REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Information Technologies

PROPOSE AI SYSTEM TO ENHANCE IMAGE STEGANOGRAPHY

Yousif Talib Zghayer AL-BAIDHANI

Master Thesis

Supervisor

Asst.Prof. Dr. Ayça Kurnaz Türkben

Istanbul 2023

PROPOSE AI SYSTEM TO ENHANCE IMAGE STEGANOGRAPHY

Yousif Talib Zghayer AL-BAIDHANI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled PROPOSE AI SYSTEM TO ENHANCE IMAGE STEGANOGRAPHY prepared by YOUSIF ZGHAYER AL-BAIDHANI and submitted on 04/05/2023 has been **accepted unanimously** for the degree of Master of Science in Information Technologies.

Academic Title – First and Last Name of the Co-Supervisor	Academic Title – First and Last Name of the Supervisor

Thesis Defense Committee Members:

Academic Title - First/Last Name	Department, University	_____
Academic Title - First/Last Name	Department, University	_____
Academic Title - First/Last Name	Department, University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Yousif Talib AL-BAIDHANI

Signature

DEDICATION

In the name of Allah the merciful.

First, I want to thank God Almighty for giving me the chance and helping me finish my Master's degree.

Dad, my darling dad.

To my guardian angel in life.. to the meaning of love and the meaning of compassion and devotion.. to the smile of life and the secret of existence, for whom your invitation was the key to my success and affection:

Dear mother..

To the one who has the largest and so I rely . and on whom I trust.. to a candle whose flame brightens the darkness of my life.. to those who have acquired limitless strength and love..to whom did you know the meaning of life

To the one who is closest to my soul, to the one who shares with me the bosom of pain, and through them I draw my strength and determination.. my brothers and sisters

Who paved the way in front of me to reach the height of science to .. my professor "I was in my studies and shared my thoughts reminder and appreciation .My friends

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Prof. Dr. AYÇA KURNAZ for all the knowledge and support he provided during my studies for my master's degree and throughout the work to complete this dissertation, which eased the difficulties I faced during my studies. I have achieved my dream.

ABSTRACT

PROPOSE AI SYSTEM TO ENHANCE IMAGE STEGANOGRAPHY

AL-BAIDHANI, Yousif Talib Zghayer

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

Date: March / 2023

Pages: 47

Steganography is one of the methods used for the hidden exchange of information and it art of invisible communication. The confidential communication is concealed so that it cannot be seen by human senses. Steganography and encryption offer an effective means of achieving that privacy. Conventional methods of image steganography tend to start with the first pixel and proceed with subsequent pixels until the last piece of the hidden message is embedded. In order to increase the security of the steganography system, modern trends involve arbitrarily hiding data in images using various clever algorithms.

Numerous methods will be used in this thesis to improve image steganography and provide high levels of security systems and exchange the secret information in secure way.

By arbitrarily concealing encrypted data in the cover, a proposed image steganography method based on Ant Colony Optimization (ACO) aims to improve geographic image steganography. Data Encryption Standard (DES) is used to encode a secret communication to increase the security of the suggested system. The use DES algorithm With using breadth algorithm to generate the key to increase the complexity against the attacker and difficult way to detect the original message. Cover image separating into groups (n*n) optimum pixels can discovered through the connection between pixels. Each block has the Ant Colony System (ACS) applied to it in order to determine the texture of colour among the pixels in the block and determine which pixel is best to use to embed the encrypted secret message bits. This process is repeated for each subsequent block until the secret message finished. The testing study demonstrates that in terms of quality (MSE and PSNR) and security.

The final experimental results between security techniques (steganography and cryptography) and artificial intelligence (ACO (ACS) with security techniques) explains. Ant Colony System (ACS) of the ACO algorithm outperforms R(RGB-LSB). The PSNR in the R(RGB-LSB) technique is 71 and ACO is 83, according to the findings of the contrast between the ACO and R(RGB-LSB).

Keywords: ACO, DES Algorithm Steganography, Cryptography, ACS, PSNR, RGB.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

ACO	:	Ant Colony Optimization
ACS	:	Ant Colony System
LSB	:	Least Significant Bit
R(RGB-LSB)	:	Red (Red, Green and Blue - Least Significant Bit)
MSE	:	Mean Squared Error
PSNR	:	Peak Signal-to-Noise Ratio
DES	:	Data Encryption Standard
SEC MSG	:	Secret Message

1. INTRODUCTION

The most current advancements in information technology require us to safeguard the privacy of digital data. The creation of a method that can satisfy criteria is essential. Several methods/strategies were used to make it happen. One of the best methods to achieve such privacy is by combining cryptography with steganography [1].

The art and science of steganography include disguising data via common cover medium [2]. Steganography, which is the study of covert communication and often concentrates on methods for disguising the existence of the message being communicated, is one method for transmitting information secretly. If done correctly, this prevents attackers and eavesdroppers from overhearing the conversation. In a variety of containers, also known as embedding materials, information may be hidden via steganography. Text, audio, video, or image data are all acceptable carriers [3]. Steganography is one of the most dependable techniques for conveying confidential messages between individuals [4].

Encoding and decoding secret messages using cryptography protects them from being accessed by unauthorized people [5]. The term "cryptography" is derived from the Greek terms "kryptós" for "secret" and "gràphin" for "writing"[6]. Cryptography aims to protect data and communication channels by using calculations and a set of rules known as an algorithm[7]. Steganography may provide a special way to communicate sensitive information that is only understandable by the talking parties[8]. Steganography and cryptography are common techniques for data preservation in computer security [7]. Ant colony optimization (ACO), one of the intelligent swarm algorithms, is influenced by the foraging methods of several ant species. These ants make smell trails on the ground that point the other ants in the colony in the direction they should proceed. Ant colony optimization approaches optimization problems in a similar manner. In ACO, a system that is based on the communication method used by actual ants is utilized to generate optimization issue solutions and communicate on their quality [9]. Ant colony optimization (ACO) was the brainchild of Marco Dorigo. A metaheuristic called the ACO algorithm was inspired by how real ants found their way to food sources [10]. The meta-heuristic optimization method ACO provides a rough solution to difficult combinatorial optimization problems. Artificial ants in ACO travel across the problem graph to provide solutions, and

they mimic real ants by leaving behind synthetic pheromones that will aid other synthetic ants in producing even better solutions in the future [11].

1.2 THE THESIS'S OBJECTIVE

This thesis uses ACO algorithms with steganography and cryptography to improve image steganography and develop a system that is more secure. Secret data is encrypted, then it is embedded in a cover image that is separated into n blocks to provide security. ACO method may be used to extract the best pixel from each block. This theory leads to improved stego image quality and increased hacker resistance (good security).

1.3 THESIS OUTLINE

The remainder of this paper is divided into the following sections.

a. Chapter Two: “Theoretical Background”, presents steganography, cryptography, DES algorithm, ACO and ACS.

b. Chapter Three: “The specifics of the proposed system's methods and their implementations are presented in "Design and Implementation of the Proposed System."

c. Chapter Four: "Results and Discussions", presents show the results of proposed system.

d. Chapter Five: “Basic findings and a number of recommendations for future works are covered in Conclusions and Recommendations for Future Work.

2. LITERATURE REVIEW

2.1 INTRODUCTION

Steganography is the science of concealing sensitive information inside of image, audio, video, or text files [12, 13, and 14]. The Greek terms steganos, which mean "covered or shielded," and Graphic, which mean "writing," are combined to form the English word "steganography" [15, 16]. Steganography has the advantage of preventing the initial hidden message from becoming the focus of careful scrutiny [12, 17].

The study of methods for transforming information from its typically understandable form into an unintelligible structure is known as cryptography [18]. The practice of transforming textual (message) into an unintelligible code is known as cryptography [19].

The primary flaw in cryptography is that it is possible for hackers to identify encrypted communications and attempt to decode them using a variety of techniques, such as automated counters or arbitrary tests based on mathematical formulas. As a result, the encryption technique still has security flaws, such as its reliance solely on decryption secrets. Another security method, such as steganography, can be used to assist and enhance the cryptography technique. One of the most helpful techniques for raising the security degree of encryption is steganography. These two approaches can effectively be combined to offer a high degree of online data protection [20]. Combining encryption and steganography improves the security of the protected data of secret and secure communication [21].

Ant Colony Optimization, or ACO, is a meateuristic used to tackle complex combinatorial optimization issues [22]. Ant Colony Optimization (ACO) is an optimization method that draws inspiration from nature and employs ants as search agents to explore a search area [23]. In ACO some of artificial ants in ACO can find the solutions through indirect communication and shortest path between theirnest and food using pheromone. [24].

2.2 STEGANOGRAPHY

Steganography is a potential technique for securing data while it is being transmitted over communication networks. Steganography methods enable us to conceal hidden messages in media artifacts like digital images [25].

There are three components of information hiding are shown in figure (1) [26. 27]:

a. Cover: It is the carrier of message such as image, audio, video or other digital media [20.26].

b. Secret Message: Information that must be hidden in digital media [26].

c. Key: used to hide secret message through Steganography algorithms [20-28].

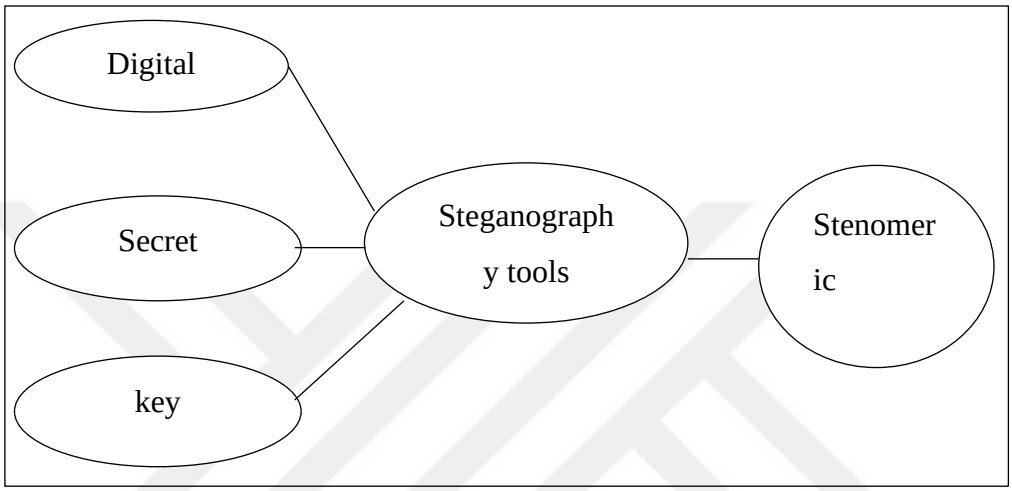

Figure 2.1: Components of Steganography [29].

There are some requirements which need to achieve a secure steganography technique; security, robustness, and embedding capacity [30.31].

a. Security: The resistance of the stego-media against steganalysis .
b. Robustness: The main requirements of the steganography techniques. The ability of the stego media strength against steganolaysis technique [30.32].
c. Capacity: Capacity refers to the amount of data hidden in a cover media without degradation of stego_media quality [30.33.34].

As shown in figure (2.2), three requirements represent a triangle in steganography [35,36].

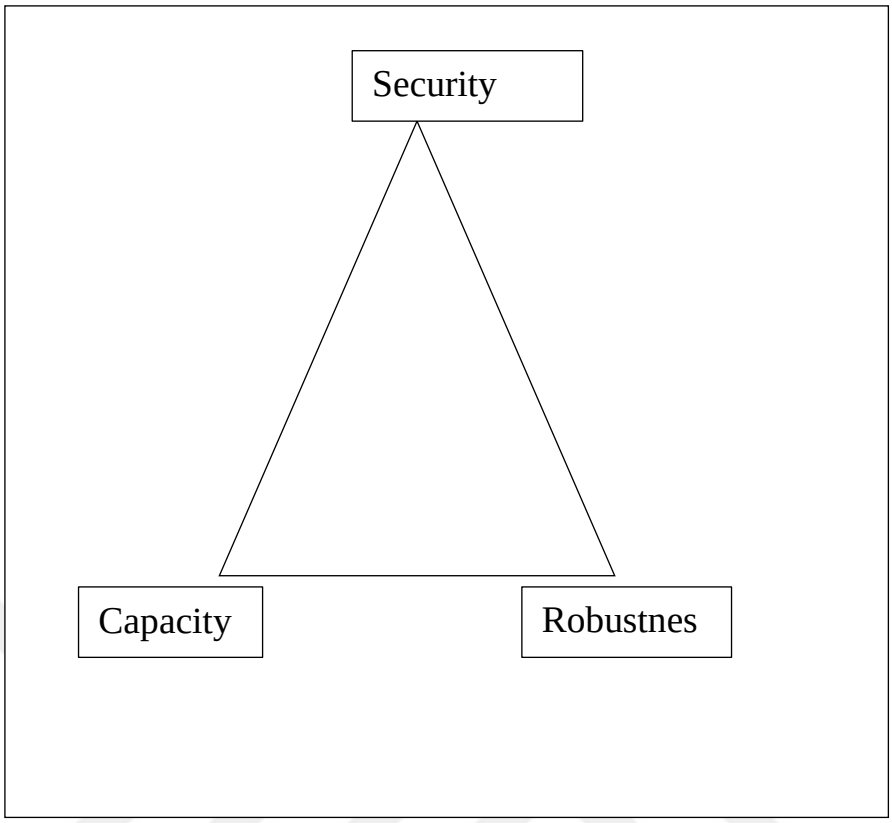

Figure 2.2: The Requirements in Information Hiding System.

2.2.1 Digital Image Steganography

The most common cover item for information concealing is an image [37]. The cover image that conceals secret information is known as the cover image [38], and the cover image that transmits a secret message is known as the stego image [39]. There are several steganographic methods that use a digital image as a carrier. Least-significant-bit (LSB) replacement is the most popular and straightforward technique, in which one bit of secret data is substituted for each LSB location in the cover image [40]. The fundamental concept behind LSB is the direct substitution of LSBs of noisy or unused bits in the cover image with the hidden message bits. The most popular method for data hiding is called LSB. It is easy to implement, has a high hiding capacity, and makes it simple to regulate the quality of the stego-image. However, it is not very robust to changes made to the stego-image, like low pass filtering and compression, and is also not very imperceptible [41]. See figure (2.3):

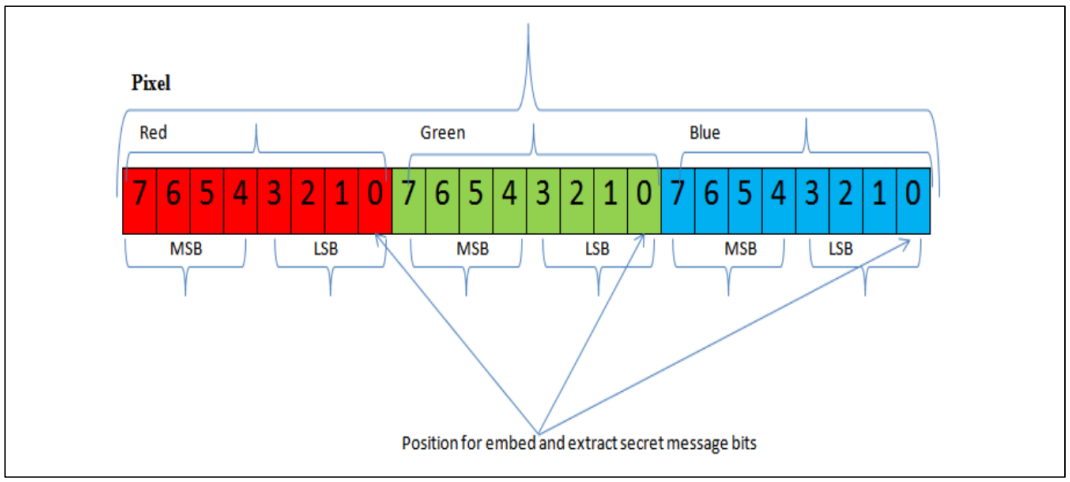

Figure 2.3: One Pixel from Image.

2.3 CRYPYOGRAPHY

In order to prevent unauthorized parties from accessing sensitive data, information, or communications, cryptography is a practice that includes the study of safe communication methods [6]. Data secrecy, integrity, and verification are just a few of the information security-related concepts that are incorporated into this practice (CIA) [42]. Decryption and encryption are the two basic operations of cryptography [21]. The Encryption process is applied before transmitting the message and decryption process applied after receiver receives the encrypted message [18]

The message's open form is referred to as "plain text," and its protected form is referred to as "cipher text." [43] show figure (2.4) [18].

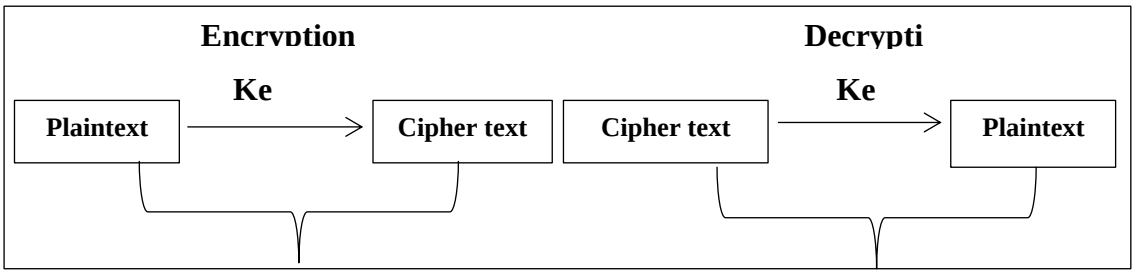

Figure 2.4: Encryption and Decryption in Cryptography.

The primary flaw in cryptography is that it is possible for hackers to identify encrypted communications and attempt to decode them using a variety of techniques, such as

automated counters or arbitrary tests based on mathematical formulas. Steganography, another security technique, can be used to support cryptography for better security [20].

Steganography and cryptography are two techniques that could be used to secure data. Steganography is a method of concealing data inside of another data, while cryptography is a method of protecting data by converting its substance into a character that the other person cannot comprehend. Because of the steganography method, the other people are unaware that the data transfer contains private information. [1]. Show figure (2.5) [20.21].

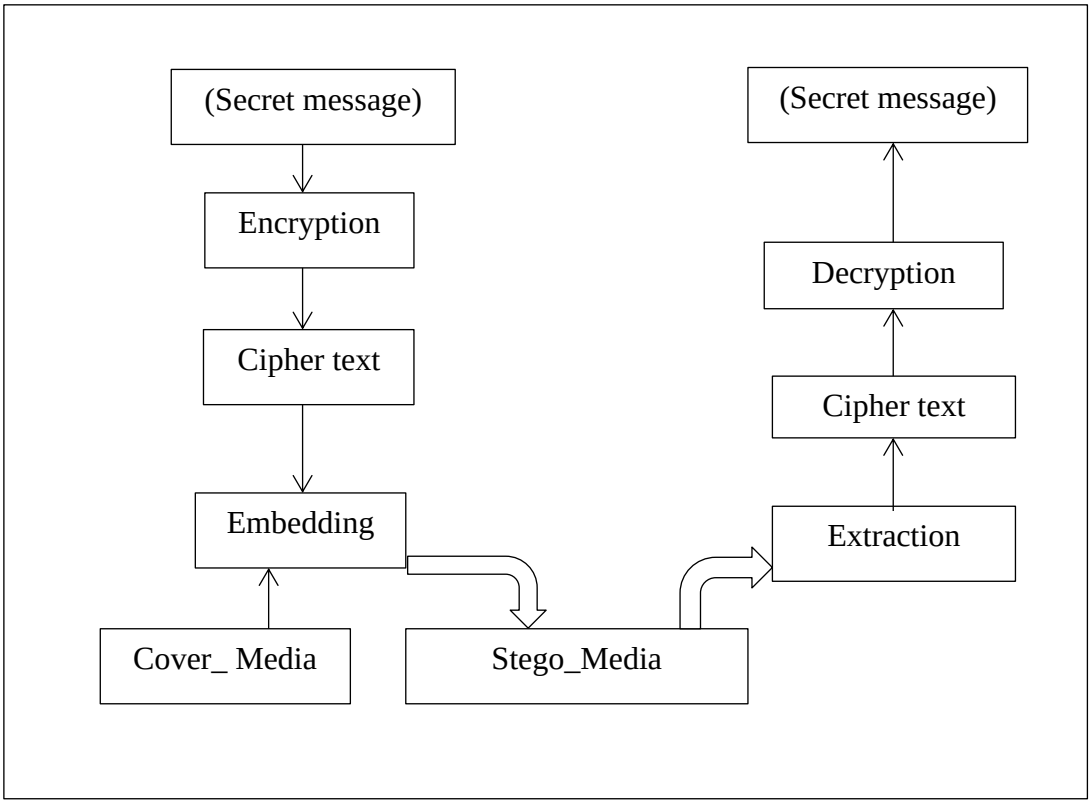

Figure 2.5: Combination of Cryptography and Steganography.

2.3.1 Data Encryption Standard (DES)

DES is a symmetric key block encryption method. Currently, this method uses the same private key for both the encryption and decryption processes (Symmetric-key). 64-bit data was used as input by the method. The method converts data into a sequence of 64 bit cipher text blocks. Every raw block goes through 16 iterations of encryption. By introducing sulky ki, the decryption procedure is carried out in the opposite order of the encryption technique

by main key k where i=1…….16 [44, 45, 46 and 47]. Figure (2.6) explain DES structure [48, 49]:

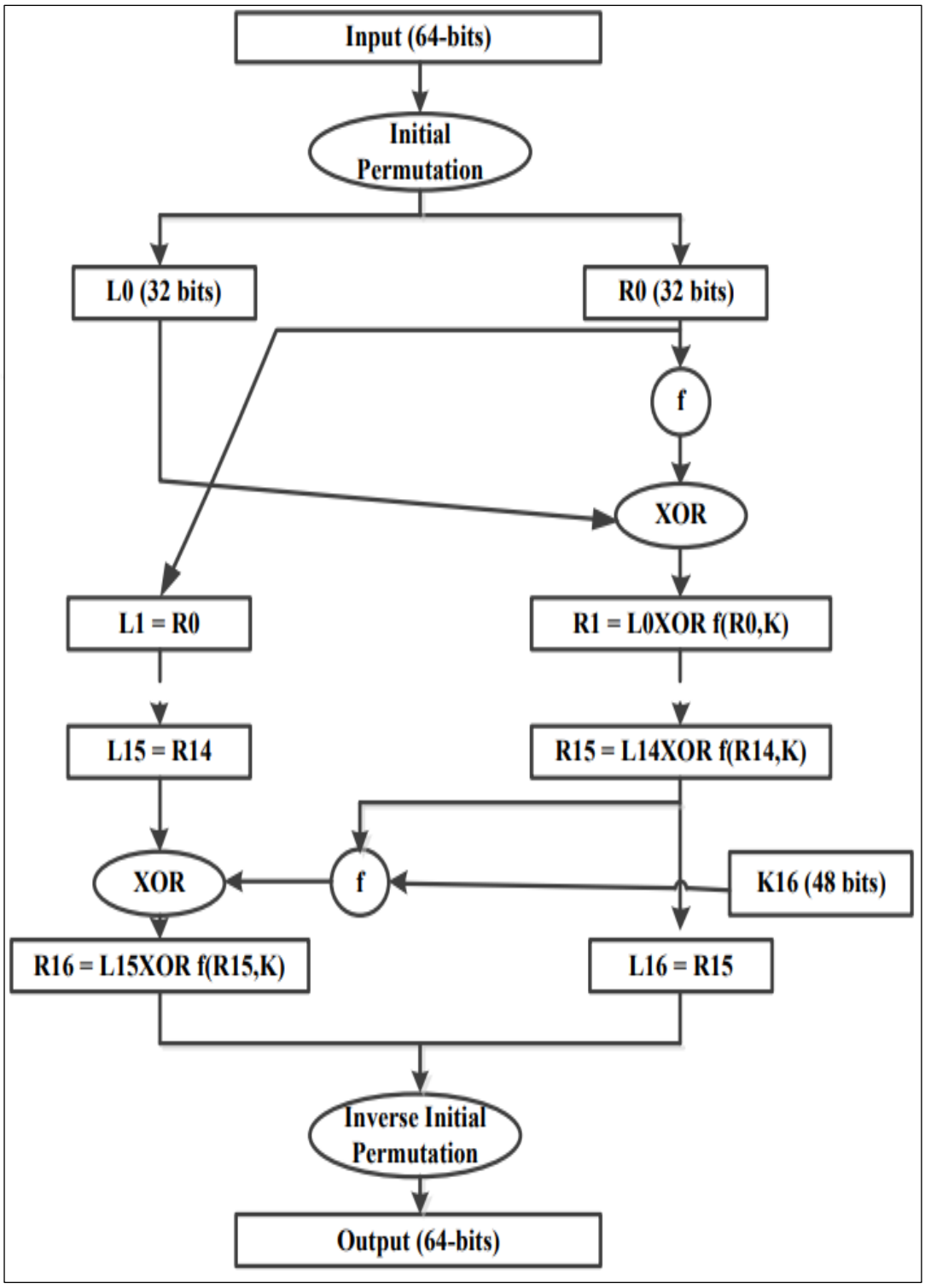

Figure 2.6: Structure of DES.

2.4 ANT COLONY OPTIMIZATION (ACO)

Ant colony optimization is the most basic swarm-based solution for discrete problems [50]. Finding excellent routes through networks is the goal of the probabilistic ant colony optimization algorithm (ACO), which is used to solve computational issues [51]. ACO is a discrete combinatorial optimization algorithm based on the foraging food of an ant group. An ant colony is able to find the shortest distance between their nest and a food source through the method of indirect contact through putting a chemical called (pheromone) when traveling along their path. The desirable path and shortest path contain a large amount of pheromone, where desirable by colony [52, 53]. The difference between ACO algorithms and search by random algorithms is that artificial ants use a rule to construct solutions (using probabilistic transition rule based on pheromone intensities on edges) [54]. The resemblances between actual ants and ant in artificialnintelligence ones used in ant colony optimization include [55]:

a. the use of a cooperative group of people to discover a more effective, global answer to the issue or job at hand.
b. using a synthetic pheromone trail for a stigmatizing reaction.
c. the use of a local motion to determine the quickest route between the nest and food.
d. Use probabilistic decision policy to navigate through neighbouring nodes.

ACO algorithm is basically a construction algorithm, that is, in each iteration of the algorithm, each ant builds a solution to the problem by traversing the construction graph.[56]:

a. Heuristic Information: measures the heuristic preference of moving from node „a‟ to node„b‟. It is denoted by ηrs and this information is not modified by the ant during the algorithm run.
b. Pheromone in artificial intelligence pathway information. It measures the acquired desire for movement. This information is progressed while the algorithm is running based on the solution found by the ants, which is denoted by ab.

c. Ant Colony System. ACS improves over AS by increasing the importance of exploitation of information collected by previous ants with respect to exploration of the search space. This is achieved via two mechanisms. First, a strong elitist strategy is used to update pheromone trails. Second, ants choose a solution component using the so-called "pseudo-random proportional rule"[57].

3. METHODOLOGY

3.1 INTRODUCTION

The enhancement of image steganography and the provision of a more secure system are the aims of the suggested system. ACO algorithms, steganography, and cryptography are used to achieve the improvement. Each block (m*m) in the image will have optimum pixels found using the ACS method. The highest optimized pixel will be chosen to include the encrypted secret message bits. Three stages make up the proposal.

a. Implementation a new method of LSB with modification on it to make steganography more secure.
b. Implementation DES algorithm to encrypt secret message.
c. Implementation ACS to find the optimal pixel in each block (m*m) which used for hide data bits. Figure (3.1) show general block diagrams of the proposed framework.

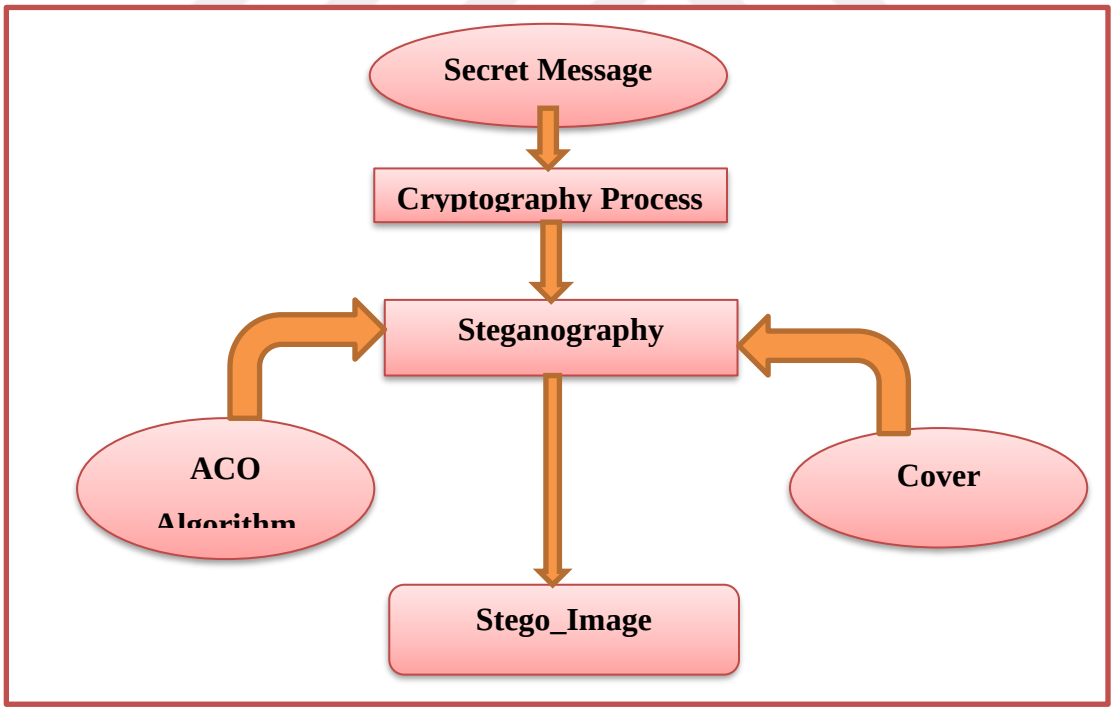

Figure 3.1: ACO And DES To Enhance Image Steganography.

3.2 STEGANOGRAPHY IN PROPOSED SYSTEM

In this part a new technique of LSB will be shown which is termed R(RGB-LSB). Figure (3.2 (a,b) explains how can embed and extract data in R(RGB-LSB):

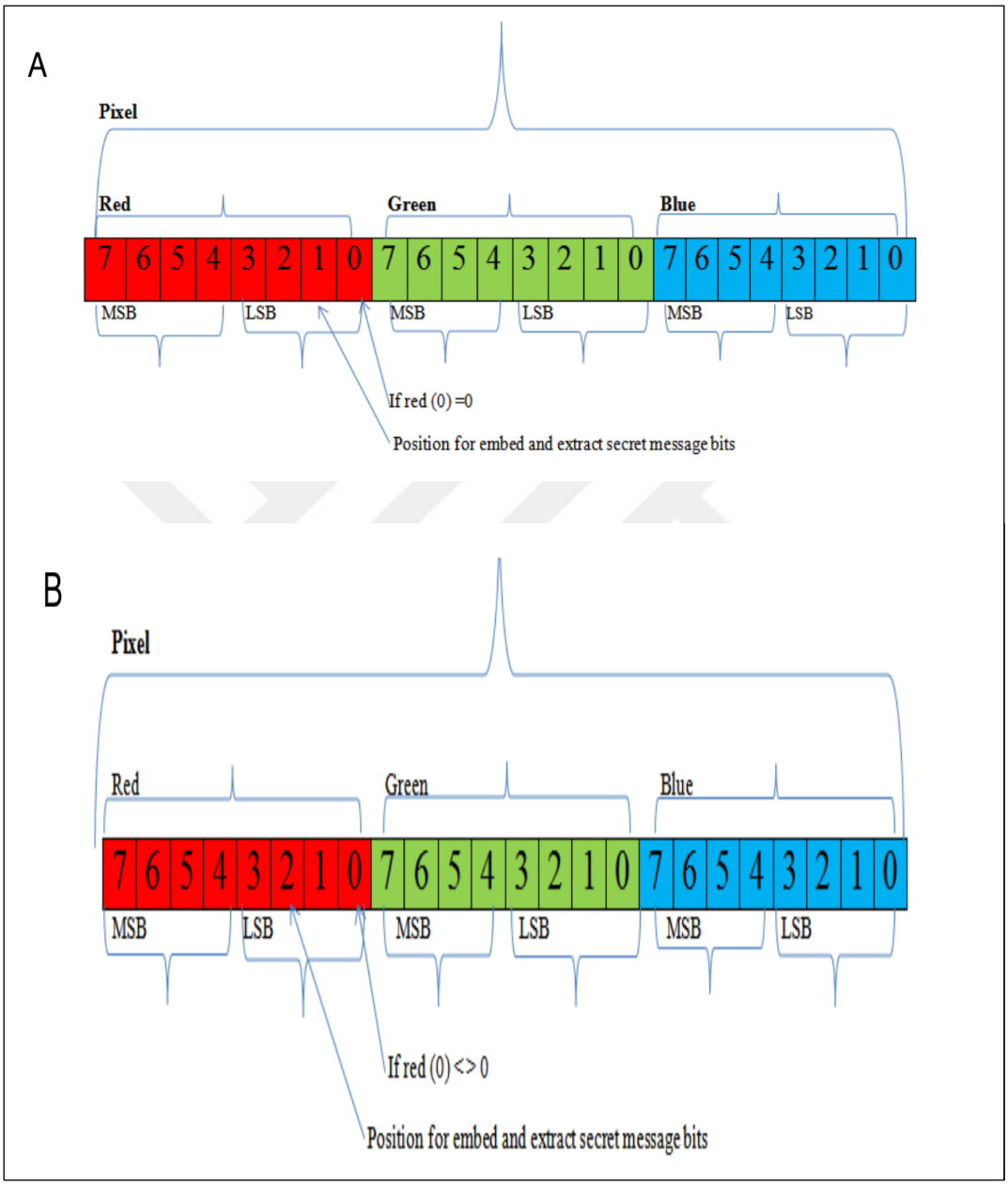

Figure 3.2: Both (A) and (B) are Embedding and Extraction in R(RGB-LSB).

3.3 CRYPTOGRAPHY IN PROPOSED SYSTEM

Encrypted secret message bits by using DES algorithm as shown in figure (3.3).). In the part will use breadth algorithm to produce key will used to encrypt secret data, this approach give good randomness for key. The results are system more secure and more resistance to hackers.

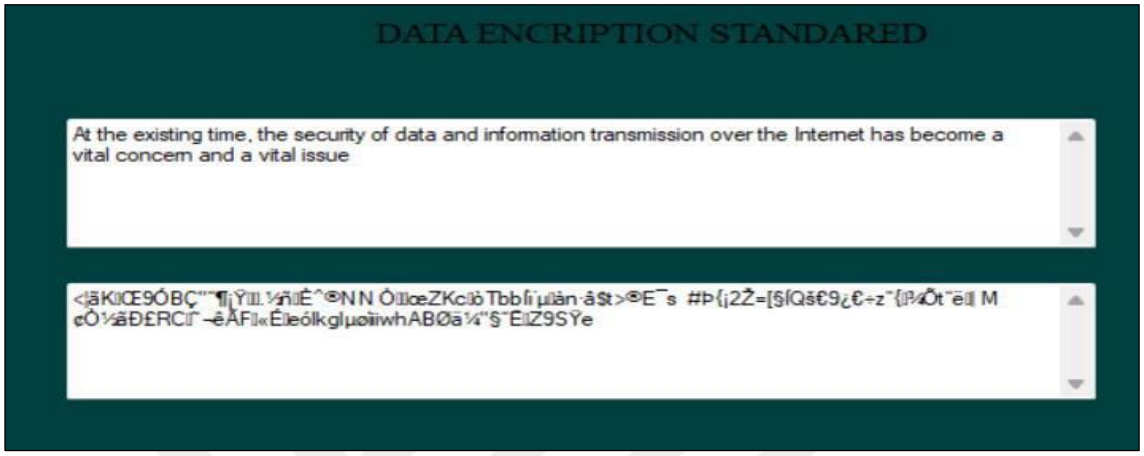

Figure 3.3: Use DES to Encrypted Secret Message.

The input is a string of eight characters, which will be converted to binary and given a 64-bit result. This 64-bit result will go into a fixed table that will be shared by both the sender and the receiver, as shown in the following table 3.1.

Table 3.1: Initial Key.

58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7

This table will be used to propagate the tree, the first 32 bits will be propagated to the left tree, and the second 32 will be to the right of the tree Then breadth algorithm will be used to generate a new 64 bits, which can be seen in the following figure (3.4).

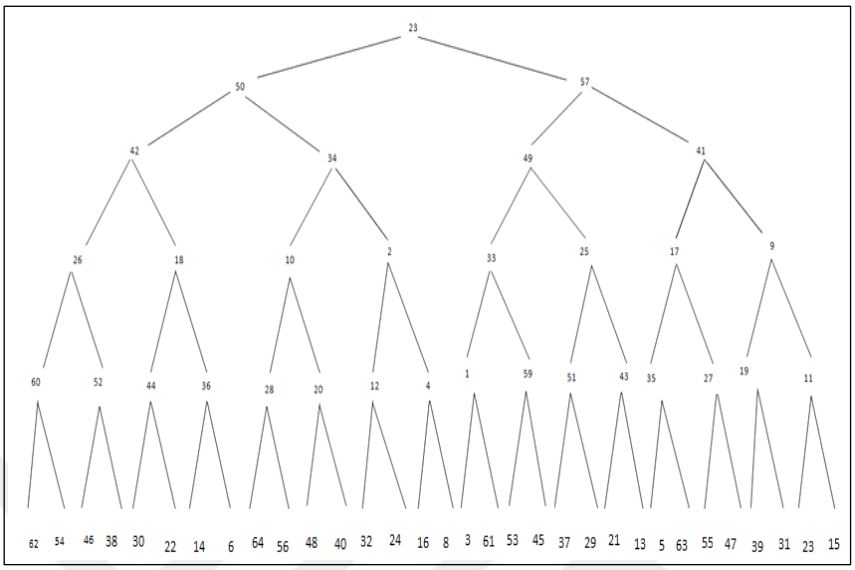

Figure 3.4: Breadth Algorithm to Generate Key.

When the breath algorithm runs in the tree, it can get a new subkey, as shown in the following table 3.2:

Table 3.2: Output Key.

58 50 57 42 39 49 41 26
28 10 2 33 25 17 9 60
52 44 36 24 20 12 4 1
59 51 43 35 27 29 11 62
54 46 38 30 22 14 6 64
56 48 40 32 24 16 8 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7

3.4 ANT COLONY OPTIMIZATION IN PROPOSED SYSTEM

To improve image steganography, we can use some of artificial intelligence such as ACO this algorithm combined Cryptography and steganography algorithms provide better results in (MSE and PSNR). Cover divided into number of blocks (horizontally) as shown in figure (3.5) and every block includes many of pixels each pixel is visited only once. ACS algorithm used to find an optimal pixel within one block. Optimal pixel cans obtained through finding the texture of colours between pixels in each block. Figure (3.6) explains how to find optimal pixel within block.

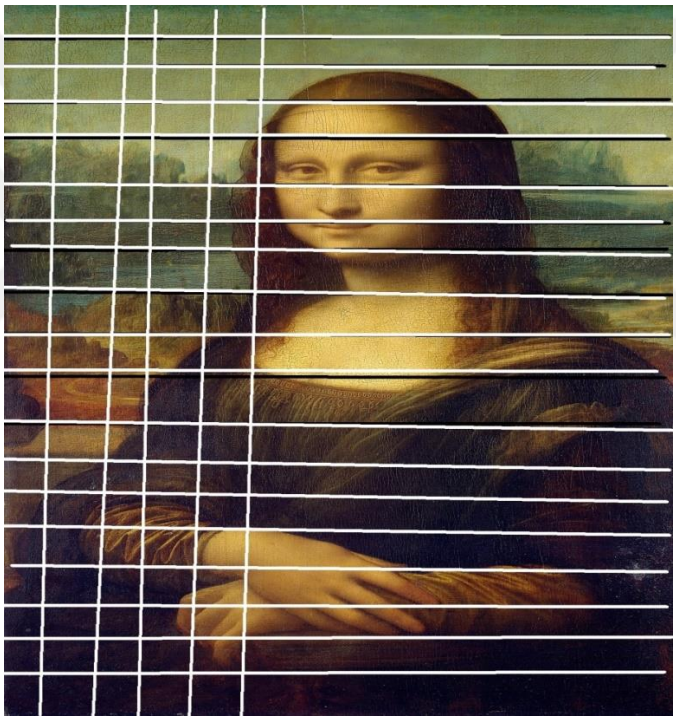

Figure 3.5: Divide Cover into Blocks (Horizontally).

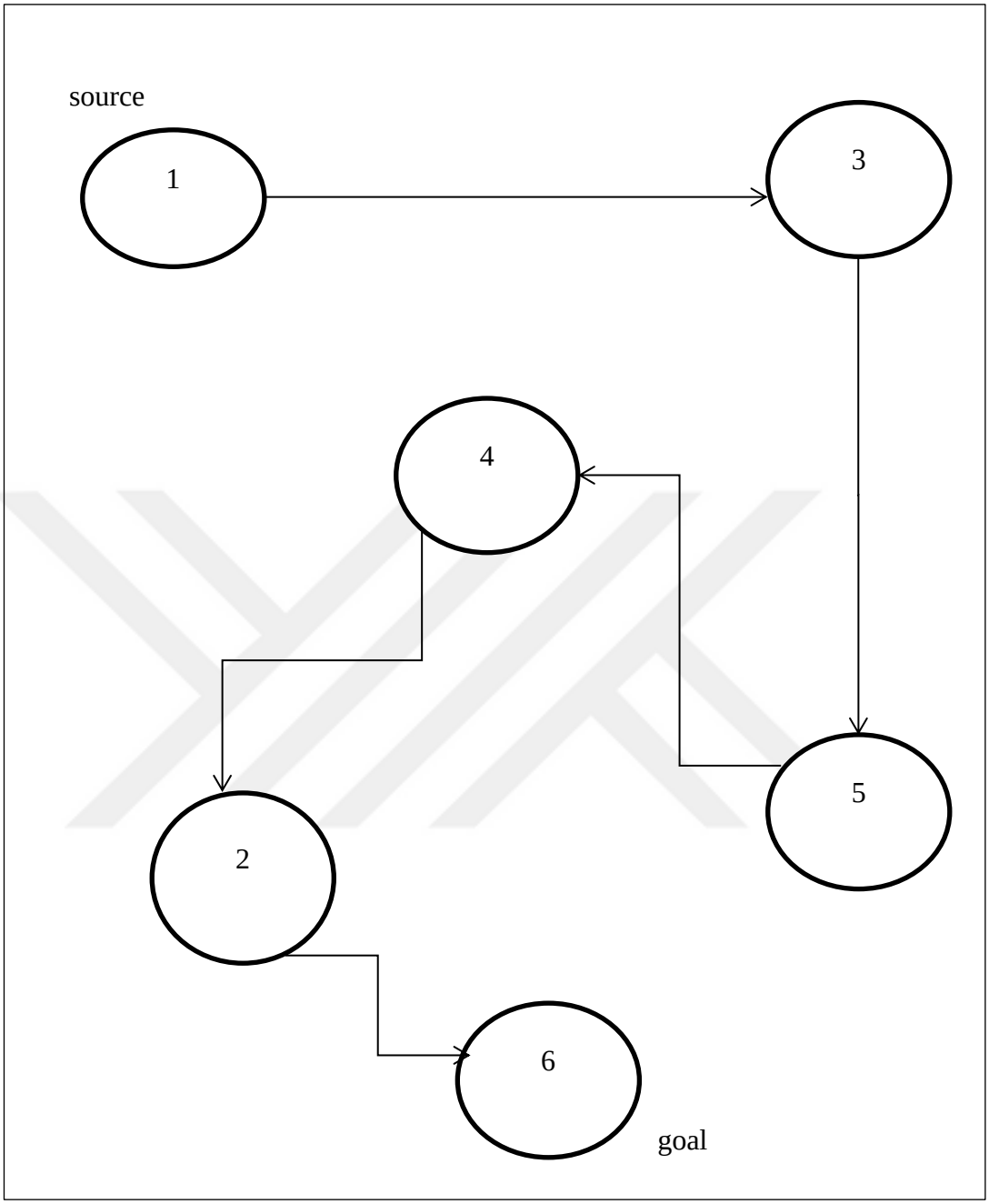

Figure 3.6: Pixels Within Block.

There is some information to how can employ ACO with steganography.

a. Block (5*5) will be used.
b. Calculate the capacity between the number of secret message bits and a cover as shown in equation (3.1).

$$\text{Capacity} = \text{cover size} / \text{number of pixel within block} \quad (3.1)$$

Capacity must be large than total number of secret message bits to ensure the security and quality.

c. After dividing the cover image in blocks (m*m), each block contains number of pixels, three bits of the secret message is embedded in each block. Figure (3.2) explains this:

d. Heuristic measure ηij : Calculated through finding MSE between pixels in cover and stego as shown in equation (3.2):

$$\eta_{ij} = 1/MSE \quad (3.2)$$

5 - Number of iterations = 5.

6 - Number of ants = 3.

7 - Each iteration the ants select pixels randomly.

8 - Alpha and Beta = 2.

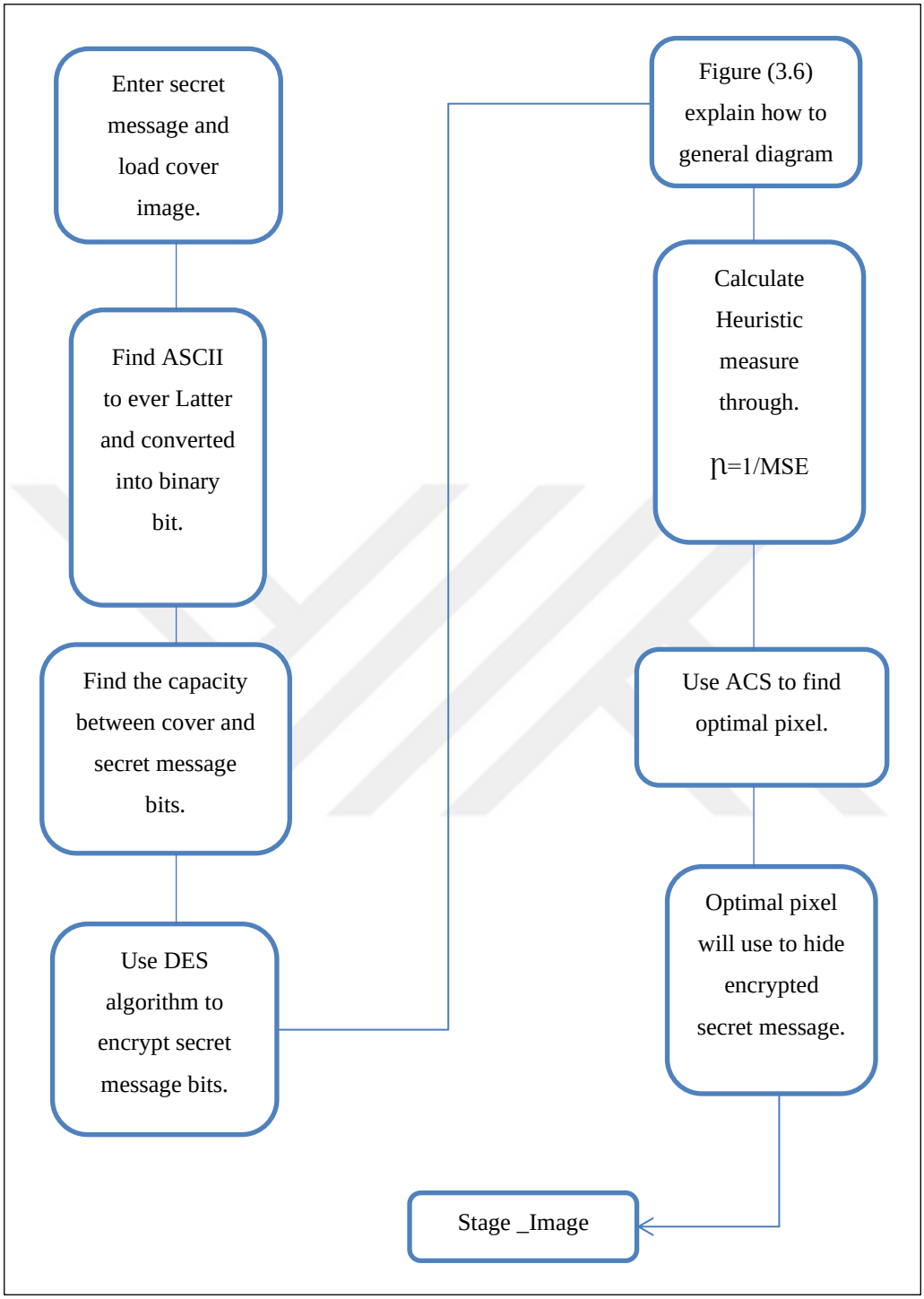

Figure 3.7: General Block Diagram of Proposed System.

4. EXPERIMENTAL RESULTS

4.1 INTRODUCTION

In this chapter we will explain the result of R(RGB-LSB) algorithm and proposed system (ACO with steganography) in details.

The proposed framework is built by using different dataset and secret message size. In the system will use (30 images different in type of the file format and size) and dataset of secret messages (three secret messages with different size). Figure (4.1(a,b)) display the images, Table (4.1) display the secret messages with their size and table (4.2) display the images file format and size.

The suggested system was developed in a Windows 7 environment with an Intel 2.50 GHz processor, 4.00 GB of Memory, and a 64-bit system type. The proposed system code was created using the Visual Basic.net 2010 and 2008 programming languages.

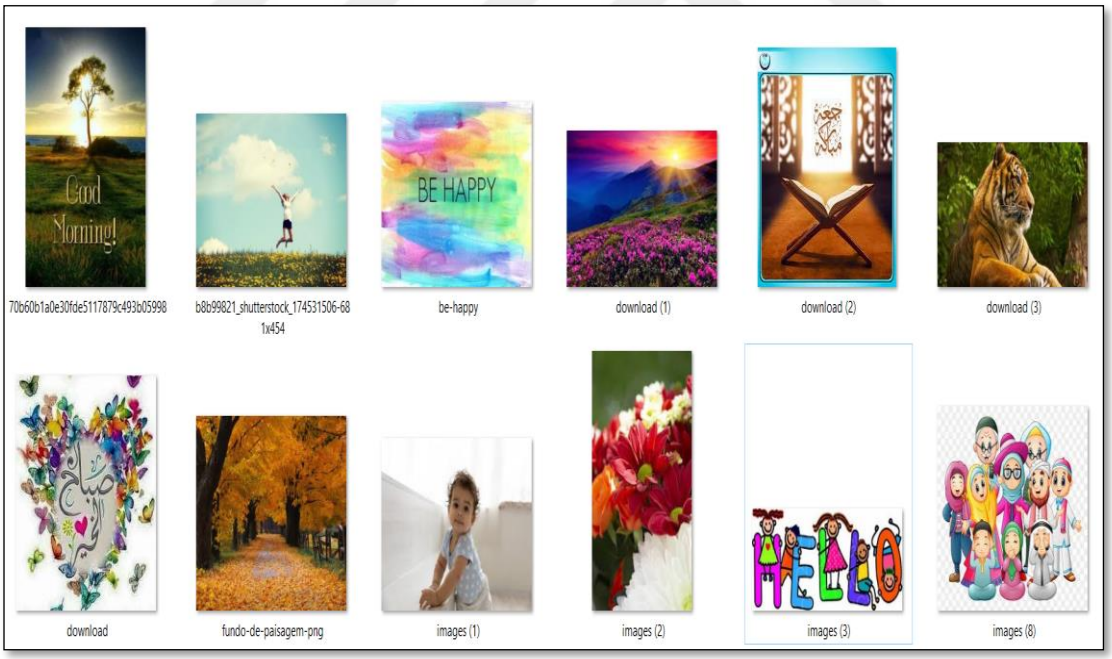

Figure 4.1: Images in Proposed System.

Table 4.1: Secret Message.

Number of Secret Message	Size (Byte)	Size (Bit)
Sec Msg 1	136	1088
Sec Msg 2	499	3992
Sec Msg 3	717	5736

Table 4.2: Images Characteristics.

Images Number	Images Size	File Format Type
1	704*880(80 KB)	JPG
2	681*454 (46KB)	JPG
3	500*345(51KB)	JPG
4	290*174(14KB)	JPG
5	225*225(10KB)	JPG
6	300*168(10KB)	JPG
7	228*221(12KB)	JPG
8	665*499(858KB)	PNG
9	275*183(5KB)	JPG
10	183*275(8KB)	JPG
11	358*141(19KB)	JPG
12	253*199(18KB)	JPG
13	259*194(11KB)	JPG
14	900*600(116KB)	JPG
15	840*525(155KB)	JPG

Table 4.2: Images Characteristics “table continued”

16	616*380(57KB)	JPG
17	300*200(139KB)	PNG
18	348*289(13KB)	PNG
19	720*480(159KB)	JPG
20	630*345(654KB)	BMP

4.2 EXPERIMENTAL RESULTS

To identify which algorithm has the highest quality, capacity, and security, experimental work comparing (R(RGB-LSB) with cryptography) and ACS with (R(RGB-LSB) with cryptography) will be shown in this part. used to guarantee superior quality and imperceptibility (security). In the suggested system, the ACO algorithm necessitates a large capacity since the image is separated into several blocks, and each block is utilized to conceal three bits of the secret message. Table (4.3) explains experimental results of (R(RGB-LSB) with cryptography) when using sec msg (1). Table (4.4) provides an explanation of experimental findings of (R(RGB-LSB) with cryptography) while utilizing sec msg. (2). Table (4.5) explains experimental results of (R(RGB-LSB) with cryptography) when using sec msg (3). The findings are provided in tables (4.3), (4.4), and (4.5). The (R(RGB-LSB) with cryptography) is excellent in terms of MSE and PSNR because the sec msg bits are incorporated in the values of the red, green, and blue colors, as illustrated in figure (4.2). (R(RGB-LSB) with cryptography) Even though it gets good quality, it gets a high imperceptible (poor security).

HISTOGRAM OF COVER

HISTOGRAM OF STAGIAIRES

Figure 4.2: Image and it Histogram

Table 4.3: Experimental Results When Using Sec Msg (1).

Cover No.	MSE	PSNR
1	0.010526	68.85765
2	0.01456635	61.665402
3	0.01067135	62.876468
4	0.01877550	61.50568
5	0.03741660	68.933505
6	0.0252056	68.568469
7	0.0078972	63.529179
8	0.0833660	70.561061
9	0.0522961	66.4324874
10	0.08114695	66.7114050
11	0.0476444	60.2884261
12	0.00845336	68.991904
13	0.019837	68.772894
14	0.0488087	71.67702
15	0.01194383	70.63068
16	0.0823714	66.773944
17	0.07257941	63.13779
18	0.00773041	68.661684
19	0.0272333	67.8442180
20	0.0151537	69.901038

Table 4.4: Experimental Results When Using Sec msg (2).

Cover No.	MSE	PSNR
1	0.01458125	65.332743
2	0.01662	66.70028
3	0.038283	60.188402
4	0.0451320	62.91546
5	0.0770444	609681
6	0.0091133	69.106505
7	0.009777	67.765590
8	0.0211087	62.87717
9	0.0119383	70.59106
10	0.0275714	65.553487
11	0.02717257	66.328050
12	0.061625	60.398426
13	0.0182703	68.5719040
14	0.0055306	66.733743
15	0.00723333	67.817284
16	0.02409375	62.359027
17	0.02296875	61.927468
18	0.06109	60.528568
19	0.007718	68.915505
20	0.0138125	69.922469

Table 4.5: Experimental Results When Using Sec Msg (3).

Cover No.	MSE	PSNR
1	0.0834488	62.73817
2	0.0593009	60.4352
3	0.172249	67.07760
4	0.0622875	67.07850
5	0.0381625	68.56429
6	0.0611015	69.31416
7	0.089214	69.32832
8	0.081467	67.49185
9	0.0622808	65.385
10	0.0572361	65.46540
11	0.094603	66.52134
12	0.007794	61.37726
13	0.08222	60.49948
14	0.0100213	70.1336
15	0.01975	71.23450
16	0.022118	69.30669
17	0.029958	69.26556
18	0.0311941	65.11245
19	0.0375	65.11587
20	0.091148	68.57512

In the proposed system, ACS algorithm with (R(RGB-LSB) with cryptography) Table (4.6) explains the number of pixels when use block (5*5).

Table 4.6: Number of Pixels.

Image no.	Number of pixels
1	17396
2	16008
3	10370
4	15181
5	10660
6	12559
7	15311
8	2176
9	11229
10	7844
11	11799
12	21847
13	18106
14	29754
15	16099
16	36225
17	19870
18	15660
19	17084
20	22362

Tables 4.7, 4.8, and 4.9 show the results of ACS's experiments. Table (4.7) shows that the image which a big size gives the high value of the MSE and PSNR as in colour shaded green. The relationship between the size of the second msg and the size of the image is very important. As seen in the following tables, this works best when the image is too huge for the secret messages.The status of the using block(5*5) gives a high random in ACS algorithm and thus will achieve high security as well as good quality as shown in figure (4.3).

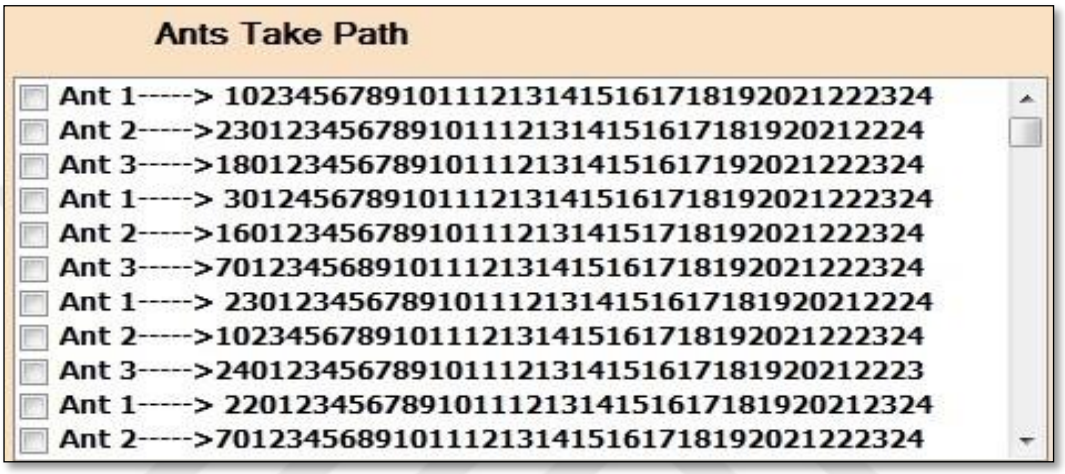

Figure 4.3: Randomization in ACS.

Table 4.7: Experimental Results When Using Sec Msg (1).

Cover No.	MSE	PSNR
1	0.0005175	80.08600171
2	0.001109259	76.30561020
3	0.0014756	78.07410581
4	0.00134231	79.18848924
5	0.001473215	76.40663
6	0.00125333	77.18045342
7	0.001034315	79..396128606
8	0.001222770	78.538732843

Table 4.7: Experimental Results When Using Sec Msg (1) “table continued”.

9	0.00131512	75.30141024
10	0.00159653	78.9261627
11	0.00103125	79.04516992
12	0.00136929	82.41836715
13	0.001018738	80.04495824
14	0.0012260705	83.93971187
15	0.00103125	77.05779825
16	0.00306375	76.97888349
17	0.0010232291	79.0817982
18	0.001209176	78.68440553
19	0.0012404040	79.25559711
20	0.00156656	80.0371199041

Table 4.8: Experimental Results When Using Sec Msg (2).

Cover No.	MSE	PSNR
1	0.00061041	79.61562
2	0.00452833	77.2376441
3	0.00266511	76.7791011
4	0.00235059	76.8578162
5	0.001192181	75.52575
6	0.003434	74.1081897
7	0.001436	77.23324908

Table 4.8: Experimental Results When Using Sec Msg (2) "table continued".

8	0.00166820	73.5245169
9	0.002641975	74.3432366
10	0.00033874	78.6512010
11	0.003059843	74.9296654
12	0.0005656178	76.3664476
13	0.001494849	80.1501648
14	0.001710705	81.8380118
15	0.002598	75.4590863
16	0.00144775	75.1340966
17	0.00294375	74.889265
18	0.00140354	76.9668685
19	0.00182263	75.9920054
20	0.001833	73.5823550

Table 4.9: Experimental Results When Using Sec Msg (3).

Cover No.	MSE	PSNR
1	0.00122607	77.5774235
2	0.00123293	76.3778568
3	0.002122143	77.8331692
4	0.002164751	75.849059
5	0.001933333	75.1663938
6	0.002115804	74.074401

Table 4.9: Experimental Results When Using Sec Msg (3) “table continued”.

7	0.001835402	77.3545914
8	0.001335987	74.48264
9	0.000722142	75.3432366
10	0.000791517	78.7318772
11	0.000243361	74.9704445
12	0.001980703	77.3913356
13	0.00121070	80.3214984
14	0.00188575	81.510118
15	0.00235	78.429840
16	0.003358645	77.1888978
17	0.00025051	75.9432159
18	0.00373141	74.9809006
19	0.002626	78.0324051
20	0.001193	79.6443440

Table (4.10) and figure (4.4(a,b)) shows the comparison among ACS algorithm and R(RGB-LSB) The results show that use ACS with DES and R(RGB-LSB) is the better in quality and security because depends on encryption algorithm, R(RGB-LSB) method, blocks and random pixel which is optimal to hide bits of secret message.

Table (4.10): Comparison Among ACS Algorithms and (R(RGB-LSB)).

	R(RGB-LSB)		ACS	
Cover No.	**MSE**	**PSNR**	**MSE**	**PSNR**
1	0.010526	68.85765	0.0005175	80.08600171
2	0.01456635	61.665402	0.001109259	76.30561020
3	0.01067135	62.876468	0.0014756	78.07410581
4	0.01877550	61.50568	0.00134231	79.18848924
5	0.03741660	68.933505	0.001473215	76.40492663
6	0.0252056	68.568469	0.00125333	77.18045342

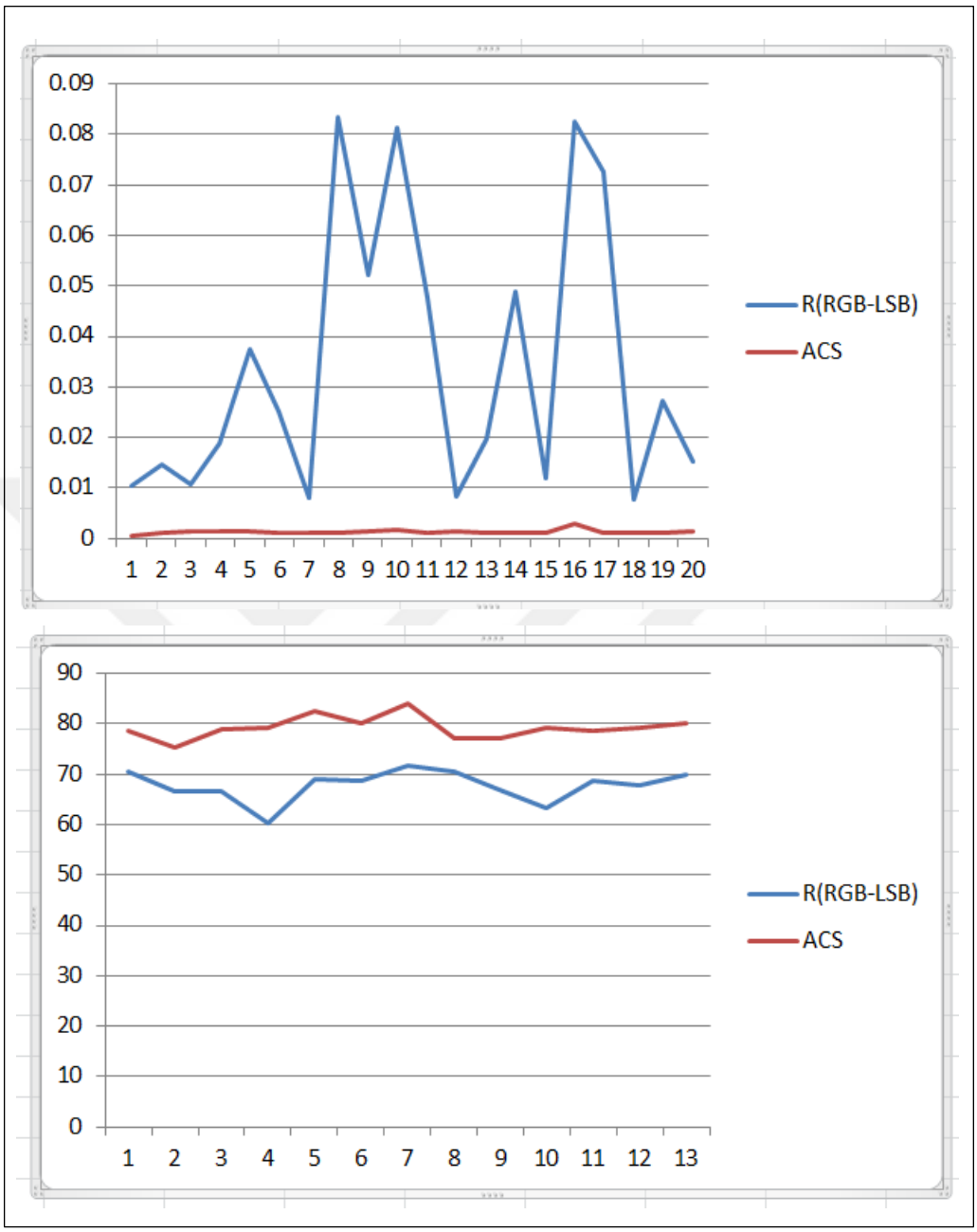

Figure 4.4: Comparison Among ACS Algorithms and R(RGB-LSB) with Cryptography (a) MSE Between (R(RGB-LSB) with Cryptography) and ACS while (b) PSNR between R(RGB-LSB) and ACS.

5. CONCLUSIONS

5.1 CONCLUSIONS

This thesis introduces new methods for image steganography to obtain secure way to exchange secret information. Three levels to in this thesis will be used. The fires one in steganography, will use simple approach of LSB which termed R(RGB-LSB) to increase security and quality. The second way is in cryptography to increase the complexity and make the system more secure and difficult to detect the secret information from attacks. The third way is in swam intelligence (ACO algorithm) will use ACS with security techniques (cryptography and steganography) to make the suggest system more powerful through increase the security and quality.

For hiding information R(RGB-LSB) provides a good security but provides a low quality. For encrypted data DES algorithm, it uses to increase security. ACO with previous algorithms provide good quality and security. With using breadth algorithm to generate the key Use ACS with hiding data provide similarity between pixels cover and stego_image this means high level of security and quality. The divided the image horizontally, number of iteration, blocks and ants is more appropriate in suggest system. ACO needs high capacity because the cover image divided into blocks and each block used to embed three bits from secret message.

In future work could be use another approach of ACO or another intelligence algorithms to obtain the optimal pixels and find appropriate way to solve the problem of capacity in ACO.

REFERENCES

[1] Nur Hadisukmana, R. (2020). An Approach of Securing Data using Combined Cryptography and Steganography. *International Journal of Mathematical Sciences and Computing*, *6*(1), 1–9. https://doi.org/10.5815/ijmsc.2020.01.01

[2] Al-Ataby, A., & Al-Naima, F. (2010). A Modified High Capacity Image Steganography Technique Based on Wavelet Transform. In *The International Arab Journal of Information Technology* (Vol. 7, Issue 4).

[3] Hamid, N., Yahya, A., Ahmad & Osamah, R. B., & Al-Qershi, M. M. (n.d.). Image Steganography Techniques: An Overview. In *International Journal of Computer Science and Security (IJCSS)* (Issue 6).

[4] Nassr, D. I., & Khamis, S. M. (2021). Applying Permutations and Cuckoo Search for Obtaining a New Steganography Approach in Spatial Domain. *International Journal of Network Security*, *23*(1), 67–76. https://doi.org/10.6633/IJNS.202101

[5] Muhammad, A., & Hikmat, R. (2016). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm. *International Journal of Computer Applications*, *143*(4), 11–17. https://doi.org/10.5120/ijca2016910143

[6] Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data Security Using Cryptography and Steganography Techniques. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 7, Issue 6). www.ijacsa.thesai.org

[7] Osman, O. M., Kanona, M. E. A., Hassan, M. K., Elkhair, A. A. E., & Mohamed, K. S. (2022). Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 327–335. https://doi.org/10.11591/eei.v11i1.3451

[8] Tayyeh, H. K., & Al-Jumaili, A. S. A. (2022). A combination of least significant bit and deflate compression for image steganography. *International Journal of Electrical and Computer Engineering*, *12*(1), 358–364. https://doi.org/10.11591/ijece.v12i1.pp358-364

[9] Dorigo M., Birattari M., and St¨utzle T.," Ant Colony Optimization Artificial Ant Computational Intelligence Technique", IEEE Computational Intelligence Magazine, Volume 1, Issue 4 November 2006.

[10] Duan, P., & AI, Y. (2016). Research on an Improved Ant Colony Optimization Algorithm and its Application. *International Journal of Hybrid Information Technology*, *9*(4), 223–234. https://doi.org/10.14257/ijhit.2016.9.4.20

[11] Fayeez, A. T. I., Subramaniam, S. K., Ramlee, R. A., & Anas, S. A. (n.d.). International Journal of Computing and Digital Systems A Critical Analysis of Heterogeneous Ant Colony Optimization for Combinatorial Optimization Problems. http://journals.uob.edu.bh

[12] Tayel M., Gamal A. and Shawky H., "A Proposed Implementation Method of an Audio Steganography Technique", Advanced Communication Technology (ICACT), February 3, 2016.

[13] Khan, S., Irfan, M. A., Arif, A., Rizvi, S. T. H., Gul, A., Naeem, M., & Ahmad, N. (2019). On hiding secret information in medium frequency DCT components using least significant bits steganography. *CMES - Computer Modeling in Engineering and Sciences*, *118*(3), 529–546. https://doi.org/10.31614/cmes.2019.06179

[14] Sarmah, D. K., & Kulkarni, A. J. (2019). Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography. *Journal of Information Security and Applications*, *45*, 90–106. https://doi.org/10.1016/j.jisa.2019.01.002

[15] Dezfouli M. A., Niksereshtt S. and Alavi S. E.," A New Image Steganography Method Based on Pixel Neighbors and 6 Most Significant Bit (MSB) Compare", Advances in Computer Science: an International Journal, Vol. 2, Issue 5, No.6 , November 2013.

[16] Saeed, J. N., Zeebaree, D. Q., Zebari, R. R., Abdulrazzaq, M., Haji, L. M., Zeebaree, S. R. M., Shukur, H. M., Zebari, D. A., Zeebaree, D. Q., Saeed, J. N., Zebari, N. A., & Al-Zebari, A. (n.d.). *Image Steganography Based on Swarm Intelligence Algorithms: A Survey Related papers Hiding Image by Using Cont ourlet Transform Diyar Q Zeebaree Facial Expression Recognit ion based on Hybrid Feat ure Ext ract ion Techniques wit h Different Classifie… Mult icomput er Mult icore Syst em Influence on Maximum Mult i-Processes Execut ion T ime Image Steganography Based on Swarm Intelligence Algorithms: A Survey*.

[17] Garg N. and Kaur K.," Hybrid Information Security Model For Cloud Storage Systems Using Hybrid Data Security Scheme", International Research Journal of Engineering and Technology (IRJET), Vol.: 03 Issue: 04 , April 2016.

[18] Assured_Data_Communication_Using_Cryptog. (n.d.-b).

[19] Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering*, *518*(5). https://doi.org/10.1088/1757-899X/518/5/052003

[20] Nassif Jassim, K., Khudhur Nsaif, A., Kuder Nseaf, A., Hazidar, A. H., Priambodo, B., Naf'An, E., Masril, M., Handriani, I., & Pratama Putra, Z. (2019). Hybrid cryptography and steganography method to embed encrypted text message within image. *Journal of Physics: Conference Series*, *1339*(1). https://doi.org/10.1088/1742-6596/1339/1/012061

[21] Bi, D., Kadry, S., & Kumar, P. M. (2020). Internet of things assisted public security management platform for urban transportation using hybridised cryptographic-integrated steganography. *IET Intelligent Transport Systems*, *14*(11), 1497–1506. https://doi.org/10.1049/iet-its.2019.0833

[22] Akhtar, A. (2019). Evolution of Ant Colony Optimization Algorithm -- A Brief Literature Review. http://arxiv.org/abs/1908.08007

[23] Skackauskas, J., Kalganova, T., Dear, I., & Janakram, M. (n.d.). XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE Dynamic Impact for Ant Colony Optimization algorithm.

[24] Zhou X. and Wang R.," Self-Evolving Ant Colony Optimization And Its Application To Traveling Salesman Problem", International Journal of Innovative Computing, Information and Control, Vol. 8, No. 12, December 2012.

[25] Melman, A., & Evsutin, O. (2021). On the Efficiency of Metaheuristic Optimization for Adaptive Image Steganography in the DFT Domain. *2021 17th International Symposium Problems of Redundancy in Information and Control Systems, REDUNDANCY 2021*, 49–54. https://doi.org/10.1109/REDUNDANCY52534.2021.9606459

[26] Akhtar N., Johri P. and Khan S.,” Enhancing the Security and Quality of LSB based Image Steganography”, International Conference on Computational Intelligence and Communication Networks, 2013.

[27] Jayaram, Ranganatha, & Anupama. (2011). Information Hiding Using Audio Steganography - A Survey. *The International Journal of Multimedia & Its Applications*, *3*(3), 86–96. https://doi.org/10.5121/ijma.2011.3308

[28] Awad W. S.,” Information Hiding Using Ant Colony Optimization Algorithm”, International Journal of Technology Diffusion, Vol 1, January-March 2011.

[29] Gupta S., Gujral G. and Aggarwal N.,” Enhanced Least Significant Bit algorithm For Image Steganography”, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

[30] Dalal, M., & Juneja, M. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. *Multimedia Tools and Applications*, *80*(4), 5723–5771. https://doi.org/10.1007/s11042-020-09929-9

[31] . Kaul N. and Chandra M.,” A Proposed Algorithm for Text in Image Steganography based on Character Pairing and Positioning”, International Journal of Computer Applications (0975 – 8887) Vol. 126, No.3, September 2015.

[32] Mohamed M. H. and Mohamed L. M.,” High Capacity Image Steganography Technique based on LSB Substitution Method”, Applied Mathematics and Information Sciences an International Journal, Vol. 10, No. 1, 2016.

[33] Mohapatra C. and Pandey M.,”A Review on current Methods and application of Digital image Steganography”, International Journal of Multidisciplinary Approach and Studies, Vol. 02, No.2, March – April, 2015.

[34] Mohapatra C. and Pandey M.,”A Review on current Methods and application of Digital image Steganography”, International Journal of Multidisciplinary Approach and Studies, Vol. 02, No.2, March – April, 2015.

[35] Shete K. H., Patil M. and Chitode J. S.,” Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA”, Published Online in MECS (http://www.mecs-press.org/), June 2016.

[36] Antonio, H., Prasad, P. W. C., & Alsadoon, A. (2019). Implementation of cryptography in steganography for enhanced security. *Multimedia Tools and Applications*, *78*(23), 32721–32734. https://doi.org/10.1007/s11042-019-7559-7

[37] Morkel, T., Eloff, J., & Olivier, M. (n.d.). *AN OVERVIEW OF IMAGE STEGANOGRAPHY*.

[38] Al-Tamimi A. T. and Alqobaty A. A.," Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm", International Journal of Computer Science and Information Security, Vol. 13, No. 1, January 2015.

[39] Swain G., " Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution", Indian Journal of Science and Technology, Vol. 7, September 2014.

[40] Mandal, J. K. (2012). Colour Image Steganography based on Pixel Value Differencing in Spatial Domain. *International Journal of Information Sciences and Techniques*, *2*(4), 83–93. https://doi.org/10.5121/ijist.2012.2408

[41] Jamdar A.S., Shah A.V., Gavali D.D. and Kurkute S.L.," Edge Adaptive Steganography Using DWT", International Journal of Engineering and Advanced Technology, Vol.-2, Issue 4, April 2013.

[42] Adee, R., & Mouratidis, H. (2022). A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*, *22*(3). https://doi.org/10.3390/s22031109

[43] 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). (2019a). IEEE.

[44] G, M. K., & Ravikumar, M. N. (2016). Color Image Encryption and Decryption Using DES Algorithm. *International Research Journal of Engineering and Technology*. www.irjet.net

[45] Mohammad, O. F., Shafry, M., Rahim, M., Rafeeq, S., Zeebaree, M., & Ahmed, F. Y. H. (2017). A Survey and Analysis of the Image Encryption Methods. In *International Journal of Applied Engineering Research* (Vol. 12, Issue 23). http://www.ripublication.com

[46] David Adeniji, O., Logunleko, K., Adeniji, O., & Logunleko, A. (2013). A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for

Information Security. *International Journal of Scientific Research in _____ Research Paper. Computer Science and Engineering, 8*(1), 45–51. https://www.researchgate.net/publication/342242454

[47] Alam Hossain, M., Biddut Hossain, M., Md Imtiaz, S., & Shafin Uddin, M. (2016). Performance Analysis of Different Cryptography Algorithms Researched on Security Challenges with Possible Solution Strategies in Cloud Computing View project smart healthcare system View project Performance Analysis of Different Cryptography Algorithms. In *International Journal of Advanced Research in Computer Science and Software Engineering* (Vol. 6, Issue 3). https://www.researchgate.net/publication/317258631

[48] Abood, O. G., & Guirguis, S. K. (2018). A Survey on Cryptography Algorithms. *International Journal of Scientific and Research Publications (IJSRP)*, *8*(7). https://doi.org/10.29322/ijsrp.8.7.2018.p7978

[49] Bedi, R. K., & Singh, A. (n.d.). *COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS*. https://www.researchgate.net/publication/323309169

[50] Zhao, D., Liu, L., Yu, F., Heidari, A. A., Wang, M., Oliva, D., Muhammad, K., & Chen, H. (2021). Ant colony optimization with horizontal and vertical crossover search: Fundamental visions for multi-threshold image segmentation. *Expert Systems with Applications*, *167*. https://doi.org/10.1016/j.eswa.2020.114122

[51] Piya, A. (n.d.). HIGH CAPACITY AND OPTIMIZED IMAGE STEGANOGRAPHY TECHNIQUE BASED ON ANT COLONY OPTIMIZATION ALGORITHM.

[52] Afshar A., Massoumi F., Afshar A. and Mariño M. A.," State of the Art Review of Ant Colony Optimization Applications in Water Resource Management", Springer, 1 July 2015.

[53] Monteiro M.S.R., Fontes D.B.M.M., Fontes F.A.C.C.," Ant Colony Optimization: a literature survey", FEB Research Journal, No. 474, ISSN. 0870-8541, December 2012.

[54] Ellabib I, Calamai P. and Basir O.," Exchange strategies for multiple Ant Colony System", Information Sciences: an International Journal, Elsevier, Vol. 177, Issue 5, March, 2007.

[55] Nwaogazie I.F., Agunwamba J.," Development of Ant Colony Optimization Software as a Solid Waste Management System", British Journal of Applied Science and Technology,Vol. 5, pp 1-19, January 2016.

[56] Garima S. and Shailja S.," A Study on Ant Colony Optimization (ACO)", IJMIE, Vol. 3, 18 June 2013.