information over the Internet can be a big risk which can be a reason of data loss, exploitation or theft. The world is suffering a high rise in cybercrime and therefore data security needs to be always up to date for the reason that data requires high protection and appropriate security for transmitting over the Internet (Mogale et al., 2018). Data needs to be first concealed with proper security before sending it over the Internet or any data transmitting mediums that operates client side of web application. To reduce this problem a number of cyber security techniques have been developed under information encryption and information hiding to address the security of information. Information encryption technique is known as cryptography that convert the secret message into unintelligible message. Traditionally, the major online applications are used cryptography hash functions in the password-based authentication process. Cryptography hash function is a one-way encryption function, which is a set of mathematical formula or well- defined procedures which is represent a fixed size of bits that created from a file of big sized, the result of this function is called hashes or hash code. The hash code generating is faster than Symmetric-key cryptography and Public-key cryptography because it is one-way function. Therefore, it much expected for integrity and authentication in this present time (Malalla et al., 2016; Shalilendra et al., 2013) and it is highly required because of cheap constructions. Recently, the use of hash functions become a typical approach for authentication in different applications. The authentication considered an important matter in secure the data. However, cryptographic techniques-based authentication is a great challenge in client-server system. Password based authentication system is one of the simplest and the most common authentication mechanism over an insecure channel/protocol/medium which provides the legal users to use the resources of server. Many researchers proposed quite a lot of password authentications schemes for secure registration and login process. However, the present Internet environment is susceptible to several attacks such as modification attack, guessing attack, replay attack and stolen-verifier attack (Gupta et al., 2015). However, cryptographic techniques-based authentication not only measure to secure while steganography can provide extra security in the authentication process which hides the existence of message by using another cover media without noticing to anyone. "Steganography" is a Greek word which is combined into two parts: Steganos which means "covered" (where a technique hides the secret messages) and the Graphic which means "writing". The very first steganographic (Judge & James, 2001) approach was developed in antique Greece around 440 B.C. In recent years, many researchers have been introduced different image steganography approaches in digital media (Singla et al., 2018; B. Feng et al., 2015; K.L. Chiew et al., 2010; L.C. Kang et al., 2010; Tiwari et al., 2010; L.C. Kang & J. Pieprzyk, 2010; J Chen et al.,2010; Kadhim & I. J., 2012; B. Feng et al., 2017; Cheddad et al., 2010; Ashwin et al., 2012; Awad, 2017; Odeh et al., 2015; Thomas, 2013) to hide secret information. It is used in different organizations like military or intelligence agents to communicate with the members. There are several image steganography techniques we found which are used in RGB images, like Least Significant Bit (LSB), Pixel Value Differencing (PVD), Discrete

Cosine Transformation Technique (DCT), Edges Based Data Embedding Method (EBE), Random Pixel Embedding Method (RPE), Mapping Pixel to Hidden Data Method, Labelling or Connectivity Method, Pixel Intensity Based Method (Nagpal et al., 2015; Beroual et al., 2018; Biradar et al., 2016) etc. Therefore, LSB is the most popular and widely used technique for image steganography (Swain, 2019; Al-Shatnawi et al., 2012; M. A. Saleh, 2018) that hides secret bits in the LSB of some pixels of the RGB cover image based on it its binary coding. The advantage of LSB is better as there is less chance for degradation of the original image and more information can be stored in an image (Sahu, 2016; Mahimah & Kurinji, 2013) also it is to embed the bits of the message directly and easily into the LSB of cover-image (Pavani et al., 2013) and stego-image quality is better in LSB. The key benefit of this technique that it provides high embedding capacity. Many researchers work on the same approaches (Khan et al., 2016; Bhuiyan et al., 2019; D.C. Wu & W.H. Tsai, 2003; Mandal & Debashis, 2012; H.C. Wu et al., 2005; Bharti & Soni, 2012; Ali, 2010; Ran & Chi, 2001; Li et al., 2015) which are started embedding from the left most corner pixel of an image as the beginning pixel into cover images. With the advancement of technology, different steganalysis algorithms are developed to compromise those approaches of pixel selection technique in LSB based image steganography. Therefore, pixel selection is an important factor for data embedding (Subhedar et al., 2014) and these selections should be done in such a way that the image will result in minimum distortion. That is, if image quality is not better then it makes the image calm to attack (Al-Shatnawi, 2012). According to (https://www.hackerone.com/top-10-vulnerabilities) improper authentication vulnerabilities' report is given below:



	Computer Hardware & Per ▼	Computer Software ▼	Consumer Goods ▼	Cryptocurrency & Blockch: ▼
Cross-site Scripting	27%	29%	29%	11%
Improper Authentication	27%	24%	24%	36%
Information Disclosure	20%	18%	18%	29%
Privilege Escalation	5%	7%	7%	3%
SQL Injection	2%	1%	1%	2%
Code Injection	1%	2%	2%	2%
Server-Side Request Forgery	0%	1%	1%	1%
Insecure Direct Object Reference	1%	2%	2%	1%
Improper Access Control	1%	4%	4%	5%
Cross-Site Request Forgery	16%	11%	11%	11%

Figure 1: Improper Authentication Report 1

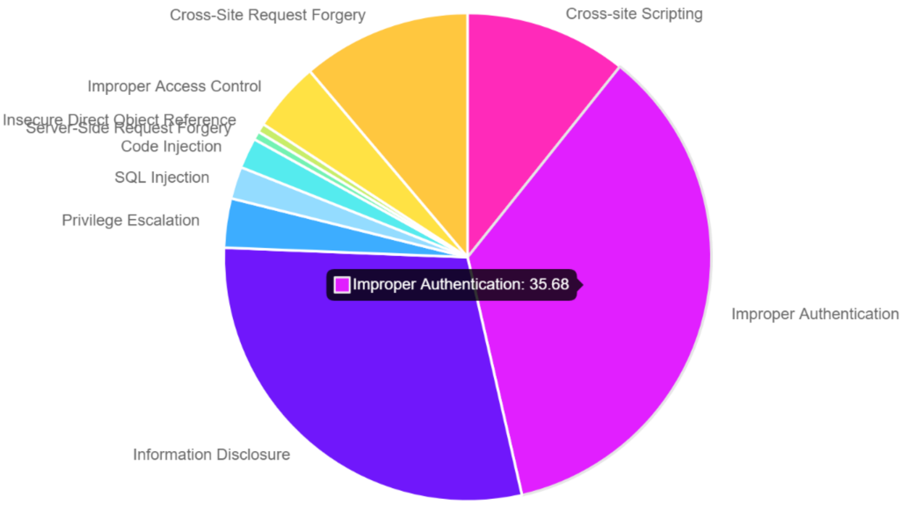


Figure 2: Improper Authentication Report 2

1.2 Motivation of the Research

In recent times, the internet has grown-up to develop a huge technological infrastructure for modern cloud applications. Various organization have now migrated from organizing software and hosting over the internet. They have given their services to customers over the internet and the users transmitting data using those web applications and to identify the users of specific organization, they have used password-based authentication system which is inefficient in present era. In present time, intruders have invented many approaches to compromise authentication system which can be a reason of secret data loss, abuse or theft. The main motivation to develop a secure approach which will provide extra layer in authentication system which is image steganography that is hard to reveal and can minimize gap of pixel selection technique.

1.3 Problem Statement

While reviewing the existing research work, it has been found that many researchers have proposed cryptography and steganography together in authentication but in steganography they have used traditional pixel selection techniques which is easy to perceptibility and intruders can recognize the presence data using steganalysis and in cryptography they have used hash function like MD5, SHA-0, BASE64, SHA-1 which have some weakness which can be break by rainbow table attack, collision attack and, dictionary attack etc.

1.4 Research Questions

1. Question 1: Is the proposed enhanced authentication model effective?
2. Question 2: Is the implemented authentication technique providing better result as compared to the other authentication techniques?

1.5 Research Objectives

- To propose a new 8 directional pixel selection-based image steganography with SHA3-512 cryptographic hash function for authentication in web application.
- To implement this model with better result.
- To compare and evaluate the propose model result with existing model

1.6 Research Scope

A lot of organization is provided their services over the internet to their users. Therefore, to identify their user, authentication plays in vital role. In recent times, intruders have invented a lot of techniques which are able to break down authentication system. However, we have to increase our security in this sector day by day. Therefore, in this area there have a lots of research scope.

1.7 Thesis Organization

In this research, IEEE referencing system has been used in this document. The paper has been furnished with five chapters which is described below:

Chapter 1: In this chapter, research background, motivation, problem statement and objectives are given.

Chapter 2: This chapter includes discussion of the existing related work and figured out the research gap.

Chapter 3: This chapter contains the research methodology and approaches as it follows for the research.

Chapter 4: This chapter compares the experimented results with existing approaches.

Chapter 5: The research outcome and the limitation of this study is presented here and the direction of the future work of the research has also been guided.

CHAPTER 2

LITERATURE REVIEW

While carrying out the research, there are numbers of research has been conducted on image steganography and cryptographic hash for authentication. The discussion of those related work is given below:

2.1 Case Study on Image Steganography

In this study, we present an overview of prior research in the domain of image steganography based on LSB. A well-known LSB based image steganography (Karim et al., 2011) presented a method that utilized the secret key to hide the information into a pixel of cover image where a bit of secret information was placed in either LSB of Green or Blue matrix of a specific pixel was decided by the secret key. However, they used traditional pixel selection technique and they calculated only two image quality measures for a distorted image with a cover image. Bloisi et al. (2007) provided a method that was able to perform steganography and cryptography at the same time which used 8*8 pixel blocks of an image as a cover object for steganography and as key for cryptography also used Huffman coding for embedding but their proposed ISC (Image-based Steganography and Cryptography) algorithm's performance have measured by comparing with only one well-known model (Westfeld, 2001). Thangadurai et al. (2014) discussed about different types of cover file format of LSB technique to hide secret information although they did not discuss about different types of file format's pixel selection techniques. A technique was proposed by Zhu et al. (2013) to hide message in least significant area of pixel of an image where they used edge adaptive image steganography based on LSBMR (least significant bit matching revisited) which utilize the sharper regions within the cover images and embed secret message with higher security, although, in their research article, they didn’t clarify why the PVD histogram of a stego-image will abnormally decrease on the threshold. Khan et al. (2016) represented an LSB technique which hides information in the cover image taking into the pixel value of color or gray level of every pixel and embedded one to four secret message bits into a single pixel by checking several conditions. However, they use several conditions that may take a longer time for embedding. A way of pixel selection is proposed by Sarkar & Karforma (2018) where they firstly selected middle region, then used four diagonal pixels of middle region as successive pixels and embedded the data into four edges of quadrilateral which was created by four diagonal pixels of cover image and finally reached towards the four corners of images. But in their model, as they just used an image quality matric (that was PSNR), as a result the detailed information of image distortion was not known clearly. T. Bhuiyan et al. (2019) proposed a data hiding technique in the spatial domain of image steganography where they proposed a scheme that takes the message bit and performed XOR operation with the 7th bit of every RGB component and, after then, the produced output was embedded within the 8th bit of each component of RGB. However, they used zig-zag pixel selection technique which is traditional/common (Sarkar & Karforma, 2018) pixel selection method, where pixels are selected from the beginning (upper left corner) of images that’s why it’s might easy to recognize the presence of secret data. Aqeel & Raheel (2018) represented a hash based LSB technique was proposed where their model used random hash key for encoding and decoding secret message and the model was embedded 3-bit secret message for RED, 2 bits for GREEN and 3 bits for BLUE portion but their technique provided low image quality. In the above-mentioned schemes most of the researchers worked on traditional zig zag pixel selection technique where attackers can easily recognize the presence of secret data. Even, most of the researchers use only PSNR and MSE to determine the quality between stego and cover image. They did not use different metrics to prove their model well.

2.2 Case Study on Symmetric-key & Public-key Cryptography

In this sub section, A system was provided by Sarmah (2010) where they develop a technique in which cryptography and steganography were used as integrated part along with newly developed enhanced security module. For Cryptography they used AES (Advanced Encryption Standard) algorithm to encrypt a message and a part of the message was hidden in DCT (Discrete Cosine Transform) of an image. Gowda (2016) was proposed a generic algorithm where they used AES to encrypt secret data and used RSA (Rivest–Shamir–Adleman) to encrypt key which was embedded a large number of secret messages into LSB in cover image but their proposed method takes more time to hide message than the standard LSB technique, told by them which is weak point of this model. Lokhande (2014) proposed LSB based image steganography technique with encryption to improve security using AES-128, they replaced a secret bit into least significant bit of blue portion of a single pixel. However, AES has key dependent weakness that was proved by Nakasone et al. (2012) also it has bit distribution weakness (Riasat et al., 2011). Mogale et al. (2018) proposed an authentication Security system that uses Image Steganography and 128-bit Advanced Encryption Standard algorithm. Where, they encrypt user's password with 128-bit AES and that message is embedded in image steganography. Therefore, AES has some weakness that was proved by Nakasone et al (2012) and Riasat et al. (2011).

2.3 Case Study on Hash Function

L Zhong et al. (2016) proposed an approach which was Java Web login authentication system with improved Message Digest Five MD5 hashing function and Their result has proved that their approach can effectively resist the brute force attack and differential attack. An image authentication technique is presented (Wahid et al., 2018) which was using MD5 as digital signature. The signature was used as a mark to substantiate the data veracity. In their work, MD5 was used to calculate digital signature row wise from the innards of selected pixels in each row. Then signature was hidden in selected pixels of each row using LSB substitution technique. The hidden signature is used to validate the integrity of the digital images. Therefore, MD5 algorithm cannot be very good against the collision attack, differential attack and dictionary attack (Wang et al., 2005; Li et al., 2019; Klima, 2006; US-CERT, 2008; Stevens, 2012; Wang et al., 2004). Thomas et al. (2015) have described usually used hash algorithms and comparative analysis of various hash processes which are used in password hashing. They described about MD5, SHA, SHA-1, SHA-2, SHA-3, and SHA-192 where they have shown that MD5, SHA, and SHA1 have collision (Stevens, 2013; Wang et al., 2005; Jasek, 2015) where they preferred SHA-3 for authentication. Several researchers (Chauhan & Sharma, 2015; Rachmawati et al., 2018; Sravani et al., 2015; Dworkin, 2015; Wu et al., 2017) discussed about different types of hash function where SHA-3 series hashing function is more secure. Therefore, among SHA hashing algorithms SHA3-512 is better than other even this technique has no any collision. However, it is the better option to use in authentication model.

CHAPTER 3

RESEARCH METHODOLOGY

To proof the proposed model an experimental design methodology has followed. In this methodology, the experimental environment has been divided into two section, the proposed steganography model and implementation of the whole proposed model for the presentation of its effectiveness:

3.1 8-Directional Pixel Selection Approach Based on LSB

In this study, an 8-directional pixel selection technique has been proposed where secret data is hiding initially into the center point followed by the direction of up, up-right, right, underneath-right, underneath, underneath-left, left, and up-left respectively. Unlike to the zig-zag pixel selection technique, this approach will choose center pixel by selecting the middle point of width and height of the cover image.

Number of pixels where the secret data will be embedded, is depended on the length of the secret message and also identify the required pixels for each direction. To satisfy the goal of proposed 8-directional pixel selection technique, it will calculate the *Total Number of Secret Message Bit Length (B_L)* using binary value of each character. Then, it will calculate the *Total Number of Pixels (T_{np})* for embedding using equation (1).

$$T_{np} = \frac{B_L}{3} \qquad (1)$$

By using the value of T_{np}, it will focus to get the value of *Pixels Number for Each Direction (P_{pn})* using equation (2).

$$P_{pn} = \frac{T_{np} - 1}{8} \qquad (2)$$

The technique will then start embedding secret message from *Center Pixel* (C_x, C_y). To calculate (C_x, C_y), it requires to find out the *Height (H)* and *Width (W)* of the cover image using equation (3).

$$(C_x, C_y) = \left\lceil \left(\frac{H}{2}, \frac{W}{2} \right) \right\rceil \tag{3}$$

Here, ⌈ ⌉ denotes as ceil function. Once the *H/2* and/or *W/2* in equation (3) provides the fraction value, ⌈ ⌉ will consider only upper limit value.

The proposed approach will embed message in the *Center Pixel* (C_x, C_y) and then find out 8 directions' pixel for embedding in rest of the message. Each direction embedding will follow the straight-line equation that is given in (eqn. 4).

$$y = mx + c \ [where, m = \pm 1 \sim 0] \tag{4}$$

Here, *y* denotes the length of vertical axis, *x* represents the length of horizontal axis, m defines the slope of straight line, and *c* is the value of *y* when $x = 0$. In Fig. 1 proposed approach presents 8 directional pixel selection technique following equation (5).

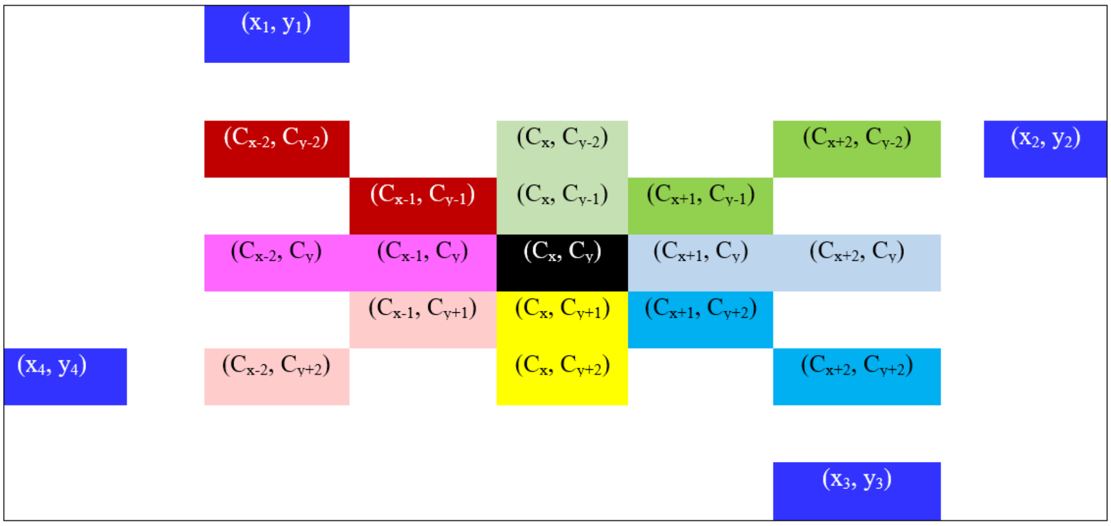


Figure 3: 8 directional pixel selection of a cover image

Equation (5) is used to find out the *8-directional Pixel Position (D$_s$)*,

$$D_s = (C_{x\pm\alpha}, C_{y\pm\alpha}) \quad [where,\ \ a = 0 \ to \ Ppn] \tag{5}$$

From the eqn. (5), pixel position will be selected e.g. the Upward equation will be $(C_x, C_{y-\alpha})$ whereas Upward-right direction will be denoted as $(C_{x+a}, C_{y-\alpha})$, Right direction will be denoted as (C_{x+a}, C_y), Underneath-right direction will be denoted as $(C_{x+a}, C_{y+\alpha})$, Underneath direction will be denoted as $(C_x, C_{y+\alpha})$, Underneath-left direction will be denoted as $(C_{x-a}, C_{y+\alpha})$, Left direction will be denoted as (C_{x-a}, C_y), Upward-left direction will be denoted as $(C_{x-a}, C_{y-\alpha})$.

Equation (6, 7, 8, 9) is used to find out the 4 pixels' position where this approach will embed the secret message bit size number which will use for retrieve message from stego image.

$$1^{st} \text{ pixel's position, } (x_1, y_1) = (\tfrac{W}{2} - 2, 1) \tag{6}$$

$$2^{nd} \text{ pixel's position, } (x_2, y_2) = (W, \tfrac{H}{2} - 2) \tag{7}$$

$$3^{rd} \text{ pixel's position, } (x_3, y_3) = (\frac{W}{2} + 2, H) \tag{8}$$

$$4^{th} \text{ pixel's position, } (x_4, y_4) = (1, \frac{H}{2} + 2) \tag{9}$$

Using equation (10) this approach will find out the value of B_L from the stego image using *Secret Message Size* (S_m).

$$B_L = (S_m * 8) \tag{10}$$

3.1.1 Embedding Technique

Fig. 4 depicts the embedding process of the proposed technique that takes Secret Message (M) and Cover Image (I) as input from the user. It will then find out the H, W, and (C_x, C_y) from that cover image following equation (3).

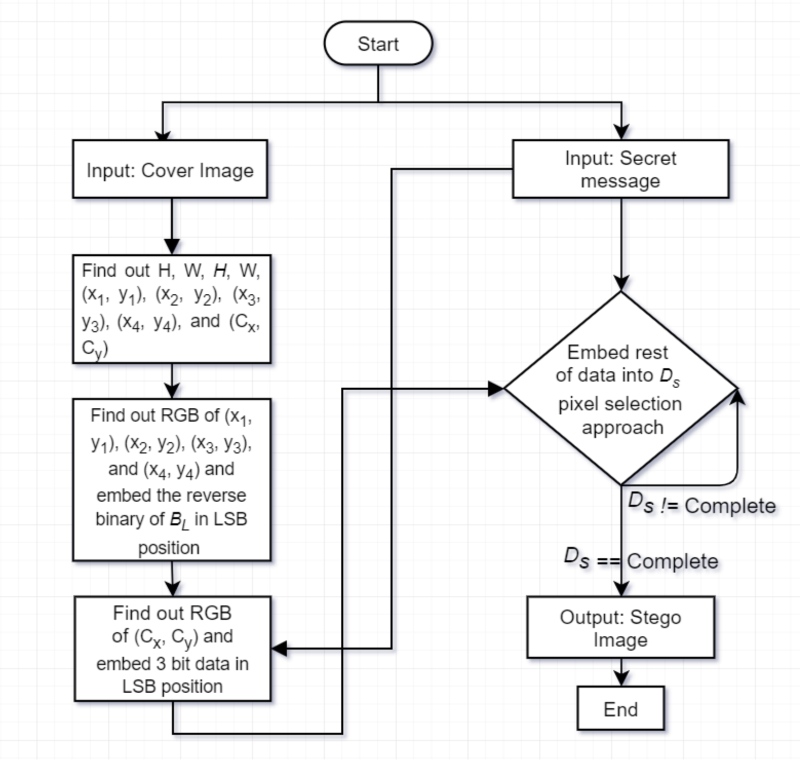

Start
Input: Cover Image
Input: Secret message
Find out H, W, H, W, (x1, y1), (x2, y2), (x3, y3), (x4, y4), and (Cx, Cy)
Find out RGB of (x1, y1), (x2, y2), (x3, y3), and (x4, y4) and embed the reverse binary of BL in LSB position
Find out RGB of (Cx, Cy) and embed 3 bit data in LSB position
Embed rest of data into Ds pixel selection approach
Ds != Complete
Ds == Complete
Output: Stego Image
End

Figure 4: Block Diagram for Embedding Technique

This cover image consists of 24-bit which is the mixer of three core colors i.e. red, green, and blue and each color has eight bits of length. It embeds a bit in each color of LSB position for (C_x, C_y) and rest of M will be kept into Ds. At last, this approach will embed the reverse of binary value of secret message size in LSB position of RGB of (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) which will use to calculate B_L in retrieve process.

3.1.1.1 Embedding Algorithm:

Result: Stego Image

```
M ← input
I ← input
W = Width of Image;
H = Height of Image;
$(C_x, C_y)$ = (H/2, W/2);
embed $((C_x, C_y))$;
$B_L$ = Length of M;
$T_{np} = B_L/3$;
$P_{pn} = (T_{np}-1)/8$;
$B_L$ ← reverse (binary ($B_L$));
$(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$ ← $B_L$;
a = 0;
while a <= $P_{pn}$ do
    $D_s = (C_{x\pm\alpha}, C_{y\pm\alpha})$;
    embed ($D_s$);
    a++;
function embed (position)
    RGB ← position;
    Update-RGB ← message;
```

3.1.1.2 Embedding Example:

At first, this technique takes secret message and cover image from the user. Suppose, the size of secret message is 75 bits which has converted from a string.

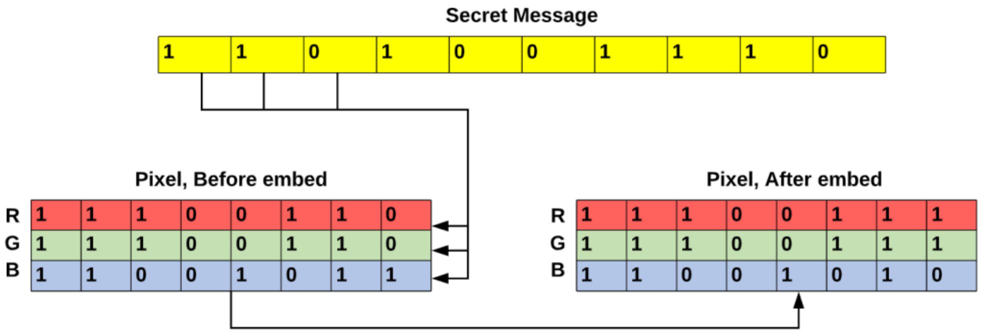


Figure 5: Secret Message Embedding Technique

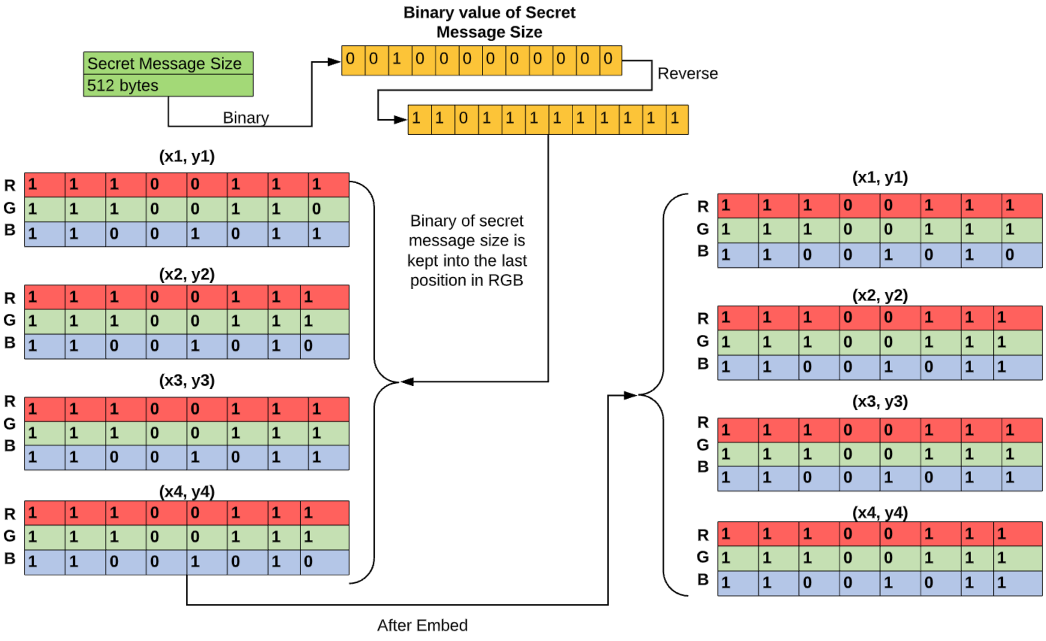


Figure 6: Secret Message Size Embedding Technique

Here, total no. of pixel will be 75/3= 25 and each direction’s pixel no. will be (25-1)/8= 3. Assume that, height, H = 7 & width, W =7 of a cover image and the center pixel will be $(C_x, C_y) = (H/2, W/2)$ = (4, 4). Then calculate the RGB which is (4, 4) and last bit of Red, Green, and Blue will replace by 3 secret message bits (showed in Fig. 5). By following 8 directional approach, it will embed rest of secret bits from upward, upward-right, etc. directions. At last this approach will embed the secret message size into (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) using equation (6, 7, 8, 9) with same technique (showed in Fig. 6).

3.1.2 Retrieving Technique

In the retrieval process of this approach, descried in Fig. 3, takes Stego Image (S) as

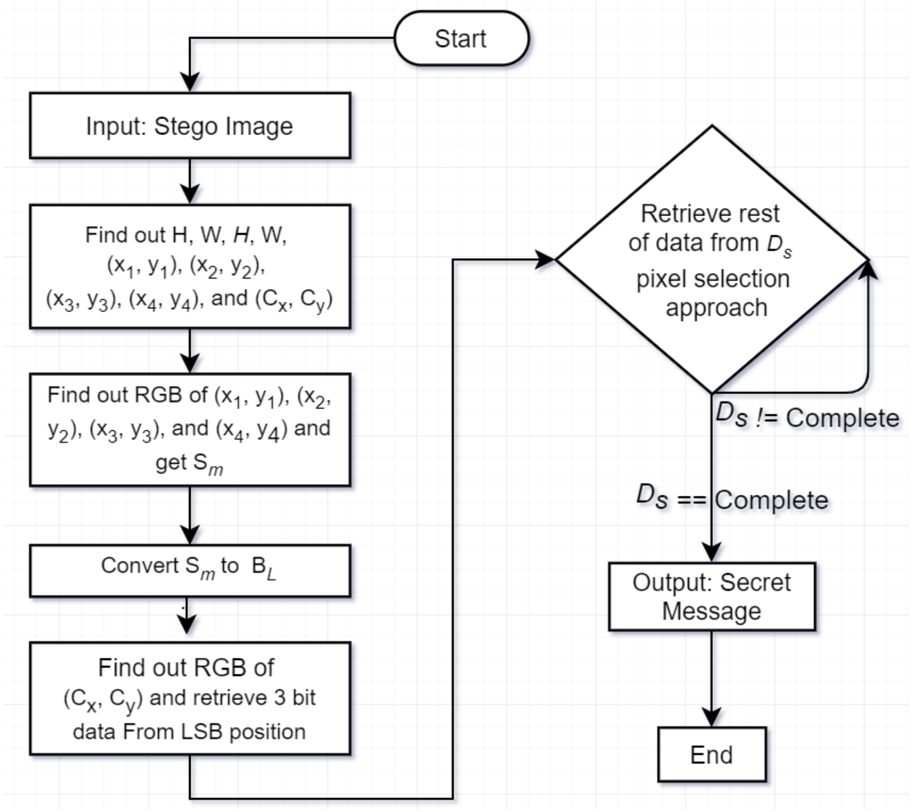

Start
Input: Stego Image
Find out H, W, *H*, W, (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), and (C_x, C_y)
Find out RGB of (x_1, y_1), (x_2, y_2), (x_3, y_3), and (x_4, y_4) and get S_m
Convert S_m to B_L
Find out RGB of (C_x, C_y) and retrieve 3 bit data From LSB position
Retrieve rest of data from D_s pixel selection approach
D_S != Complete
D_S == Complete
Output: Secret Message
End

Figure 7: Block Diagram for Retrieving Technique

input from the user initially. H, W, into (x1, y1), (x2, y2), (x3, y3), (x4, y4) of that stego image will then be calculated and also find out BL which has been kept into LSB position of the RGB of these 4 pixels. Afterward, find out the RGB value of (Cx, Cy) where RGB value will be converted into binary format. The technique will extract the secret message from LSB position of each color bit. Algorithm for embedding and retrieval process for this technique is furnished below.

3.1.2.1 Retrieving Algorithm:

Result: Secret Message

```
S ← input
S_m ← (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4);
S_m ← decimal (reverse (S_m));
B_L ← (S_m * 8);
W = Width of Image;
H = Height of Image;
(C_x, C_y) = (H/2, W/2);
retrieve ((C_x, C_y));
B_L = Length of M;
T_np = B_L/3;
P_pn = (T_np-1)/8;
B_L ← reverse (binary (B_L));
a = 0;
while a <= P_pn do
    D_s = ($C_{x\pm\alpha}, C_{y\pm\alpha}$);
    retrieve (D_s);
    a++;
function retrieve (position)
    RGB ← position;
    Update-RGB ← message;
```

3.1.2.2 Retrieving Example:

In retrieving process, this technique takes stego image from the user. Assume that, height, H = 7 & width, W =7 of a cover image. The *(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)* will be calculate using equation (6, 7, 8, 9) which provide 12-bit binary value that will be reversed and convert to decimal value (showed Fig. 8).

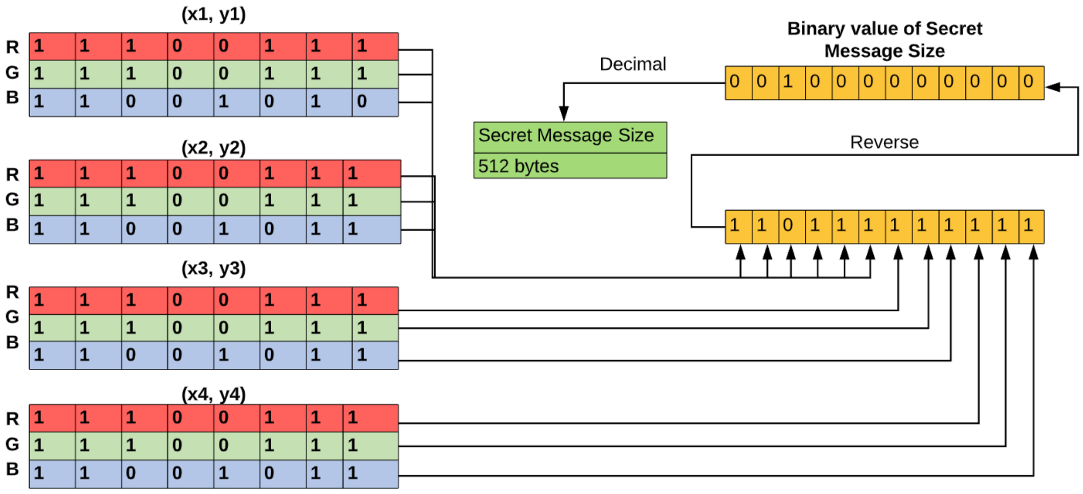


Figure 8: Secret Message Size Retrieving Technique

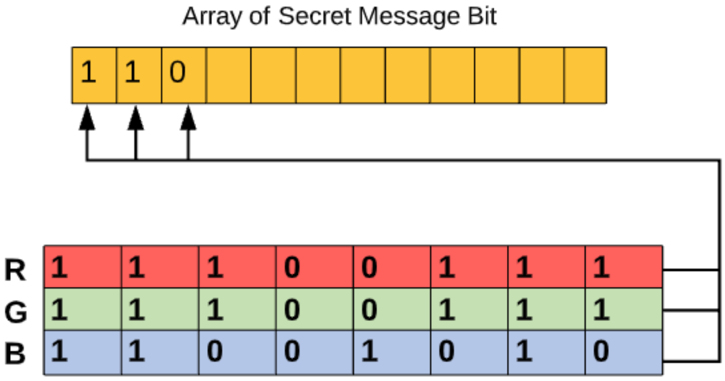


Figure 9: Secret Message Retrieving Technique

Afterward get the value of Sm, it will calculate the value of BL using equation (10). The center pixel will then be calculated which is (Cx, Cy) = ((H/2), (W/2)) = (4, 4). The

RGB will be calculated of (4, 4) position and last bit of Red, Green, and Blue will be taken which will keep in array (showed in Fig. 9). By following Ds, it will take rest of secret bits from upward, upward-right, etc. directions. And at last that array will convert into a string and that string will be the secret message.

3.2 Proposed Model for Authentication

In this study, proposed model will merge with steganography and cryptographic hash function together where it used SHA3-512 for cryptographic hash function.

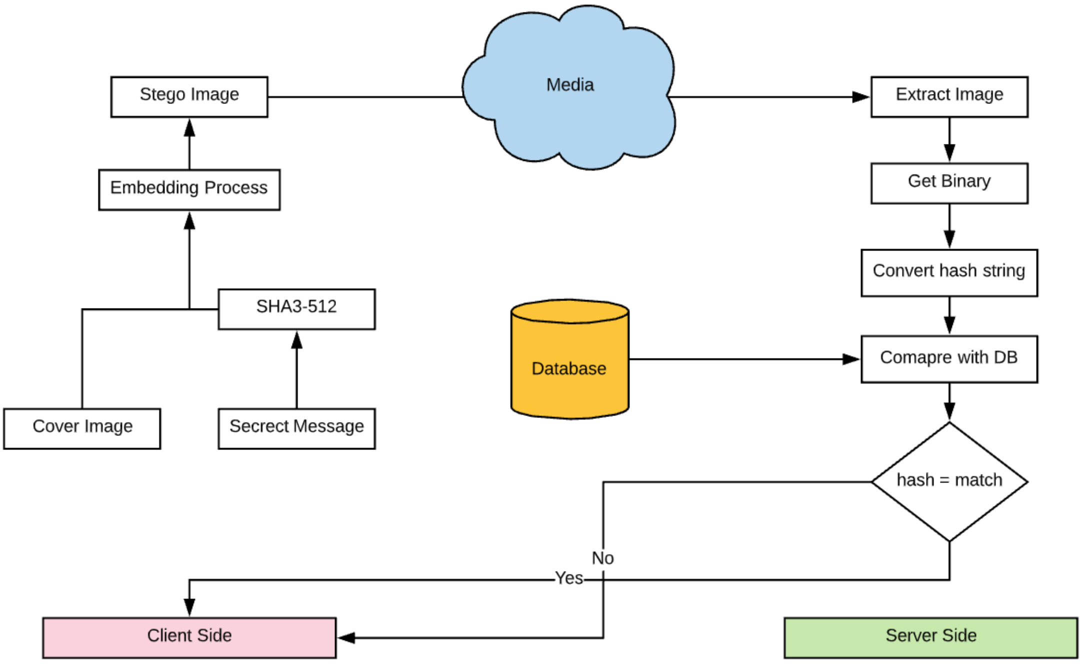


Figure 10: Proposed Authentication Model

In here, a user will input secret message using input field of web application which is a password and a cover image. After input, the secret message will come in hash function and that secret message will convert into SHA3-512 hashing string and this hash string or hash code will convert into a binary form and that binary data will embed in LSB position of that cover image in 8 directional pixel selection techniques which is described in section 3.1.1. After embedding all secret binary data in a cover image to specific pixels, it will convert into a stego image all of these processes will occur into client side using JavaScript.

After getting a stego image in client side then this image will throw to server by a media or protocol. When stego image will reach to server then this server will take that stego image and extract that image using retrieving process which is mentioned in section 3.1.2. After retrieving system will get binary string which will convert into hash string from binary. And server will start to match that hash string with database using database query. After run that query server will start to match that hash string with dataset which is stored in registration time. If the hash string will match with dataset of database then system will create a session for that user and if hash string will not match with dataset of database then system will throw a failure message to that user. All of those tasks of server side will be done by LARAVEL which is a framework of PHP programming language.

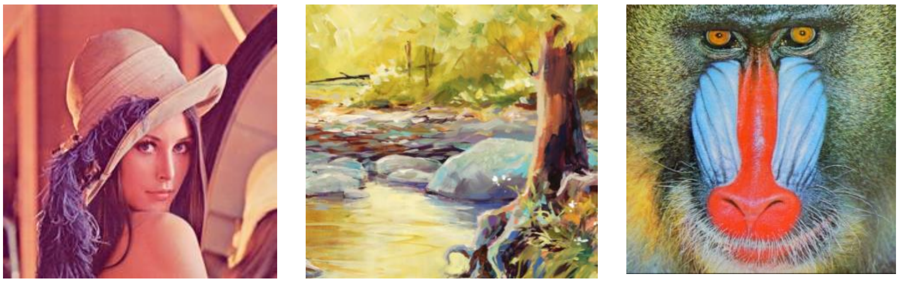
CHAPTER 4

RESULTS AND DISCUSSION

In this section, the results are presented in term of visual interpretation and comparison between cover and stego image. Also, outcomes of the proposed technique are also compared with other known methods to verify the effectiveness. The statistical analysis of the study is furnished with five quality measurement metrics that includes Mean-Square Error (MSE), Root Mean Square Error (RMSE), Signal-to-Noise Ratio (SNR), Mean Absolute Error (MAE), Peak Signal-to-Noise Ratio (PSNR). Embedding Time also considered to verify the efficiency of the proposed solution and it is denoted as Time to Generate a Stego Image (TGSI).

4.1 MSE, RMSE, SNR, MAE, PSNR and TGSI Investigations

Three images (i.e. Lena, Baboon and Nature) which are shown in Fig. 6, have been used for the investigation to proof the proposed technique. Here, 512 X 512 sized images are taken into account for the analysis as it is mostly common size of the related study. Inspiration behind the selection is wide use of these figures among several papers of steganography (Mahimah & Kurinji, 2013; Karim et al., 2011; Khan et al., 2016; Bhardwaj & Sharma, 2016; Huang et al., 2019; Roy et al., 2013; Jassim, 2013).



a) Lena b) Nature c) Baboon

Figure 11: Cover images

To measure the effectiveness and security of the steganography process, we will look for at the difference between the cover image and the stego image. PSNR, SNR, MSE, MAE and RMSE are the quality measurement metrics that can utilized to compare both the images (Hore & Ziou et al., 2010; Kellman & McVeingh, 2005; Vora et al., 2010; Jain, 2011; Liuet al., 2007).

PSNR → Peak Signal to Noise Ratio.

MAE → Mean Absolute Error

SNR → Signal to Noise Ratio.

MSE → Mean Square Error.

RMSE → Root Mean Square Error.

The Mathematical definition for MSE is –

$$MSE = (1 \; x \; M \; x \; N) \quad \sum_{i=1}^{M} \quad \sum_{j=1}^{N} (a_{ij} - b_{ij})^2 \qquad (11)$$

In this equation, a_{ij} refers to the pixel value of the position i and j of the cover image where b_{ij} refers to the pixel value of the position i and j of stego image.

The Mathematical definition for RMSE is –

$$RMSE = \sqrt{MSE} \tag{12}$$

The Mathematical definition for PSNR is –

$$PSNR = 10\ log10\ 255^2/MSE \tag{13}$$

Unit of PSNR is dB, PSNR depends on MSE. Several researches prove that if the value of PSNR between cover and stego image become more than 40dB then it can be considered as high quality.

The Mathematical definition for SNR is –

$$\mathrm{SNR} = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \hat{f}(x,y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - \hat{f}(x,y)]^2} \tag{14}$$

The formula is from Digital Image Processing (Gonzalez et al., 2007) where $\hat{f}$ refers is the noisy image, f refers the original image and x, y refers the position of a pixel.

The Mathematical definition for MAE is –

$$MAE = \frac{1}{3MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [C(\varkappa, y) - S(x, y)]_1 \tag{15}$$

Where M & N denote the image dimension, (x, y) refers the position. C represent the cover image and S represent the stego image and $[]_1$ denotes the city-block norm.

The proposed technique has been implemented using PHP programming language for data hiding, extracting information, and figure out the embedding time where **microtime ()** function is used. MATLAB R2016a is used to find the value of quality measurement matrices and also to create histogram for both cover and stego image.

Result of the proposed technique are measured with three different sized payloads such as 512 bytes, 256 bytes, and 128 bytes on the selected three images. Table 1. represents the results of five quality measurement matrices for given images and embedding time of the stego image

Table 1:

MSE, RMSE, SNR, MAE and PSNR of Proposed Algorithm on Different Payload.

Image	size	Payload	MSE	RMSE	SNR	MAE	PSNR	TGSI
Lena	512* 512	512bytes 256bytes 128bytes	0.0027 0.0013 0.0007	0.0519 0.0363 0.0260	68.6906 71.8004 74.6989	0.0027 0.0013 0.0007	73.8282 76.9380 79.8365	0.08507 0.06055 0.03479
Baboon	512* 512	512bytes 256bytes 128bytes	0.0026 0.0013 0.0006	0.0512 0.0356 0.0252	68.6393 71.7910 74.7883	0.0026 0.0013 0.0006	73.9487 77.1005 80.0977	0.09543 0.06168 0.04086
Nature	512* 512	512bytes 256bytes 128bytes	0.0017 0.0009 0.0004	0.0417 0.0298 0.0212	71.0757 74.0117 76.9490	0.0017 0.0009 0.0004	75.7208 78.6569 82.5942	0.09701 0.06307 0.05905

In this table, 512 X 512 sized image were used for Lena, Baboon, and Nature where payload size of 512 bytes, 256 bytes, and 128 bytes respectively had been taken for consideration. The proposed technique's MSE values for Lena were 0.0027, 0.0013, and 0.0007 respectively where 0.0026, 0.0013, and 0.0006 were found for Baboon. For Nature, the MSE value were 0.0017, 0.0009, and 0.0004 consecutively. RMSE is shown in another vital parameter to assess the quality of an image. The value of RMSE for Lina were 0.0519, 0.0363, and 0.0260 where it was observed 0.0512, 0.0356, and 0.0252 sequentially for Baboon and 0.0417 ,0.0298, and 0.0212 respectively were found for Nature. The values of SNR for Lena were 68.6906, 71.8004, and 74.6989 consecutively and it were 68.6393, 71.7910, and 74.7883 for Baboon. For Nature, the SNR values were 71.0757, 74.0117, and 76.9490 respectively. The seventh column represents the parameter, MAE where its values for Lena were 0.0027, 0.0013, and

0.0007 sequentially where 0.0026, 0.0013, and 0.0006 were detected for Baboon and 0.0017, 0.0009, 0.0004 were found for Nature. PSNR values for Lena were 73.8282, 76.9380, and 79.8365 but the same value for Baboon were 73.9487, 77.1005, 80.0977 accordingly. PSNR value of 75.7208, 78.6569, and 82.5942 were observed for Nature. TGSI is also an important factor that represents the embedding time in second. For Lena, the values of TGSI were 0.08507s, 0.06055s, and 0.03479s where it was 0.09543s, 0.06168s, and 0.04086s for Baboon. The TGSI value for Nature were 0.09701s, 0.06307s, and 0.05905s respectively.

4.2 Comparison with Existing Algorithm

This sub-section represents the experimental output, analysis and comparison among other recent steganographic techniques (Khan et al., 2016; Sarkar & Karforma, 2018; Bhuiyan et al., 2019) where Sarkar & Karforma (2018) are represented 4 direction-based model, T. Bhuiyan et al. (2019) proposed XOR based model, Thresholding based model is represented by Khan et al. (2016). The comparison is done on the basis of number of image performance metrics which are given above in sub section 4.1. The first column name is techniques and the value for MSE, RMSE, SNR, MAE, PSNR and Embedding time are shown in 4th, 5th, 6th, 7th, 8th and 9th columns. Payload is shown in 3rd column and image size are shown in 2nd column.

Table 2: Comparison among four techniques

Techniques	Size	Payload	MSE	RMSE	SNR	MAE	PSNR	TGSI	Image name
Thresholding model	512*512	128 bytes	0.0040	0.0636	66.9215	0.0008	72.0590	0.04536	Lena
4 direction model	512*512	128 bytes	0.0007	0.0258	74.7731	0.0007	79.9107	0.05791	
XOR model	512*512	128 bytes	0.0007	0.0259	74.7400	0.0007	79.8776	0.04644	
Proposed model	512*512	128 bytes	0.0007	0.0260	74.6989	0.0007	79.8365	0.03479	
Thresholding model	512*512	128 bytes	0.0056	0.0746	65.3612	0.0010	70.6707	0.05486	Baboon
4 direction model	512*512	128 bytes	0.0007	0.0257	74.6347	0.0007	79.9441	0.04748	
XOR model	512*512	128 bytes	0.0007	0.0256	74.6683	0.0007	79.9778	0.04644	
Proposed model	512*512	128 bytes	0.0006	0.0252	74.7883	0.0006	80.0977	0.03479	
Thresholding model	512*512	128 bytes	0.0037	0.0610	67.7825	0.0005	72.4277	0.08748	Nature
4 direction model	512*512	128 bytes	0.0005	0.0242	76.4490	0.0005	81.0073	0.07098	
XOR model	512*512	128 bytes	0.0005	0.0220	76.6237	0.0005	81.2689	0.07199	
Proposed model	512*512	128 bytes	0.0004	0.0212	76.9490	0.0004	82.5942	0.05905	

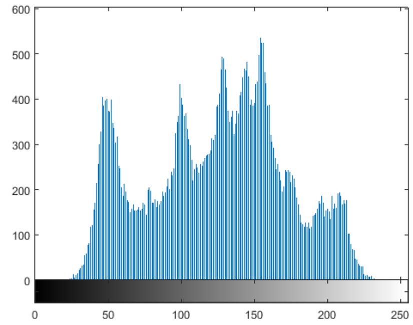
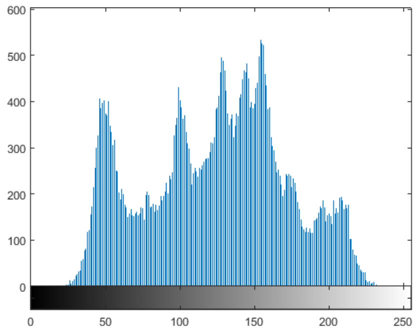
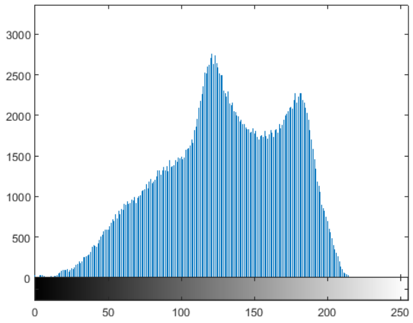
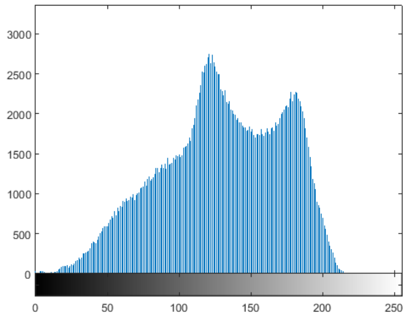
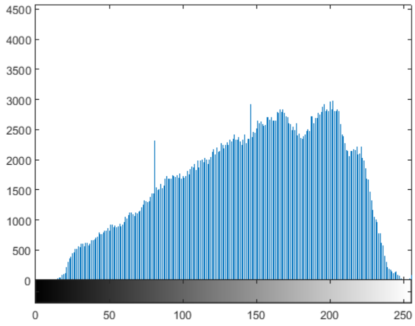
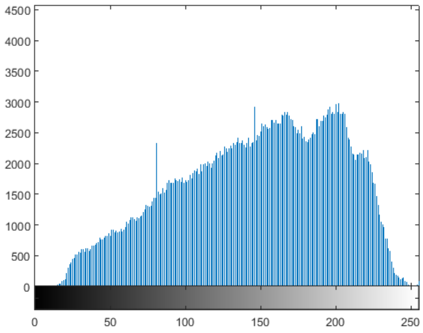
Table 2. shows the comparison among four techniques for Lena, Baboon and Nature cover image. Proposed technique provides 0.0007, 0.0260, 74.6989, 0.0007, 79.8365 and 0.03479 for MSE, RMSE, SNR, MAE, PSNR and TGSI respectively for Lena. Here, the value of TGSI for proposed technique shows the less embedding time among other related techniques mentioned in the above table and it is evident that the given proposed technique is more efficient compared to other concurrent approaches where the image quality remains almost same. For Baboon, proposed technique provides 0.0006, 0.0252, 74.7883, 0.0006, 80.0977 and 0.04086 for MSE, RMSE, SNR, MAE, PSNR and TGSI respectively and these values are indicating better output than other related techniques. For Nature, it provides 0.0004, 0.0212, 76.9490, 0.0004, 82.5942

and 0.05905 for MSE, RMSE, SNR, MAE, PSNR and TGSI consecutively which provide more efficient results than other techniques.

4.3 Comparative Histogram for Cover and Stego Images

The Table 3. shows the histogram for both 512 X 512 sized cover and stego images for the above three images.

Table 3: Comparative Histogram of Cover and Stego images

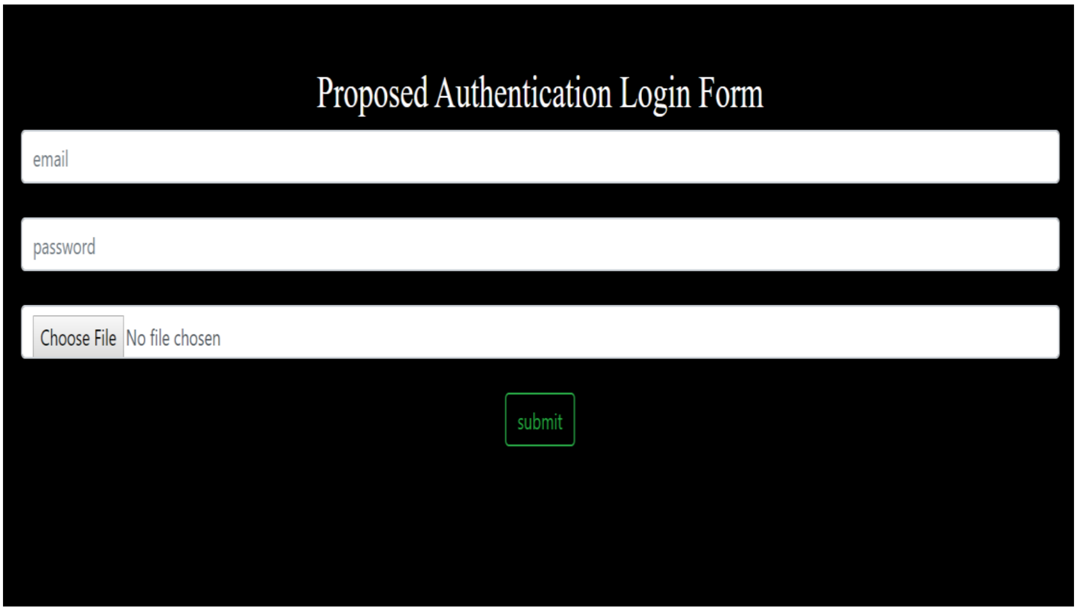
512 x 512 cover image	512 x 512 stego image
Cover Lena 	Stego Lena 
Cover Baboon 	Stego Baboon 
Cover Nature 	Stego Nature 

At first, it is converted the color image into the grayscale image to see the change of RGB component in a single plot where it is used “rgb2gray”. Here, "imhist" method in MATLAB is used to create the histogram. There are no major changes between cover and stego images are observed based on histogram analysis. As per result of histogram, the difference between two images is insignificant which variance cannot be recognized by naked eye.

This data hiding approach is applied in this experiment which shows proposed algorithm works better as compared to other related algorithms

4.4 Implementation on Web App

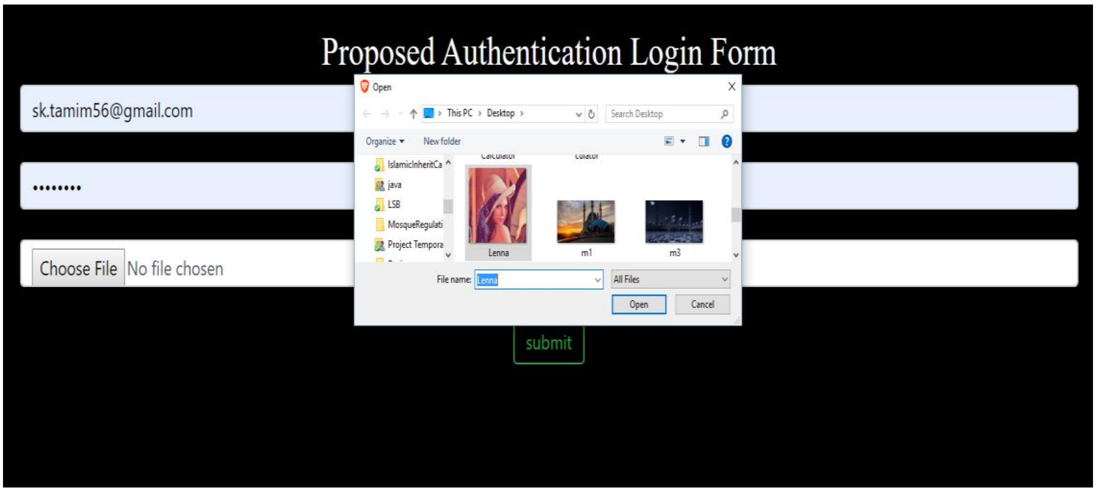
In fig. 12 & 13, there have a login form where a user will input his secret data which is email, password and a cover image.



Proposed Authentication Login Form

Figure 12: Login Form

In client side the cover image and password will embed together which was done by JavaScript. Where password is converted into SHA3-512 hash string and that hash string will convert into binary form and that binary form will embedded into cover image which has given by user. And after embedding a stego image will bring out and that stego image will go in server instead of hash string which is our main contribution.



Proposed Authentication Login Form

sk.tamim56@gmail.com

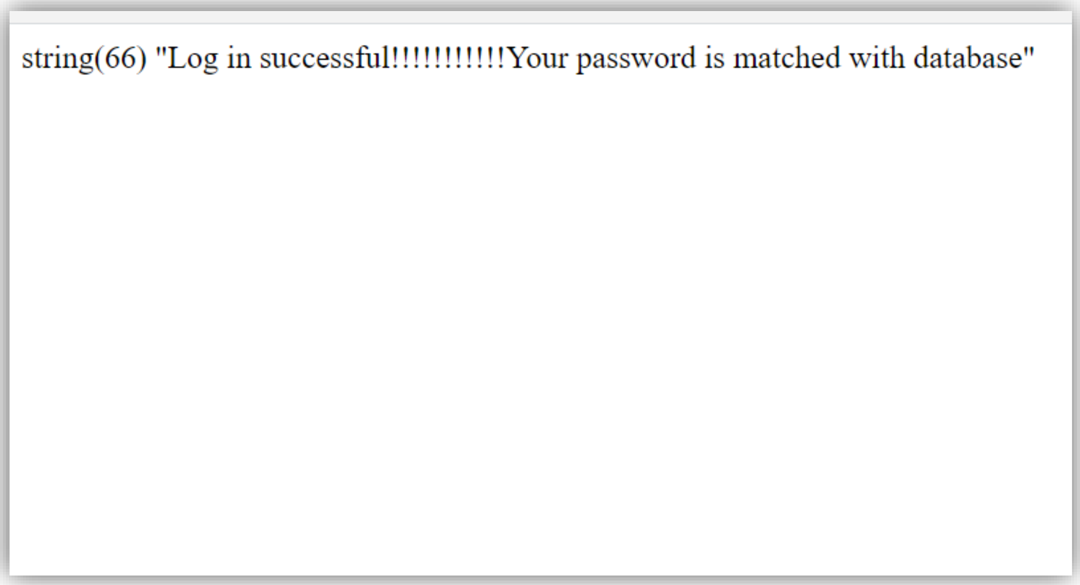
••••••••

Choose File No file chosen

File name: Lenna

All Files

Figure 13: Input Secret Information into Login Form



```
string(66) "Log in successful!!!!!!!!!!!Your password is matched with database"
```

Figure 14: Session Create

In server side, that stego image will take and extracting to get binary information and that binary information will convert into string and that string is that hash string which was embedded in client side and that string will compare to database. If the hash string will match with database then it will throw success message and if don't match then it will throw failure message shown in (Fig. 14)

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings and Contributions

In this paper, a new authentication model is presented which is merged with a new 8 directional pixel selection technique with LSB and SHA3-512 cryptographic technique. In image steganography it embeds secret information which is converted to SHA3-512 hash string in the cover image based on pixel value. LSB replacement algorithm is evident to be fruitful and proficient solution in spatial domain of image steganography. The above discussion and comparative result analysis proved that our proposed steganography data hiding approach provides extra security and less imperceptibility that makes our technique enhanced over some other existing data hiding techniques.

5.2 Recommendations for Future Works

The result of this approach shows that it is able to recognize the authorize user, but it is not proved by BAN (Burrows–Abadi–Needham) logic. In future work, we will prove our model by BAN logic. Which will help its users control whether exchanged data is trustworthy and secured against eavesdropping and in future if SHA3-512 is compromised by collision attack then we will add salt with password to protect from collision attack.

REFERENCES

Ali A.N. (2010). An Image Steganography Method with High Hiding Capacity Based on RGB Image, International Journal of Signal and Image Processing, Vol. 1, Iss.4, pp. 238-241.

Al-Shatnawi, A. M. (2012). A new method in image steganography with improved image quality. Applied Mathematical Sciences,6(79), 3907-3915.

Aqeel, I., Raheel, M. (2018, October). Digital Image Steganography by Using a Hash Based LSB (3-2-3) Technique. In International Conference on Intelligent Technologies and Applications (pp. 713-724). Springer, Singapore.

Ashwin, S., Ramesh, J., Kumar, S. A., Gunavathi, K. (2012, December). Novel and secure encoding and hiding techniques using imagesteganography: A survey. In 2012 International Conference on Emerging Trends in Electrical Engineering and EnergyManagement (ICETEEEM) (pp. 171-177). IEEE.

Awad, A. (2017). A survey of spatial domain techniques in image steganography. Journal of Education College Wasit University,1(26), 497-510.

B. Feng, J. Weng, W. Lu, B. Pei (2017). Steganalysis of content-adaptive binary image data hiding, J. Vis. Commun. ImageRepresent. 46, 119–127.

Beroual, A., Al-Shaikhli, I. F. (2018). A Review of Steganographic Methods and Techniques. International Journal on Perceptiveand Cognitive Computing, 4(1), 1-6.

Bhuiyan T., Sarower M. A. H., Karim M. R, Hassan M. M. (2019). An Image Steganography Algorithm using LSB Replacementthrough XOR Substitution.

Bhardwaj, R., Sharma, V. (2016). Image steganography based on complemented message and inverted bit LSB substitution. Procedia Computer Science, 93, 832-838.

Bharti P., Soni R. (2007, March). A new approach of data hiding in images using cryptography and Steganography, IJOCA (0975-8887), vol.58, no. 8 (2012, November).Bloisi, D. D., Iocchi, L.: Image based steganography and cryptography. In VISAPP (1) (pp. 127-134).

Biradar, R. L., Umashetty, A. (2016). A survey paper on steganography techniques. High Impact Factor, 9(1), 721-722.

Chauhan, J. S., & Sharma, S. K. (2015). A comparative study of cryptographic algorithms. Int. J. Innov. Res, 24-28.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P.(2010). Digital image steganography: Survey and analysis of current methods.Signal processing, 90(3), 727-752.

D.C. Wu, and W.H. Tsai.: A Steganographic method for images by pixel-value differencing, Pattern Recognition Letters,Vol. 24, pp. 1613-1626.

Dworkin, M. J. (2015). SHA-3 standard: Permutation-based hash and extendable-output functions (No. Federal Inf. Process. Stds. (NIST FIPS)-202).

Feng, B., Lu, W., & Sun, W. (2015). Binary image steganalysis based on pixel mesh markov transition matrix. Journal of Visual Communication and Image Representation, 26, 284-295.

Gonzalez, R. C., Woods, R. E. (2007). Digital image processing.

Gowda, S. N. (2016, December). Advanced dual layered encryption for block-based approach to image steganography. In 2016 InternationalConference on Computing, Analytics and Security Trends (CAST) (pp. 250-254). IEEE.

Gupta, N., & Rani, R. (2015). Implementing high grade security in cloud application using multifactor authentication and cryptography. *International Journal of Web & Semantic Technology*, *6*(2), 9.

Hore, A., Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. In 2010 20th International Conference on Pattern Recognition (pp. 2366-2369). IEEE.

H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang. (2005). Image Steganographic Scheme Based on Pixel Value Differencing and LSBReplacement Method, IEEE Proceedings on Vision, Image and Signal processing, Vol. 152, No. 5, pp. 611-615.

Huang, L., Cai, S., Xiong, X., Xiao, M. (2019). On symmetric color image encryption system with permutation-diffusionsimultaneous operation. Optics and Lasers in Engineering, 115, 7-20.

J. Chen, W. Lu, Y. Fang, X. Liu, Y. Yeung, Y. Xue (2018). Binary image steganalysis based on local texture pattern, Journal of Visual Communication and Image Representation, 55, 149-156.

Jassim, F. A. (2013). A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprintarXiv:1307.0642.

Jain, A., Bhateja, V. (2011, December). A full-reference image quality metric for objective evaluation in spatial domain. In 2011 InternationalConference on Communication and Industrial Application (pp. 1-5). IEEE.

Jasek, R. (2015). SHA-1 and MD5 cryptographic hash functions: Security overview. Communications-Scientific letters of the University of Zilina, 17(1), 73-80.

Judge, James C. (2001). Steganography: past, present, future. No. UCRL-ID-151879. Lawrence Livermore National Lab., CA(US).

Kadhim, I. J. (2012). A New Audio Steganography System Based on Auto-Key Generator. Al-Khwarizmi Engineering Journal,8(1), 27-36.

Karim, S. M., Rahman, M. S., Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In 14thinternational conference on computer and information technology (ICCIT 2011) (pp. 286-291). IEEE.

Kellman, P., McVeigh, E. R. (2005). Image reconstruction in SNR units: a general method for SNR measurement. Magneticresonance in medicine, 54(6), 1439-1447.

Khan, Z., Shah, M., Naeem, M., Mahmood, T., Khan, S., Amin, N. U., Shahzad, D. (2016). Threshold-based steganography: anovel technique for improved payload and SNR. Int. Arab J. Inf. Technol., 13(4), 380-386.

K.L. Chiew, J. Pieprzyk (2010). Binary image steganographic techniques classification based on multi-class steganalysis, in: Inter-national Conference on Information Security Practice and Experience, Springer, pp. 341–358.

KLIMA, V. (2006). Finding MD5 Collisions - a Toy for a Notebook.

L.C. Kang, J. Pieprzyk (2010). Blind steganalysis: A countermeasure for binary image steganography, in: Ares '10 InternationalConference on Availability, Reliability, and Security, pp. 653–658.

L.C. Kang, J. Pieprzyk (2010). Estimating hidden message length in binary image embedded by using boundary pixels steganog-raphy, in: Ares '10 International Conference on Availability, Reliability, and Security, pp. 683–688.

Liu, Z., Lagani`ere, R. (2007). Phase congruence measurement for image similarity assessment. Pattern Recognition Letters, 28(1),166-172.

Li, B., Wang, M., Li, X., Tan, S., Huang, J. (2015). A strategy of clustering modification directions in spatial image steganography. IEEE Transactions on Information Forensics and Security, 10(9), 1905-1917.

Li, Y., HeLu, X., Li, M., Sun, Y., & Wang, L. (2019, July). Implementation of MD5 Collision Attack in Program. In International Conference on Artificial Intelligence and Security (pp. 595-604). Springer, Cham.

Lokhande U. (2014). An Effective Way of using LSB Steganography in images along with Cryptography. International Journal ofComputer Applications, 88(12).

M. A. Saleh (2018, September). Image Steganography Techniques - A Review Paper, Ijarcce, vol. 7, no. 9, pp. 52–58.

Mahimah, P., Kurinji, R. (2013, December). Zigzag pixel indicator based secret data hiding method. In 2013 IEEE International Conferenceon Computational Intelligence and Computing Research (pp. 1-5). IEEE.

Malalla, S., & Shareef, F. R. (2016). Improving Hiding Security of Arabic Text Steganography by Hybrid AES Cryptography and Text Steganography. Journal of Engineering Research and Application, 6(6), 60-69.

Mandal J. K., Debashis D. (2012, July). Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain, InternationalJournal of Information Sciences and Techniques (IJIST) Vol.2, No.4.

Mogale, H., Esiefarienrhe, M., & Letlonkane, L. (2018, December). Web Authentication Security Using Image Steganography and AES Encryption. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)* (pp. 1-7). IEEE.

Nagpal, K. D., Dabhade, P. D. S. (2015). A Survey on Image Steganography and its Techniques in Spatial and Frequency Domain.International Journal on Recent and Innovation Trends in Computing and Communication, 3(2), 776-779.

Nakasone, T., Li, Y., Sasaki, Y., Iwamoto, M., Ohta, K., Sakiyama, K. (2012, November). Key-dependent weakness of AES-based ciphersunder clockwise collision distinguisher. In International Conference on Information Security and Cryptology (pp. 395-409). Springer, Berlin, Heidelberg.

Odeh, A., Elleithy, K., Faezipour, M., Abdelfattah, E. (2015). Novel Steganography over HTML Code. In Innovations and Ad-vances in Computing, Informatics, Systems Sciences, Networking and Engineering (pp. 607-611). Springer, Cham.

Pavani, M., Naganjaneyulu, S., Nagaraju, C. (2013). A survey on LSB based steganography methods. International Journal ofEngineering and Computer Science, 2(8), 2464-2467.

Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018, March). A comparative study of Message Digest 5 (MD5) and SHA256 algorithm. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012116). IOP Publishing.

Ran Z. W., Chi F. L., Ja C. L. (2001). Image hiding by optimal LSB substitution and Genetic algorithm, Pattern RecognitionSociety. Published by Elsevier Science Ltd., pp.671-683.

Riasat, R., Bajwa, I. S., Ali, M. Z. (2011, July). A hash-based approach for colour image steganography. In International Conferenceon Computer Networks and Information Technology (pp. 303-307). IEEE.

Roy, R., Changder, S., Sarkar, A., Debnath, N. C. (2013, January). Evaluating image steganography techniques: Future research challenges.In 2013 International Conference on Computing, Management and Telecommunications (ComManTel) (pp. 309-314). IEEE.

Sahu, A. K., Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. Indonesian Journalof Electrical Engineering and Computer Science, 2(3), 712-719.

Sarmah, D. K., Bajpai, N. (2010). Proposed System for data hiding using Cryptography and Steganography. International Journalof Computer Applications, 8(9), 7-10.

Sarkar, A., Karforma, S. (2018). A new pixel selection Technique of LSB based steganography for data hiding. InternationalResearch Journal of Computer Science (IRJCS), Issue 03, Volume 5.

STEVENS, M. (2013). New Collision Attacks on SHA-1 Based on Optimal Joint Local-collision Analysis, Lect. Notes Comput. Sc., No. 7881, pp. 245-261.

STEVENS, M. (2012). Single-block Collision for MD5.

Shailendra M. P., Sandip R. S., Vipul D. P., and Puja S. (October 2013). A Survey on compound use of Cryptography and Steganography for Secure Data Hiding, International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.3, Issue 10, ISSN: 2250-2459.

Singla, S., Bala, A. (2018, April). A Review: Cryptography and Steganography Algorithm for Cloud Computing. In 2018 Second Inter-national Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 953-957). IEEE.

Sravani, M. M., & Pallavi, C. H. (2015). Design of Compact Implementation of SHA-3 (512) on FPGA. International Research Journal of Engineering and Technology (IRJET), 2(02), 41-46.

Subhedar, M. S., Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. Computer science review,13, 95-113.

Swain, G (2019). Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arabian Journal for Science and Engineering, 44(4), 2995-3004.

Thangadurai, K., Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In 2014 International Conferenceon Computer Communication and Informatics (pp. 1-4). IEEE.

Thomas, P. (2013). Literature survey on modern image steganographic techniques. International Journal of Engineering Researchand Technology, 2, 107-111.

Thomas, C GThomas, Robin Assistant, Jose. (2015, October). A Comparative Study on Different Hashing Algorithms. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Special Issue 7.

Tiwari, N., Shandilya, D. M. (2010). Evaluation of various LSB based methods of image steganography on GIF file format. International Journal of Computer Applications, 6(2), 1-4.

US-CERT (2008). MD5 Vulnerable to Collision Attacks.

Vora, V. S., Suthar, A. C., Makwana, Y. N., Davda, S. J. (2010). Analysis of Compressed Image Quality Assessments, M. TechStudent in E C Dept, CCET, Wadhwan-Gujarat.

Wahid, M., Ahmad, N., Zafar, M. H., & Khan, S. (2018, February). On combining MD5 for image authentication using LSB substitution in selected pixels. In 2018 International Conference on Engineering and Emerging Technologies (ICEET) (pp. 1-6). IEEE.

Wang, X., Yu, H. (2005). How to break MD5 and other hash functions. Springer, Heidelberg.

WANG, X., YU. H. IN, Y. L. (2005). Efficient Collision Search Attacks on SHA-0, Lect. Notes Compute. Sc., vol. 3621, pp. 1-16.

WANG, X., FENG, D., LAI, X, YU, H. (2004). Collision for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD.

Westfeld, A. (2001, April). F5—a steganographic algorithm. In International workshop on information hiding (pp. 289-302). Springer,Berlin, Heidelberg.

Wu, X., & Li, S. (2017, October). High throughput design and implementation of SHA-3 hash algorithm. In 2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC) (pp. 1-2). IEEE.

Zhong, L., Wan, W., & Kong, D. (2016, July). Javaweb login authentication based on improved MD5 algorithm. In 2016 International Conference on Audio, Language and Image Processing (ICALIP) (pp. 131-135). IEEE.

Zhu, Z., Zhang, T., Wan, B. (2013, June). A special detector for the edge adaptive image steganography based on LSB matching revisited.In 2013 10th IEEE International Conference on Control and Automation (ICCA) (pp. 1363-1366). IEEE.