REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

AN IMPROVED STEGANOGRAPHY SYSTEM BASED ON CONTRAST VARIATION WITH FIBONACCI DECOMPOSITION TO INCREASE IMPERCEPTIBILITY

Amjed Fadhil Hamody AL-BAYATI

Master's Thesis

Supervisor

Asst. Prof. Dr. Mesut ÇEVİK

Istanbul, 2023

AN IMPROVEMENT STEGANOGRAPHY SYSTEM BASED ON CONTRAST VARIATION WITH FIBONACCI DECOMPOSITION TO INCREASE IMPERCEPTIBILITY

Amjed Fadhil Hamody AL-BAYATI

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled AN IMPROVEMENT STEGANOGRAPHY SYSTEM BASED ON CONTRAST VARİATİON WİTH FİBONACCİ DECOMPOSİTİON TO INCREASE IMPERCEPTİBİLİTY prepared by AMJED FADHIL HAMODY AL-BAYATI and submitted on 18/12/2022 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering

Asst. Prof. Dr. Mesut ÇEVIK
Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Mesut ÇEVİK	Department of Electrical and Electronics Engineering, Altınbaş University	_______
Asst. Prof. Dr. Hasan ABDULKADER	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Hatice ÇOBAN	Department of Software Engineering, Doğuş University	_____

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

Submission date of the thesis to the Graduate Education Institute: ____/____/____

I hereby declare that all information 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.

Amjed Fadhil Hamody AL-BAYATI

Signature

DEDICATION

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents, whose words of encouragement and push for tenacity ring in my ears.

PREFACE

I might want to thank my administrator: Asst. Prof. Dr. Mesut ÇEVİK Please let me express my profound feeling of appreciation and gratefulness to both of you for the information: direction and unrestricted help you have given me. I want you to enjoy all that life has to offer and further achievements and accomplishments throughout your life.

ABSTRACT

AN IMPROVEMENT STEGANOGRAPHY SYSTEM BASED ON CONTRAST VARIATION WITH FIBONACCI DECOMPOSITION TO INCREASE IMPERCEPTIBILITY

AL-BAYATI, Amjed Fadhil Hamody
M.Sc., Electrical and Computer Engineering, Altınbaş University,
Supervisor: Asst. Prof. Dr. Mesut ÇEVİK
Date: 08/2023
Pages: 39

There are currently many obstacles in the way of the design and development of a reliable image steganography system. These include low capacity, weak robustness, and invisibility. Overcoming these restrictions requires enhancing the steganography system's capacity and security while keeping the signal-to-noise ratio high (PSNR). In light of these considerations, the purpose of this research is to create a technique to successfully embed secret data into a cover image, thereby realizing a strong steganography scheme. The planning and execution of the suggested method occurred in multiple stages. To boost the scheme's text security and payload capacity, a novel encryption approach dubbed shuffle the segments of secret message was integrated with an improved Huffman compression algorithm. To further strengthen the approach, the bit depth of each pixel was doubled from 8 to 12 using a Fibonacci-based picture transformation decomposition method. Third, the schemes stealthiest was bolstered by the use of an enhanced embedding technique by combining a random block/pixel selection with the implicit secret key generation. Experimental evaluations of the suggested scheme's performance are conducted to determine its stealthiest, security, robustness, and capacity. Against the proposed scheme, resistance is analysed for their resistance to non-structural, 2, and statistical steganography detection attacks. The acquired PSNR values indicated that the proposed technique was successful in achieving the higher imperceptibility and security than the reported findings while preserving the larger capacity. In a nutshell, the problems were

fixed since the proposed steganography system was superior to existing data hiding schemes on the market.

Keywords: UAV, ML, DL, LFD, CNN.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

AI	:	Artificial Intelligence
DL	:	Deep Learning
CNN	:	Convolutional Neural Network
PAN	:	Personal Area Network
LSB	:	Least Significant Bit
PVD	:	Pixel Value Differencing

1. INTRODUCTION

A general overview of information concealment and the impetus for this study are described here. The statement of the issue, research questions, research objectives, and study scope comes next. The study's contribution and relevance are outlined briefly as well. The thesis's structure is outlined at the end. Security issues around the concealment of information have garnered a lot of focus in the previous decade. Due to its vast application area in various disciplines of study, notably in image security and steganography, the security of hiding data in pictures has recently been appealing to the vision community. After the advent of the internet, data security has been a crucial component of any communication involving sensitive information. The literature is packed with techniques for keeping the message hidden.

Similarly, to steganography, "information hiding" refers to secretly transmitting information by embedding it inside seemingly innocuous visual or linguistic cues. Information can be concealed in various formats, including text, images, videos, audio, and protocols. Neither one is without flaws. However, photographs are often used in online media since they are readily accessible and straightforward to use [13]. Therefore, using images to conceal data has several advantages, including higher levels of security, more storage space, and the potential to fool would-be intruders. Steganography, the practice of secreting information within non-obvious formats, is illustrated in Figure 1.1, which shows the variety of host media that can conceal a message. Steganography refers to the practice of concealing information, often text, inside a medium such that it goes unnoticed. The capacity to store a lot of information and the fact that it's hard for hackers to peek at that information justify the usage of images as a hosting medium.

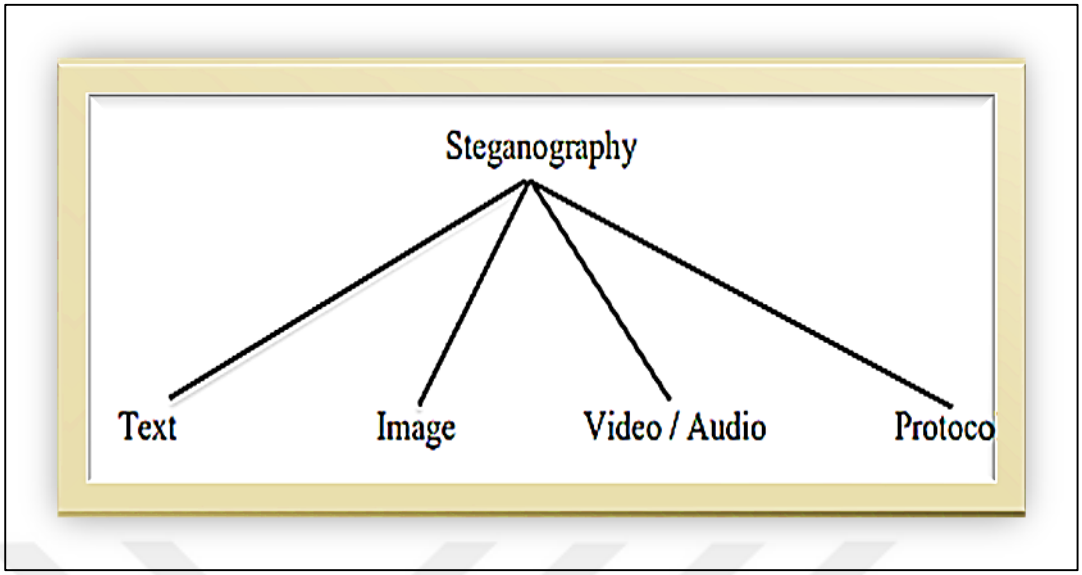

Figure 1.1: Areas of Steganography [1].

1.1 BACKGROUND

The Internet has become more critical in data transfer and communication. Concerns over personal privacy have increased the need for robust data security measures. Much of the data that passes via the Internet, from medical diagnoses to financial records to classified military plans, is very sensitive and must be protected at all costs. The practice of secretly storing data has roots that stretch back over a thousand years. In practice, it often fails since all it does is rely on a technique called encryption to make the contents of messages less visible. Suppressing the discovery of a communication's existence is often essential in competitive situations to prevent the suspicion of rivals [1]. As the Internet has developed, digital material has become a fast and efficient means of disseminating information (i.e., images, audio, textual documents, and videos). Developing forgeries tools and programs that enable criminals to steal, change, or delete data while in transit is a negative side effect of this progress. Information encryption and information concealing are the two primary tenets of the security system introduced to handle information security and avoid manipulation.

Cryptography is a method of encoding information so that only the intended recipient, via an "agreed upon" mechanism, can read the encoded message. However, cryptography is not foolproof since an unauthorized intruder might inject and combine unwanted data, which can interfere with the sent information. Further, encrypting sensitive data isn't always a good idea because it might invite unwanted attention. For this reason, there must sometimes be an

invisibility of communication. For this very reason, some kind of secret-keeping system is essential.

Hiding information is keeping a message hidden without making its presence obvious [2]. Steganography and watermarking, as seen in Figure 1.2, are two methods that can be used to accomplish this goal. In many ways, steganography and watermarking are the same but with opposite ends. Watermarking is commonly used to guard intellectual copyrights because it may preserve sensitive data while hiding or revealing the presence of communication. In contrast, steganography focuses on hiding the fact of communication and keeping hidden information safe from prying eyes, according to the authors [2, 3].

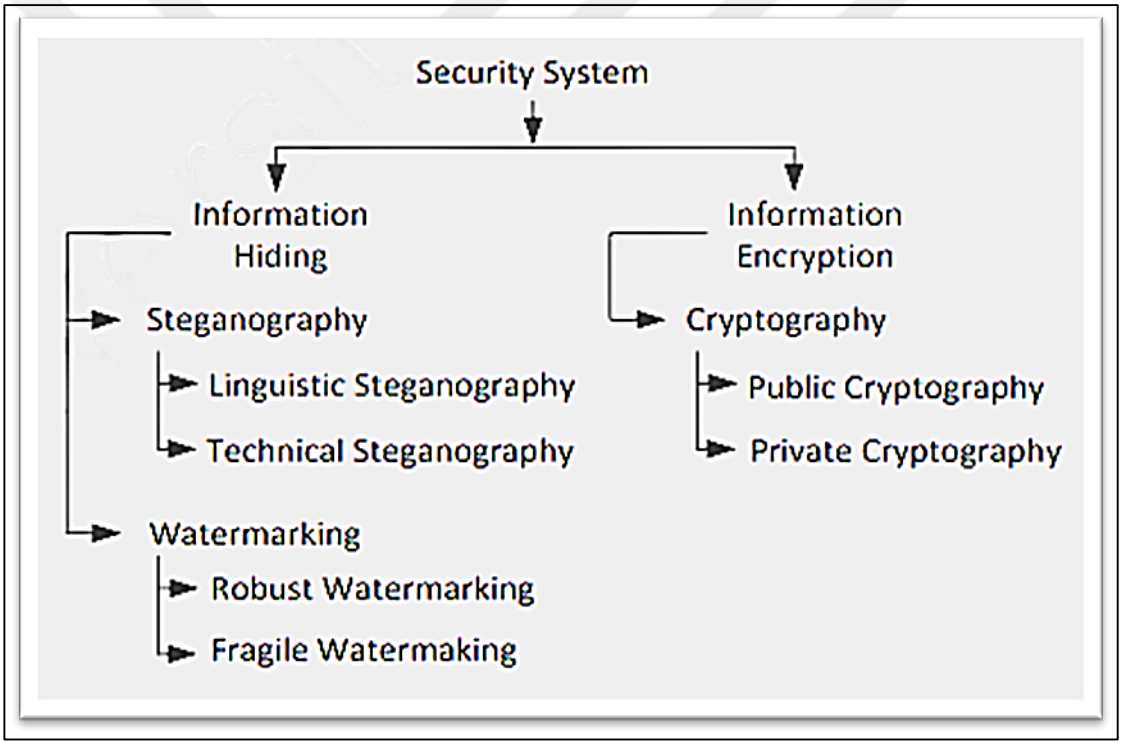

Figure 1.2: Structure of the Security System [2].

Regarding secret messaging, steganography has recently been the go-to method. In a combat zone, the military may swap top-secret maps or surveillance footage [4]. Medical pictures, such as X-rays and MRI scans, are encrypted whenever they are sent between medical facilities or stored on a server [5]. The same is true of commercial and monetary institutions like banks, which can safeguard their clients' account information against theft or other forms of unlawful usage. To effectively conceal its sensitive information, the communication mentioned above technologies necessitates digital steganography.

Furthermore, the academic community has a vested interest. The graph also shows the academic scholars' interest in steganography and its equivalent, as shown in Figure 1.3. The overall graph displays the fluctuating levels of interest; however, since 2010, this field has once more demonstrated a more significant and more constant level of interest from the scientific community, as seen by the rising number of publications published.

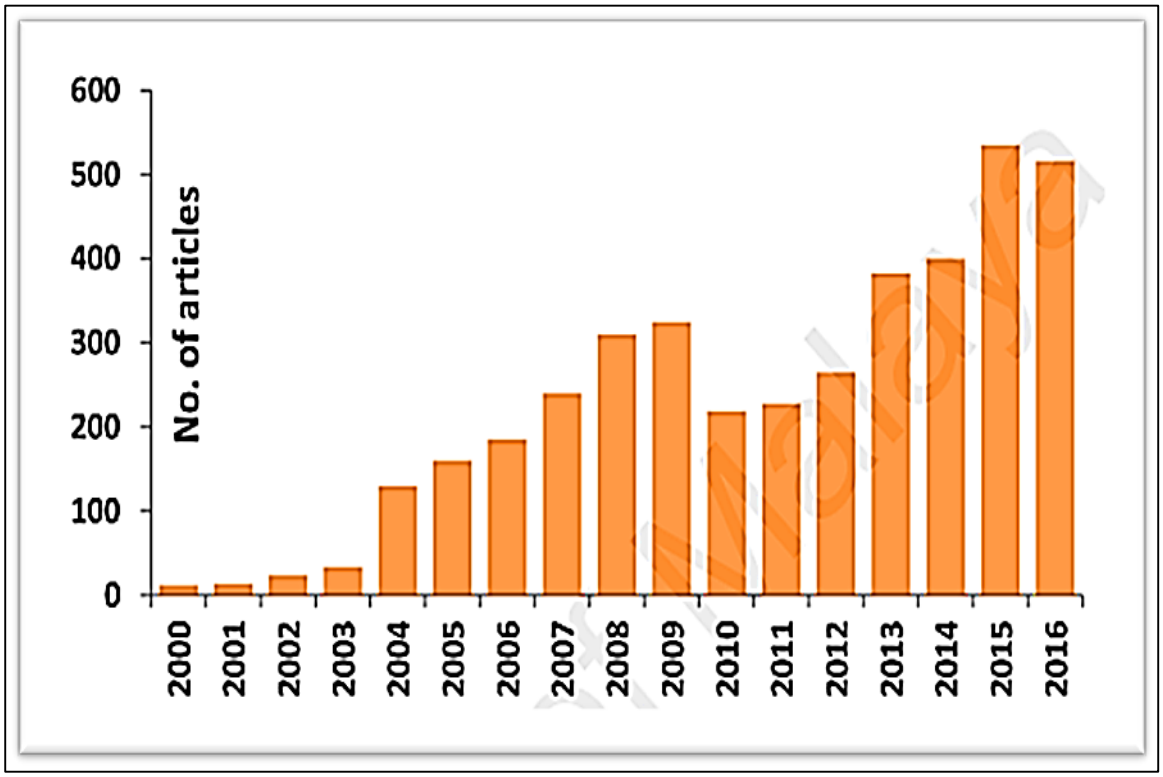

Figure 1.3: The Number of Annual Journals and Conferences Listed on "Web of Science" Publications With "Steganography" or "Steganalysis" in the Title [6].

Furthermore, the choice of the medium is crucial in the steganography mechanism. The authors claimed that the ideal medium for encoding secret information must have two characteristics [6]. The medium must be widely used, and any modifications must be imperceptible to outsiders. To the author's knowledge, the picture is the media most frequently utilized in digital steganography literature now in publication. Meanwhile, the photographs are freely accessible thanks to cutting-edge, affordable hardware and low-cost internet infrastructure. The picture also has a high rate of redundancy, which enables unseen effects to be used to hide the hidden data. Therefore, image-based steganography is the main emphasis of this study. The spatial and transform domains of picture steganography and full descriptions of each component are provided in Chapter 2.

Do the following primary goals assess the most typical success criteria for every image-based steganography method: How much embedding space in a stego-image payload can be accommodated? Second, imperceptibility, or how similar to the original/cover picture, the stego-image is perceptual. How can a stego-image withstand various steganalysis detection attacks? This is the third security question. To retain the best ratio of capacity, image quality, and security, the optimum steganographic approach must thus achieve the abovementioned goals concurrently or, at the very least, maintain balance.

Different sorts of picture steganography techniques are used to accomplish the aforementioned steganographic goals, and they are discussed in various works of literature. Least Significant Bit (LSB), Pixel Value Differencing (PVD), Exploiting Modification Directions (EMD), Pixel Pair Matching (PPM), Prediction Error Edge Based, Histogram Based, and Hybrid Steganographic Algorithms are all prevalent steganography techniques [3].

The primary emphasis of this research will be on the hybrid steganographic techniques; using a pixel value decomposition technique based on the Fibonacci sequence will increase the security of picture steganography. The system's security will be increased by switching the LSB to an unusual form.

1.2 PROBLEM STATEMENT

Automating the creation of analytical models is the goal of machine learning, a data-analysis technique [7]. Algorithms can gather information about a machine's past actions and then provide that information to the machine to "learn" (emulate) the intended actions. In addition, the machine may be trained to estimate or forecast operational states by analysing the collected data.

Among the numerous replacement and pixel, differencing-based steganographic algorithms published to achieve high capacity, imperceptibility, and security are as follows in the literature. Data concealing techniques are under the umbrella term of steganography, also known as the "art of covert concealment" under the guise of a carrier signal [8, 9].

Previous studies and hackers are familiar with the practice of relying on the least significant bit (LSB) of an image pixel, and random ordering and algorithms that rely on this method have

become inadequate in terms of security due to the limitations and conditions of random functions, which continue to be a weakness [10].

Changes in the crucial region of the pixel, as well as the overall image balance and distortion, affect how much of a difference may be made in the LSB before they become perceptible to the human eye. The data embedding method to a picture must be modified since it directly impacts the image's clarity in addition to the amount of data included [11].

There is a flaw in the hiding operations; the amount of concealed data in the picture is affected by the concealing technology in the LSB and the logical processes that take place there [12].

1.3 RESEARCH OBJECTIVES

The main goal of this research is to improve the security of hiding information in an image by using a new embedding method based on contrast variation with Fibonacci decomposition. Therefore, this proposal is carried out to fulfil the following objectives:

a. To improve image steganography security by using an algorithm based on Fibonacci decomposition for pixels' value. Changing the LSB to an unfamiliar form will increase the system's security.

b. To increase the imperceptibility of the system by a new embedding strategy to make balance between payload capacity and image quality.

1.4 RESEARCH CONTRIBUTIONS

To improve the imperceptibility and reduce the ratio (MSE) and thus increase (PSNR), we will use the variance technique as a condition in the embedding process, and this is applied by randomly choosing two neighbouring pixels from the cover image, one of them has a high-intensity value and the other low-intensity, and the difference between the two pixels value is determined in advance. For example, if we set the value of the difference to 50, any two neighbouring pixels and the difference between their intensity of 50 will embed the secret code in them.

The secret code will be embedded in the pixel based on the value of the intensity of the two pixels, where if the value of the secret code is (1), it will be included in the low-intensity pixel, but if the secret code value is (0), it will be included in the high-intensity pixel.

To avoid standard embedding, such existing method that embeds directly in the LSB of the pixels, we aim to embed in a different way which depends on decimal embedding, not digital like before, in addition to using Fibonacci decomposition to analyse the pixel value in 12 bits instead of 8 bits in binary decomposition.

1.5 RESEARCH QUESTIONS

a. The study's primary research questions are as follows.
b. What method will be used to improve the security of image steganography?
c. How to use the Fibonacci decomposition to be the numerical value of the 12-bit pixel?
d. How to embed the secret text or watermark into an image?

1.6 THESIS OUTLINE

This is the outline of the thesis: In Section 2, we examine the current work related to stenographic methods for images. In Section 3, we provide a complete description of the proposed approach. In Section 4, we provide a thorough explanation of our model and its implementation. In Section 5, we run our model simulations and record the results. Finally, in Section 6, we draw a line under our work and consider its potential future applications.

2. LITERATURE REVIEW

2.1 CHAPTER OVERVIEW

This chapter provides a brief description of some of the most common image stenographic techniques.

2.1.1 Steganographic Algorithms

Over time, advances in steganography and Steg system design have made it possible to conceal data transmission. However, capacity, complexity, and security must be considered when deciding on a technique. Therefore, there is no one steganographic technique that can meet all the needs. The procedures used in steganography often include substituting a pseudorandom secret message for a noise component of a digital picture and are typically categorized according to the domain into which the data was entered. In the spatial domain, the concealed message is embedded directly, and the most prevalent approach is the LSB. However, the LSB is notoriously vulnerable to visual and statistical assaults; thus, new steganalysis techniques have had to be developed to compensate. More information on the most common types of steganography is provided below.

2.1.2 The Least Significant Bit Family

Because of its ease of usage, the LSB approach is the most popular. The incapacity of the human eye to detect subtle variations at the pixel level is exploited by LSB, as was discussed in Chapter 2. When an image is embedded, its least significant bit is swapped out for message bits in the spatial domain, making it vulnerable to noise and transportation faults. Pseudorandom or sequential replacement is both possible. Each cover image pixel is updated sequentially with the embedded bits in the succeeding replacement.

In contrast, pseudorandom replacement uses a key as input to a random number generator, changing each pixel's specification number. Data concealed by the LSB technique is vulnerable to nearly every picture change, even if security measures are strictly adhered to [14]. Because the LSB method is applied to noise, the result will likely be affected by further compression, filtration, etc.

2.1.2.1 LSB+

As a defence against the histogram attack, LSB+ embeds a few extra bits on purpose so that the histogram appears natural [15]

2.1.2.2 LSB++

By making fewer adjustments to the cover image's perceptual and statistical characteristics, the LSB++ improves upon the LSB+ [16].

2.1.2.3 LSB matching

If the private bit doesn't resemble the LSB of the covering image's pixels, the LSB Matching technique adjusts the pixel values by adding or removing one. In LSB, there is an equal chance of either raising or reducing a pixel's value, but this imbalance artifact is eliminated [17].

2.1.2.4 LSB matching revisited

This technique can eliminate the asymmetry trait brought on by LSB since it only involves embedding data for a single set of pixels at a time [18].

2.1.2.5 Steghide

The Steghide LSB implementation for pictures is another popular option. Applying graph theory slightly adjusts the original method to modify pixels less frequently. The communication is encrypted and compressed before embedding it for extra safety. Afterward, a password-based key derivation mechanism generates a pseudorandom number sequence. The LSB of the cover pixels, where this sequence resides, will hold some of the messages. The least significant bit (LSB) that differs from the bit to embed is examined for exchange with another LSB that is the same as the bit to embed to increase concealment. A graph governs the process, where the vertices stand for the potential for change and the edges for potential trades. Once both parties have finished exchanging information, the rest message bits are encoded in place of the LSB [19], [20].

2.1.2.6 S-uniward

As the total absolute difference between the wavelet coefficients used to depict the cover and stego pictures, UNIWARD is a universal distortion function. To achieve its results, UNIWARD solely uses wavelet coefficients that operate in the highest frequency range. The spatial variant,

known as S-UNIWARD [21], conceals information as pixel values. Some peculiar behaviors are displayed by U-UNIWARD, such as the formation of interlaced stripes of high and low embedding probability in texturized and noisier areas. The embedded probabilities have been accused of being a potential security risk. However, there is research that demonstrates the method's durability [22].

2.1.2.7 Jphide and jpseek

The author of this study also created JPHide (for embedding) and JPSeek (for extraction), two more famous JPEG steganographic implementations based on LSB [23]. Instead of altering LSB pixels, JPHide inserts a hidden message using LSB overwriting quasi-quantized DCT coefficients, as employed by the JPEG method. A pseudo-random numbers maker that a password could influence as the seed is used to determine the DCT coefficients inserted into the data stream. The Blowfish algorithm is used for LSB randomized and encryption, which means that the location of the bits of the encrypted file is chosen randomly. In addition to the least significant bits (LSBs) of the chosen coefficients, it should be noted that, when switched to that mode, JPHide allows for the insertion in the second least significant bit as well as modifying the bits of the second least significant bit-plane [24].

2.1.2.8 F5

A matrix encoding and subtraction technique, F5, is to ensconce convert only non-zero bits into DCT coefficients by reducing the absolute value of that number by one [25]. It employs matrix encoding to conceal previously permuted data to maximize efficiency, changing the cover picture as little as possible for every given message. Therefore, the amount of modifications during embedding is decreased, making matrix encoding more effective.

2.1.2.9 Spatial domain

Data embedding is straightforward in the spatial domain, often called the picture domain. It's possible to encode information in individual picture pixels' hue, saturation, hue-magnitude relationship, etc., [26].

Unlike compression algorithms, which only permit restoration to estimate the original data, the compression ratio is a type of compression algorithm that permits optimally retrieving and reconstructing the original data and returning it as before compression, making spatial domain

techniques like (LSB), (PVD), etc. applicable to a wide range of lossless media [28]. This part discussed the many spatial domain steganographic methods now in use, as well as a brief overview of the research done in this area and the progress made in recent years.

2.1.2.10 Pixel value differencing

Steganography in the prominent edge direction is one of the approaches or algorithms that can take advantage of the human visual system to conceal massive quantities of data. The number of hidden bits is calculated from the difference in value between two adjacent pixels in a block [28].

In the research on image steganography by the authors, the upper left pixel of that block combines a certain number of bits to the underground bit stream, using a modified form of PVD in which the inclusion of confidential data is in both vertical and horizontal edges, the confidential data is enclosed by the other pixels of the same block. 2x2 non-overlapping pixel blocks are used to segment cover pictures. Results showed that the method was high-performing compared to earlier studies, with average values for the PSNR and SSIM complex wavelet indices of 1.4 dB and 0.9 dB, and 11.6% and 8.5%, respectively [29]. Additionally, the imperceptibility was improved over earlier studies with an average increase of 13.6%.

Using MPVD, LSB replacement, Encryption Standard, and lossless compression, the authors present a way to conceal high-capacity data. Secret information is first compressed by algorithmic encoding before being encrypted via AES technology, LSB replacement, and MPVD [30]. Experimental results showed that the proposed method was superior to the existing methods, allowing an extra 214132 bits to be embedded by using compression and (MPVD); compression provided a 22% higher percentage in the embedding ability, while encryption and MPVD improved the embedding ability by 25%. Furthermore, the method provided high levels of visual quality, with an average of 36.38 dB at 4.00 bpp, and they met all of the requirements set forth by the researchers (RS).

2.1.3 Machine Learning in Steganalysis

Optimal detectors are used by most classic steganography detection methods [31]. However, machine learning, specifically SVMs and ANNs, has recently become the norm in steganalysis.

Put differently, using a statistical model of cover objects, determine which statistical test is best about some criterion.

In both the spatial and transform domains, SVM is used as a classifier by the authors of this research [32]. The author of this study has created a steganalysis technique based on a spatial domain SVM classifier with a Gaussian kernel, with an emphasis on detecting anomalous pixels [33]. The authors recently employed linear, polynomial, and Gaussian SVMs' kernels to detect the stego picture with 73% accuracy and estimate the length of the concealed message with 33.6% accuracy [34]. Recent work uses the Spatial domain Rich Model as a feature extractor and SVM as a classifier to improve S-detection UNIWARD's error rate to about 42% [35].

There has been a lot of work on steganalysis using ANNs. Authors examined a particular type of DL framework in picture steganalysis [36], whereas studies [37, 38, and 39] developed CNN-based steganalysis for the BOSS Base dataset and focused on the spatial domain. In CNN-based steganalysis, a well-designed neural network is used to construct a feature extractor/classifier that operates from beginning to finish. In this study [40], the accuracy of J-UNIWARD (UNIWARD algorithm applied in transform domain) yielded 72.9% by utilizing Convolutional DCTR kernels, while in [41], testing error for steganalysis using Combined CNN was 45%, and detection error was 42.93%).

In the field of visual steganalysis, Neural Networks are very effective. Multi-channel neural networks allow S-UNIWARD steganalysis to achieve 81.55% detection accuracy, as recently demonstrated by [42].

Compared to SVMs or ANNs, FL and GAs approaches are in their infancy. New developments in image processing and steganography, however [43, 44, and 45], have been made in recent years.

2.1.4 Research Summary

Many steganographic techniques have been developed as steganography has grown in popularity. Also, there have been attempts to streamline the steganographic process using automation. This chapter offers a high-level overview of steganography.

The steganographic review, on the other hand, demonstrates how challenging it is to find ways to improve upon existing approaches. Although various steganalysis approaches have been developed to uncover hidden data, much work must be done to decipher messages. In addition, the classification stage in contemporary steganalysis accounts for the importance of machine learning.

3. MATERIALS AND METHODS

3.1 GENERAL INTRODUCTION

Any steganography system includes three main stages pre-processing stage, the embedding stage, and finally evaluation stage. In the first stage, an image is selected to encode a hidden message. For this purpose, first, we perform pre-processing of the input data. We must prepare the secret message and cover image in the pre-processing stage. The proposed method converts messages into binary bits and images into Fibonacci decomposition. For embedding, we contribute the embedding position within image pixels in terms of contrast variation. Evaluation of the system used three critical criteria Peak Signal Noise Ratio (PSNR), measuring the quality of the image and Human Visual System (HVS) to stand against any attack, and Capacity Detection (CD). The flow chart of the proposed embedding process algorithm is depicted in Figure 3.1. The main aim of this study is to improve the security of image steganography by using an algorithm based on Fibonacci decomposition for pixels' values. Changing the LSB to an unfamiliar form will increase the system's security.

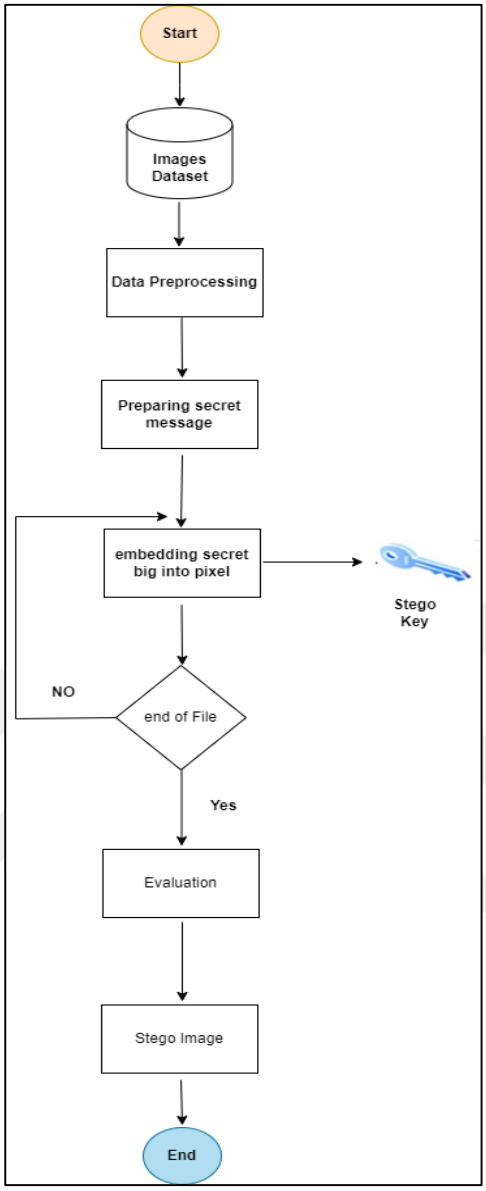

Figure 3.1: The Flow Chart of the Proposed Embedding Process Algorithm [9].

The input image consists of small units called pixels, which are numerical values that reflect the color luminance in the image. The numerical peak of a pixel is from 0 to 255, and to be accepted as a numeric value, it takes 8 bits. In our proposed system, we get out of the standard method and use the Fibonacci decomposition to be the numerical value of the 12-bit pixel, as shown in Figure 3.2. First, we take an input image and perform some preprocessing steps. After that, the proposed approach is preparing the secret message. Now, Fibonacci decomposition is used. After that, the evaluation is used, and the stego image is found.

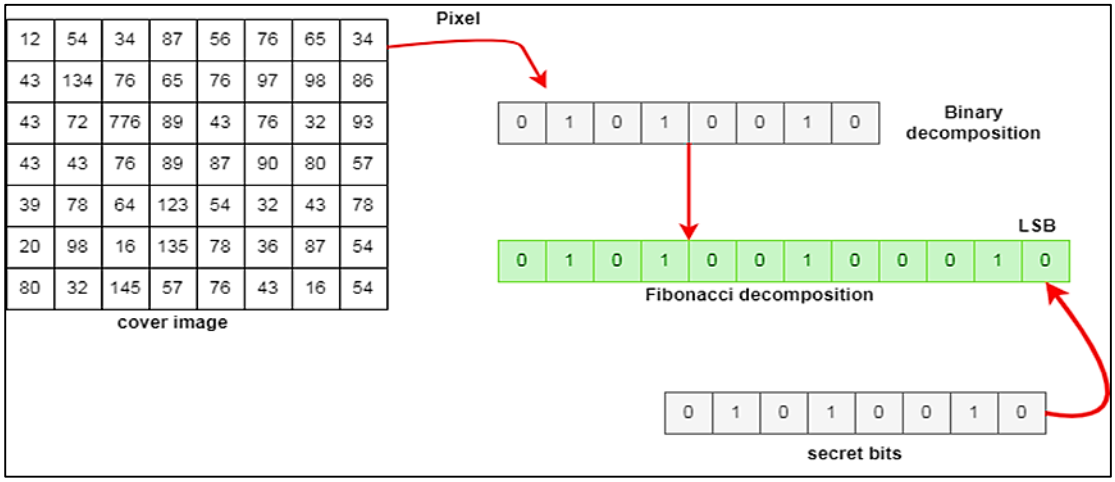

Figure 3.2: Flow of Fibonacci Decomposition [15].

3.2 DATA PREPROCESSING

The suggested steganography system relies heavily on the pre-processing stage to easily identify the secrecy of the hidden message. Thus, at this stage, the cover image and the secret message are both being prepared simultaneously. An effective embedding procedure, known as cover image preparation, is achieved by applying a pre-processing stage to the proposed scheme prior to the embedding process. The methods of picture splitting and image transformation decomposition are broken down in depth below.

3.2.1 Image Splitting Technique

Before doing anything with the provided image, this stage involved selecting and analysing it. First, an image is chosen at random from the available set. Now, the suggested system deals with 8-bit greyscale images directly. If the image is 24-bit RGB, however, the suggested approach first performs a channel-by-channel analysis of the RGB image to evaluate whether or not it is suitable for further implementation. After the separation process is complete, the single 8-bit matrix's picture channels all grow to the size of the original image. Simply said, an 8-bit image is created in this stage for each of the three channels. In order to determine which of the three channels has the secret bit, the system must examine all three values for each pixel.

3.3 STEGANOGRAPHY SYSTEM

The steganography system consists of two side's sender that embeds hidden text and the receiver that extract the secret message from the stego image. Extracting on the contrary of

embedding in terms of algorithm. The flow chart of the proposed extraction process algorithm is depicted in Figure 3.3, and the general architecture of the steganographic system is shown in Figure 3.4. Assume that you have a message that you want to convey to someone using the steganographic transmission. To conceal the embedded message, the sender must first input a cover message into the stego-system. The term "embedded message" refers to a secret message. Something buried in the cover is called an embedded message, and a steganographic method mixes the cover massage with this hidden message. Steganographic keys (stego keys) are optionally used secret information that may or may not be required for the algorithm to complete the concealed procedure. In most cases, you'll need the original key (or a similar one) to get to the hidden message again.

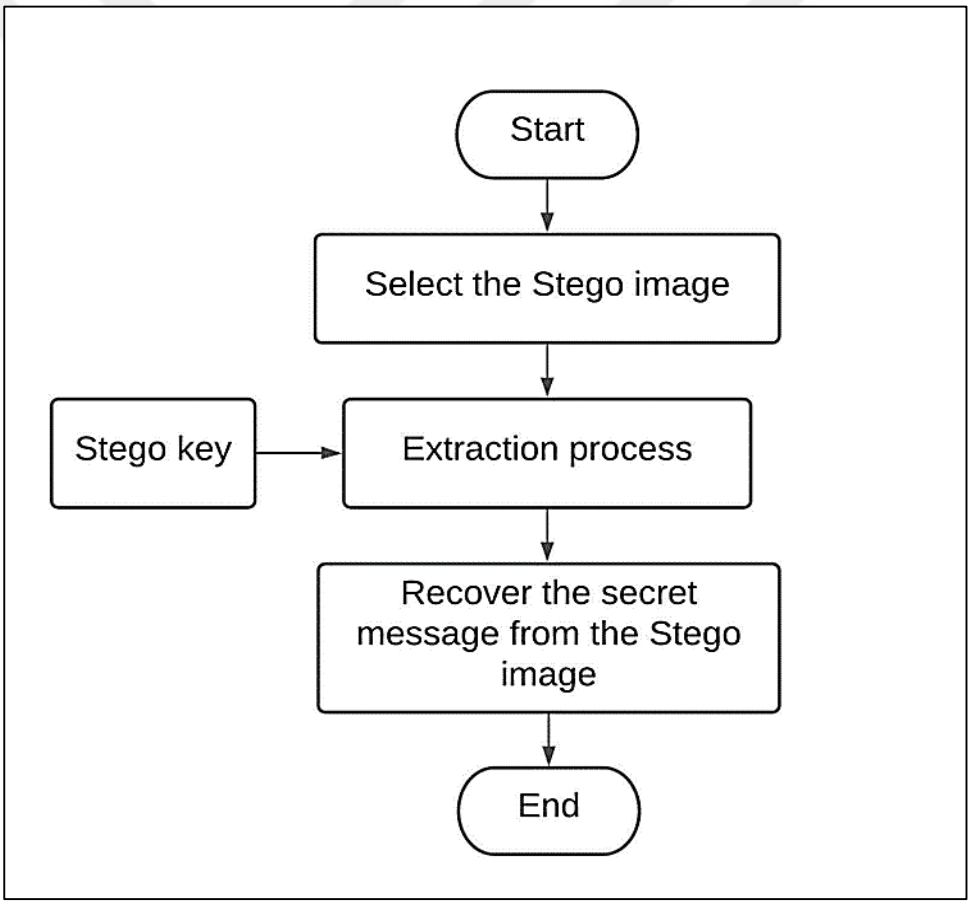

Figure 3.3: The Flow Chart of the Proposed Extraction Process Algorithm [46].

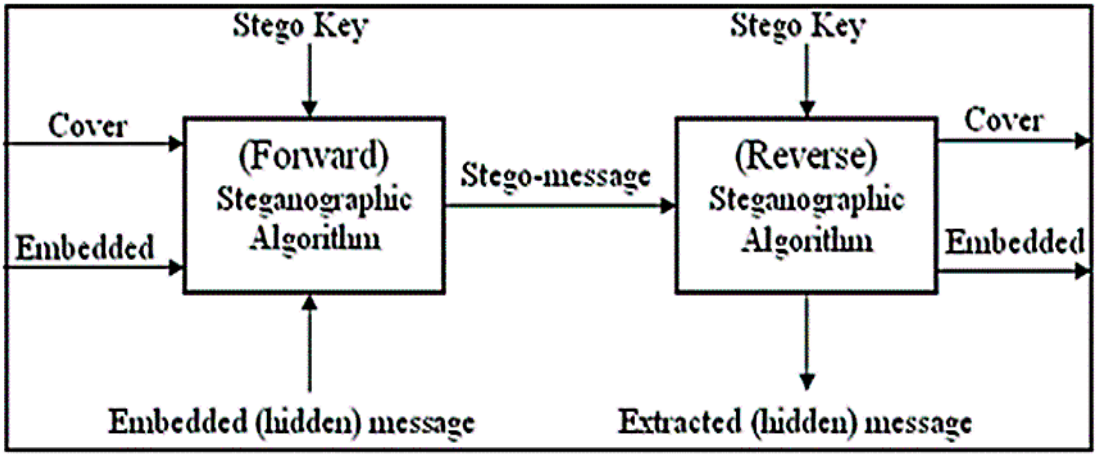

Figure 3.4: A General Steganography System [47].

3.4 LSB DECOMPOSITION

The Least Significant Bit approach [10] is one of the simplest ways to store data inside a digital cover secretly. The pixel values in an I×J picture are represented by decimal numbers in a range proportional to the number of bits utilized. Each pixel in an 8-bit grayscale picture takes on a value between zero and 255, and equation 1 may be used to represent any positive integer.

$$F_{10} = f_0 + f_1 B^1 + f_2 B^2 + \cdots = \sum_{i=1}^{n} f_i B^i \quad (3.1)$$

Where B is the constant, this feature enables the picture to be broken down into binary images by segmenting them into n bit planes.

Traditional LSB embedding strategies include substituting the least significant bits of the cover image with the secret message or modifying them using an 'inverse' function. Sequential insertion, selected text embedding in "noisy" places, or random dispersal over the picture are other viable options for the embedding approach. In more modern approaches, LSB is used in the LSB plane and in additional planes or a hybrid of the two. Based on the number of pixels picked based on brightness and contrast attributes, the quantity of data embedded might be constant or variable in size.

The primary benefit of this method is that the amplitude of the fluctuation in pixel values is limited to within a range of l; thus, the alteration of the LSB plane does not degrade the image in the eyes of the viewer. The human visual system has masking features that make large volumes of embedded information not visible to the naked eye under typical viewing

conditions. The term "masking" describes the situation in which one signal becomes undetectable to an observer due to the existence of another signal. Refer to [46, 47, and 48] for a comprehensive analysis of these methods. Low-density-block (LSB) data concealing also boasted a large embedding capacity and a low computing cost. The key drawbacks relate to the system's vulnerability to manipulation, geometric assaults, filtering, and compression.

3.5 FIBONACCI DECOMPOSITION

Leonardo of Pisa, often known as Fibonacci, introduced the Fibonacci sequence in his work Liber Abaci [2] in the 13th century. The famous rabbit issue that leads to the numbers 1, 1, 2, 3, 5,8, 13, 21, 34, 55,89, 144,233 was first presented by him. Following is the recurring connection that characterizes the Fibonacci sequence of numbers:

$$\begin{cases} 0 & n < 0 \\ 1 & n = 0 \\ B(n-1) + B(n-2) & n > 0 \end{cases} \tag{3.2}$$

The sequence numbers provide the foundation B_n of the Fibonacci representation.

$$B(n) = B(n-1) + B(n-2) \quad n \geq 2 \tag{3.3}$$

For certain values of n, the system of binary and Fibonacci numbers coincides. Shown in below Table.

Table 3.1: Both Representations Have Their Differences, Which May be Seen Clearly [2].

N	0	1	2	3	4	5	6	7	8	9	10
Bin	0	1	2	4	8	16	32	64	128	256	512
Fib	0	1	1	2	3	5	8	13	21	34	55

Maximum bit error after embedding for each plane in Table 2.

Both representations have their differences, which may be seen clearly in Table 1.

Table 3.2: Maximum Bit Error After Embedding for Each Plane [2].

Bit Plane	1	2	3	4	5	6	7	8
Bin	+1	+2	+4	+8	+16	+23	+64	+128
Fib	+1	+2	+3	+5	+8	+13	+21	+34

Both representations have their differences, which may be seen clearly in Table 1.

a. Generally, when N>2, the range of numbers that may be represented binary-wise using the same amount of bits increases. The Fibonacci representation uses a range of [0, 54], while the binary representation uses the total [0, 255].

b. Generally, when N>2, the range of numbers that may be represented binary-wise using the same amount of bits increases. The Fibonacci representation uses a range of [0, 54], while the binary representation uses the total [0, 255].

c. Generally, when N>2, the range of numbers that may be represented binary-wise using the same amount of bits increases. The Fibonacci representation uses a range of [0, 54], while the binary representation uses the total [0, 255].

Given that each natural number may be written as a sum of Fibonacci numbers, the Fibonacci representation serves no practical purpose. For instance, 16 can be written as 13+3, 8+5+3, or 8+5+2+1. However, one Fibonacci standard representation permits a certain kind of decomposition of natural numbers. An essential foundation for this is Zeckendorf's theorem [49], which claims that "any positive integer m may be written as the sum of different integers in the sequence of Fibonacci sequence using no 2 sequential Fibonacci numbers."

Zeckendorf's theorem states that every positive integer can be written as;

$$F_b = f_0 + f_1 B^1 + f_2 B^2 + \cdots = \sum_{i=1}^{n} f_i B^i \tag{3.4}$$

When there isn't a string of two consecutive 1's.

4. PROPOSED METHOD

The proposed steganography strategy's central idea is to conceal a message inside the original image, maintain the hosted image's quality so that it looks identical to the original, and transfer the two images from the sender to the authorized receiver side without raising suspicion among uninitiated viewers. Using steps like pixel selection and implicit essential creation, this research proposes a new steganography technique for concealing secret messages behind cover images. The intensity of the two pixels is used to determine which pixel the secret code will be embedded in; if the secret code value is one, the pixel will have a low intensity, and if it is zero, the pixel will have a high intensity. The Fibonacci-based decomposition method was utilized to make embedding the private data more secure and efficient. In this study, the pixel count was converted from its original decimal form to its Fibonacci decomposition before further processing. The Fibonacci decomposition was used to conceal information within the cover art, suggesting that the numbers formed an integral design component. Due to the binary encoding, the bit plane of an image was the 8-bitplanes. As a result, the Fibonacci decomposition was logically converted to the 12-bitplanes through implementation. Algorithm 4.3 shows the steps for achieving the Fibonacci number sequence. The procedures necessary to obtain the Fibonacci sequence are laid forth in Algorithm 4.1.

Algorithm 1: Fibonacci number

The Fibonacci decomposition was used mainly for three important reasons in this study. I) Due to the attacker's difficulty predicting confidential data, the switch to the Fibonacci decomposition improved security. II) Since 12-bit-planes were used, the system became more secure. III) Inconsistent information made visual identification challenging.

4.1 THE PROPOSED EMBEDDING METHOD

The suggested steganography system is based on the principle that a secret message can be effectively concealed within a specific image (the original image) while maintaining the same high quality of the hosted image during transmission from the sender to the authorized receiver side. The suggested robust image steganography system's primary objective is to ensure that the intruder is entirely oblivious to the presence of some text within the image. Three fundamental processes, including random block and pixel selection, adjusting the contrast

level, and generating an implicit key, were proposed in this work to obtain a secure stego-picture, which would conceal the secret message within the cover image.

4.2 RANDOM BLOCKS AND PIXELS SELECTION

The main benefit of creating an ISS is providing a safe place for steganographic images to transport sensitive data across the web. Figure 4.1 shows the proposed method's bit stream fragmentation. We broke the image into 8x8 squares, each consisting of 64x64 pixels. Figure 4.2 depicts selecting the block and selecting the pixels inside that block to be embedded.

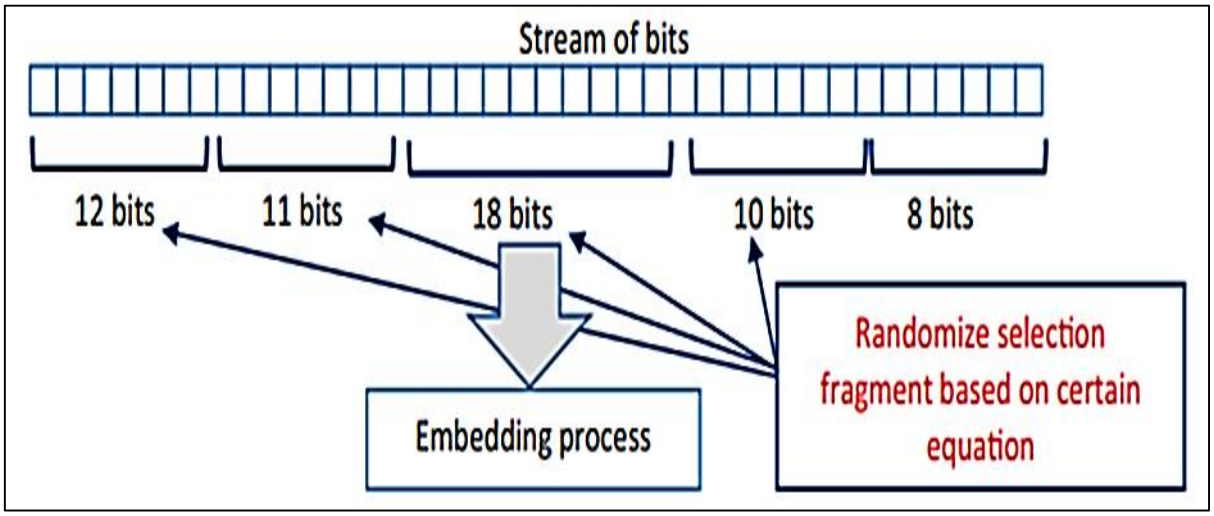

Figure 4.1: Fragmentation of A Bit Stream by the Suggested Technique.

The random procedure chooses the first pixel to embed by using a random function three times. This technique divides the cover image into sub-blocks. The random process in a steganography system typically involves a round random function, but other algorithms like the Knight Tour or the Henon map are also possible. There are two parameters in the Henon random function that were utilized to address the scheme's high security concerns. This random function is beneficial in term of increasing the complexity of the aimed blocks or pixels selection processes up to 10^30round steps (theoretically).

In reality, a random function is utilized to achieve such a high level of security. To protect the text contained within the image, the Henon map function was run 10^30 times, yielding approximately 2^100 random processes. The standard random function picks a number using a single parameter; given 10^15random processes as the beginning condition for this function

(single), the probability of finding these numbers is2^20. In order to make the estimation of numbers more difficult, we employ a constant value of two control parameters.

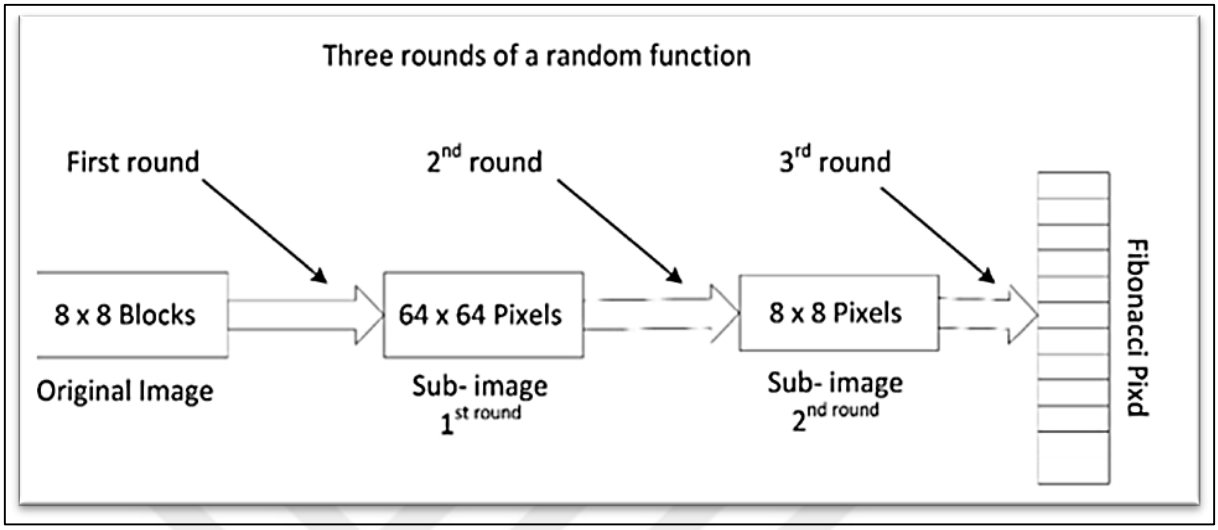

Figure 4.2: Fragmentation of a Bit Stream by the Suggested Technique.

Think of X' as the total number of cover picture blocks. After some initial random rounding, the image can be divided into blocks of size S = 64 in order to generate an x-dimensional vector. Therefore, every Z is an integer, since Z = X'/S is in the domain.

$$d_i = i + (S * Z) \tag{4.1}$$

$$V = [d_1, d_2, d_3, d_4, \ldots\ldots, d_Z] \tag{4.2}$$

Where d_i denotes block I and the vector (V) stands for the location where labelled blocks can be kept. The random blocks had to be remembered so that the stego key could be used to decrypt the secret message embedded inside them.

5. RESULTS DISCUSSIOV

Various evaluation metrics establish that the applied processing via the proposed approach impacted image quality and led to some information loss. Both objective and subjective methods can be used to assess the stego image. Finding the differences between two data sets required the objective approaches to apply mathematical criteria and use many criteria, including ground truth and prior knowledge of the statistical issue at hand. Contrarily, subjective approaches relied solely on human observation and subjective judgment, with no referring criteria provided. The embedding capacity (EC), peak signal-to-noise ratio (PSNR), mean square error (MSE), and bit per pixels (BPP) were taken into account as objective approaches for evaluating the proposed scheme in this research. In the suggested technique, the EC value is proportional to the ratio of message bits to the number of cover pixels. One pixel could contain an arbitrary number of message bits, and the EC is written as:

$$EC = \frac{\text{Number of text bit}}{\text{Number of image pixel}} \tag{5.1}$$

The simulation runs on the following set of parameters:

a. When 1 bit of two pixels was incorporated, the total size of the image was 16,384 bytes, or 6.25 percent. The image had a resolution of (512 by 512) pixels.

b. When 1 bit of 1 pixel is embedded, the total number of bytes required to store the image is 32,768 (12.5 percent), assuming that each pixel in the image has a value of 8 bits (1/8 = 12.5%).

c. Since each two pixels were allocated to 16 bits, 3/16 = 18.75% while 1.5 bit with one pixel was inserted, the number of bytes required to store a 512 by 512 pixel image was 49,152, or 18.75%.

To maintain parity with previously published works in this area, the current study utilized a range of payload capacities and presented them as percentages. Figure 5.1 displays examples of stego pictures employed in the suggested method. As mentioned earlier, the image produced after embedding is called a Stego- image. To evaluate the quality of a stego image, we use a peak signal-to-noise ratio (PSNR) scale and mean square error (MSE) scale. The PSNR block calculates the peak signal-to-noise ratio, in decibels, between two images. This ratio is used as

a quality measure between the original image and the compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image.

After the embedding procedure, the image quality is assessed by calculating the PSNR and comparing the original and stego versions of the image. When the PSNR is less than 30 decibels, data embedding is deemed to be unnoticeable to the HVS. This expression is used to derive the PSNR value:

$$PSNR = 10\log_{10}\left(\frac{\mathrm{MAX_I}^2}{MSE}\right) \tag{5.2}$$

Figure 5.1: Various Stego Images Using Proposed Approach.

While, the MSE scale indicates the difference of pixel by pixel between the Stego image and the cover image, which is calculated as in the following equation:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \tag{5.3}$$

Where, m is no. of row in original image and n is no. of column in original image.

The PSNR is calculated from the MSE that had a negative impact. PSNR parameters allowed the equation to be standardized across all approaches and image formats.

The testing and training phases are important to the success of the suggested method. . To test whether or not a stego image is undetectable in traditional image processing, one would use the

The PSNR scale. The PSNR metrics are used to compare the stego image to its original carrier image and determine how authentic the stego image is. We may compare the stego picture's distortion to that of the carrier image in terms of decibels (dB). Since a lower PSNR score indicates a lower likelihood of detecting an attack using the HVS, a higher PSNR value indicates a higher-quality image. During the training phase, the PSNR decreased as the MSE grew, suggesting that the mismatch between the actual picture and the stego message had grown more severe. Due to the inverse relationship between MSE and PSNR, the results are unsatisfactory when MSE is high. The issue is resolved in the testing phase, and the resulting results are superior to those obtained by other methods. In this work, we used three distinct embedding techniques to assess the efficacy of the developed method with varying EP: a straightforward LSB embedding, an embedding using the Fibonacci decomposition method, and an embedding with the grayscale standard SIPI images (Lena, Baboon, and Tiffany (512512)). The experimental results show the final variation in images, as shown in Figure 5.2.

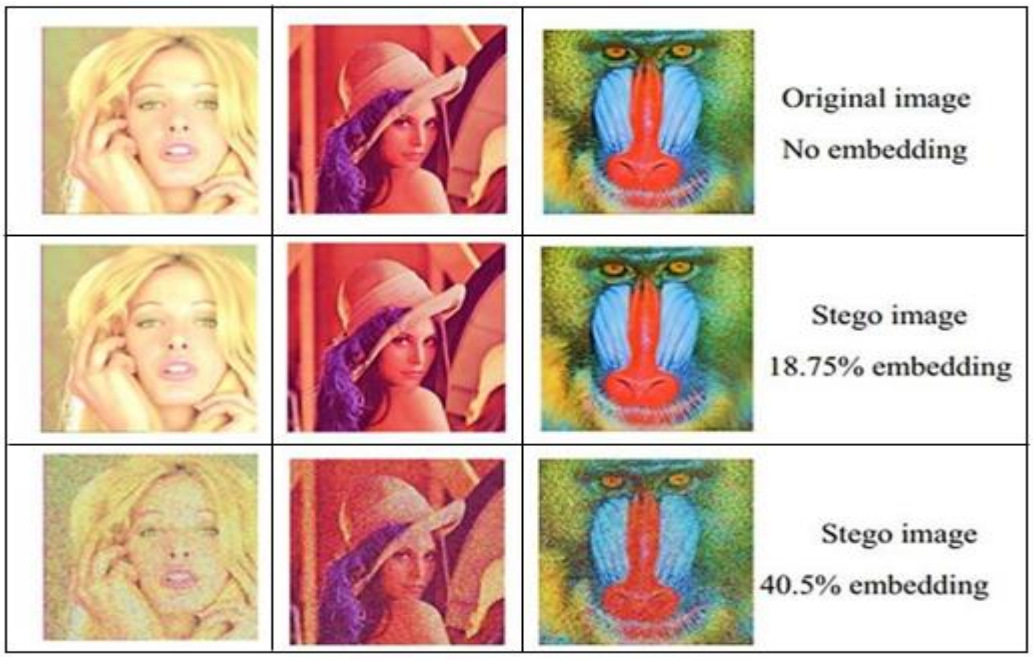

Figure 5.2: Variations of Original and Stego Images.

Different stego pictures with varying amounts of EP are used to evaluate the effectiveness and quality of the proposed method. Compare the stego images in Figure 5.3 to the original image in different Payload capacities to see the similarities. As seen in the second row of the figure, the original image looked like a stego image with a reasonable degree of embedding. However, as the final row of the graphic shows, the image is destroyed when the embedding limit is surpassed, making it recognizable by a hacker.

6. CONCLUSION AND FUTURE WORK

In this research, we offer a strong image steganographic technique for the safe transfer of confidential information over the web. Today's security applications require more than just a steganographic technique that doesn't compromise on aesthetics or payload. Using the proposed steganography technique, this research included the experimental outcomes, analyses, discussion, and comparisons. There are three key criteria offered to assess the result and whether or not it addressed the most crucial problems with the steganography scheme. The use of a novel decomposition approach unfamiliar to the hacker helps improve capacity and robustness. Using encryption and random selection during the embedding process, the new method improves the system's security, which is based on the distinction grade value and integrity system. The results are presented in tabular and graphical formats for each criterion to facilitate easy interpretation and comprehension.

Many promising future avenues were uncovered by this effort. For instance, combining the frequency domain and the special domain can improve security. The resulting security and robustness may be improved. The results suggest that combining the suggested approach with the DWT and embedding may produce high coefficients. Since large embedding coefficients have been employed by several methods previously, this is not a new consideration. Yet, DGV adoption has the potential to improve outcomes including security and stealth.

REFERENCES

[1] Wu, Min, and Bede Liu. Multimedia data hiding. Springer Science & Business Media, 2003.

[2] Stefan, Katzenbeisser, and Petitcolas Fabien AP. "Information hiding techniques for steganography and digital watermarking." (2000).

[3] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." Computer science review 13 (2014): 95-113.

[4] Jenifer, K. Steffy, G. Yogaraj, and K. Rajalakshmi. "LSB approach for video steganography to embed images." International Journal of Computer Science and Information Technologies 5.1 (2014): 319-322.

[5] Liu, Jing, Guangming Tang, and Yifeng Sun. "A secure steganography for privacy protection in healthcare system." Journal of medical systems 37.2 (2013): 1-10.

[6] Zielińska, Elżbieta, Wojciech Mazurczyk, and Krzysztof Szczypiorski. "Trends in steganography." Communications of the ACM 57.3 (2014): 86-95.

[7] Pudney, Peter, and Phil Howlett. "Critical speed control of a solar car." Optimization and engineering 3.2 (2002): 97-107.

[8] Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." Proceedings of the IEEE 87.7 (1999): 1062-1078.

[9] Wang, Huaiqing, and Shuozhong Wang. "Cyber warfare: steganography vs. steganalysis." Communications of the ACM 47.10 (2004): 76-82.

[10] Rustad, Supriadi, Abdul Syukur, and Pulung Nurtantio Andono. "Inverted LSB image steganography using adaptive pattern to improve imperceptibility." Journal of King Saud University-Computer and Information Sciences 34.6 (2022): 3559-3568.

[11] Ogundokun, Roseline Oluwaseun, and Oluwakemi Christiana Abikoye. "A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography." International Journal of Digital Multimedia Broadcasting 2021 (2021).

[12] Xu, Xinhao. "Image Data Hiding Based on Logical Operation of LSB." 2021 5th International Conference on Artificial Intelligence and Virtual Reality (AIVR). 2021.

[13] Singh, Siddharth, Rajiv Singh, and Tanveer J. Siddiqui. "Singular value decomposition based image steganography using integer wavelet transform." Advances in signal processing and intelligent recognition systems. Springer, Cham, 2016. 593-601.

[14] Rocha, Anderson, and Siome Goldenstein. "Steganography and steganalysis in digital multimedia: Hype or hallelujah?." Revista de Informática Teórica e Aplicada 15.1 (2008): 83-110.

[15] Wu, Hao-tian, Jean-Luc Dugelay, and Yiu-ming Cheung. "A data mapping method for steganography and its application to images." International Workshop on Information hiding. Springer, Berlin, Heidelberg, 2008.

[16] Ghazanfari, Kazem, Shahrokh Ghaemmaghami, and Saeed R. Khosravi. "LSB++: an improvement to LSB+ steganography." TENCON 2011-2011 IEEE Region 10 Conference. IEEE, 2011.

[17] Ker, Andrew D. "Steganalysis of LSB matching in grayscale images." IEEE signal processing letters 12.6 (2005): 441-444.

[18] Mielikainen, Jarno. "LSB matching revisited." IEEE signal processing letters 13.5 (2006): 285-287.

[19] Giarimpampa, Despoina. "Blind Image Steganalytic Optimization by using Machine Learning." (2018).

[20] Hetzl, Stefan, and Petra Mutzel. "A graph–theoretic approach to steganography." IFIP international conference on communications and multimedia security. Springer, Berlin, Heidelberg, 2005.

[21] Sedighi, Vahid, Jessica Fridrich, and Rémi Cogranne. "Toss that bossbase, alice!." Electronic Imaging 2016.8 (2016): 1-9.

[22] Denemark, Tomáš, Jessica Fridrich, and Vojtěch Holub. "Further study on the security of S-UNIWARD." Media Watermarking, Security, and Forensics 2014. Vol. 9028. SPIE, 2014.

[23] Giarimpampa, Despoina. "Blind Image Steganalytic Optimization by using Machine Learning." (2018).

[24] Li, Bin, et al. "A survey on image steganography and steganalysis." J. Inf. Hiding Multim. Signal Process. 2.2 (2011): 142-172.

[25] Westfeld, Andreas. "F5—a steganographic algorithm." International workshop on information hiding. Springer, Berlin, Heidelberg, 2001.

[26] Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.

[27] Miri, Aref, and Karim Faez. "Adaptive image steganography based on transform domain via genetic algorithm." Optik 145 (2017): 158-168.

[28] Pradhan, A., Sekhar, K. R., & Swain, G. (2017). Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks. Security and Communication Networks, 2017. https://doi.org/10.1155/2017/1924618.

[29] Fouad, Mohamed M. "Enhancing the imperceptibility of image steganography for information hiding." 2017 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2017.

[30] Shukla, Awdhesh K., et al. "A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing." IEEE Access 6 (2018): 51130-51139.

[31] Ker, Andrew D., et al. "Moving steganography and steganalysis from the laboratory into the real world." Proceedings of the first ACM workshop on Information hiding and multimedia security. 2013.

[32] Lyu, Siwei, and Hany Farid. "Steganalysis using color wavelet statistics and one-class support vector machines." Security, steganography, and watermarking of multimedia contents VI. Vol. 5306. SPIE, 2004.

[33] Cogranne, Rémi, et al. "Is ensemble classifier needed for steganalysis in high-dimensional feature spaces?." 2015 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2015.

[34] Menori, Marcelinus Henry, and Rinaldi Munir. "Blind steganalysis for digital images using support vector machine method." 2016 International Symposium on Electronics and Smart Devices (ISESD). IEEE, 2016.

[35] Boroumand, Mehdi, and Jessica Fridrich. "Applications of explicit non-linear feature maps in steganalysis." IEEE Transactions on Information Forensics and Security 13.4 (2017): 823-833.

[36] Qian, Yinlong, et al. "Deep learning for steganalysis via convolutional neural networks." Media Watermarking, Security, and Forensics 2015. Vol. 9409. SPIE, 2015.

[37] Pibre, Lionel, et al. "Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover sourcemismatch." Electronic Imaging 2016.8 (2016): 1-11.

[38] Xu, Guanshuo, Han-Zhou Wu, and Yun-Qing Shi. "Structural design of convolutional neural networks for steganalysis." IEEE Signal Processing Letters 23.5 (2016): 708-712.

[39] Xu, Guanshuo, Han-Zhou Wu, and Yun Q. Shi. "Ensemble of CNNs for steganalysis: An empirical study." Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. 2016.

[40] Zeng, Jishen, et al. "Large-scale JPEG image steganalysis using hybrid deep-learning framework." IEEE Transactions on Information Forensics and Security 13.5 (2017): 1200-1214.

[41] Hu, Donghui, et al. "Adaptive steganalysis based on selection region and combined convolutional neural networks." Security and Communication Networks 2017 (2017).

[42] Liu, Kai, et al. "Multi-channel neural network for steganalysis." 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC). IEEE, 2017.

[43] Zhang, Yuan-Hang, Xie Li, and Jing-Yun Xiao. "A digital fuzzy edge detector for color images." arXiv preprint arXiv:1701.03364 (2017).

[44] Goodarzi, Mahdi Hassani, Arash Zaeim, and Amir Shahab Shahabi. "Convergence between fuzzy logic and steganography for high payload data embedding and more security." 2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA). IEEE, 2011.

[45] Liu, Qingzhong, and Andrew H. Sung. "Detect information-hiding type and length in JPEG images by using neuro-fuzzy inference systems." 2008 Congress on Image and Signal Processing. Vol. 5. IEEE, 2008.

[46] Lin, Eugene T., and Edward J. Delp. "A review of data hiding in digital images." PICS. Vol. 299. 1999.

[47] Yeung, Minerva M., and Fred Mintzer. "An invisible watermarking technique for image verification." Proceedings of international conference on image processing. Vol. 2. IEEE, 1997.

[48] Maity, Santi P., and Malay Kumar Kundu. "Robust and Blind Spatial Watermarking In Digital Image." ICVGIP. 2002.

[49] Hoggatt, Verner E. Fibonacci and Lucas numbers. Houghton Mifflin, 1969.