Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

# A secure image steganography technique based on Data Mapping and Genetic Algorithm

**Anas I. Al-jumaili**

Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, Egypt

anas.aljumaili@alexu.edu.eg

**Maysa Kh. Noby**

Faculty of information technology and computer science, Sinai University, Egypt

maysa.khalil@su.edu.eg

**Shawkat K. Guirguis**

Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, Egypt

shawkat_g@yahoo.com

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

## Abstract

The Internet revolution facilitated digital communication; nevertheless, it raised problems and challenges for securing data across an open network. Steganography is one of the most effective techniques that deal with this issue and ensure information security. Many previous studies focused solely on the capacity factor without considering how safe this method is, which is regarded as one of the steganography's points of weakness. In this paper, secure image steganography in the spatial domain is proposed, where a combination of data mapping and genetic algorithm GA technique are used to make image steganography more imperceptible and very secure. The first step is selecting a specific part of the image (start position key) to hide the secret message by using data mapping. It matches every 2 bits of a secret message with 2 bits of a pixel and generates a mapping position according to the location of the match. In the second step, a GA-based technique is designed to use these mapping positions, find the best possible location to embed them again in other parts of the image, and generate an index key. After a compression process of the start position key, the coefficient rule key, and the index key, the stego key is created. Furthermore, extracting the secret message would be impossible without getting all three parts of the stego key together. The implementation results indicate that the proposed model is secure, has higher imperceptibility, and it is almost impossible to find the hidden data without obtaining the parts of Stego key together.

**Keywords:** *Image Steganography, Spatial Domain, Genetic Algorithm GA, Data mapping, Least Significant bits LSB, Stego Key.*

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

## 1. Introduction

The internet revolution, combined with the digitization of information, has exponentially increased the use of data transmission over the internet. The malicious acts of attackers and hackers have become too familiar during the data transfer over the internet, a publicly accessible network. As a result, a security mechanism is required to safeguard the sent data from any unwanted access (Kalaichelvi et al., 2021). Since the inception of the internet, several techniques for information and system security have been continuously developed in response to this problem. Information security is classified into two broad categories: encryption and information hiding. While encryption and information hiding have the same ultimate purpose, their methodologies are quite different (Taha et al., 2019).

Encryption converts the information into a scrambled and unreadable format; however, it draws attention that there is a secret message. The better option is to use an invisible method for data transmission without giving a chance for the intruders to notice the existence of any secret communication channels. In contrast, information hiding does not alter the format of data or messages and preserves their original content (Khan et al., 2020).

Information hiding is divided into two subfields: steganography and watermarking. Both techniques are for concealing a secret message, and while they are related, they serve distinct purposes. Watermarking is typically used to safeguard the integrity of embedded secret data by hiding the communication's existence or without hiding it. It is primarily used to determine ownership, ensure the validity or integrity of data, and guard against copyright infringement (Panah et al., 2016; Shih, 2017). The purpose of steganography is to conceal secret data in an undetected manner within a cover media. Secret data types include image files, video files, binary bits, and text data. Additionally, it is acceptable to use any commonly used digital format for the cover media, including but not limited to images, videos, and texts (Alsaidi et al., 2018).

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

The term "secret data" refers to data concealed within a cover/host media, whereas "Stegomedia" refers to the cover media after it has been embedded with the secret data. The stego-media is aimed to be sent above an open and unprotected channel. The ideal medium for embedding secret messages must have two characteristics: it must be widely available and capable of concealing the secret data therein with unnoticeable effects. As a result, image files are the most commonly embedded media type (Hussain et al., 2018). In image steganography, the image used to conceal the secret message is referred to as a "cover image", while the final output image concealing the secret message is referred to as a "stego-image".

Methods of image steganography can be categorized into two broad types based on their embedding domain: spatial domain and frequency domain (Qin et al., 2019). In the spatial domain, the secret message is embedded straight in the cover image pixels. For example, this can be done by substituting secret bits such as least significant bits (LSB) for the pixel value and by pixel value differencing (PVD). On the other hand, in the transform domain, the embedding procedure is applied after the cover image is changed into another form. discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT) are the most of transform domain methods (Dalal & Juneja 2021). Spatial domain offers many benefits including, ease of use, visual quality, and high embedding capacity. This makes its techniques preferred over the transform domain techniques despite the fact that the spatial domain offers less security (Bairagi et al., 2016).

The least significant bits' substitution (LSB) is one of the most extensively utilised spatial domain hiding strategies (Bhuiyan et al., 2019). The Least Significant Bit (LSB) can be classified as sequential and random. The concept behind this technology is that the least significant bits in an image reflect only rudimentary information. Therefore, slight

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

modifications that apply to it are undetectable by the naked eye. LSB technique is used to insert the secret message straight into the cover image without affecting the visual quality of the cover image. LSB has a low computing complexity and a great capacity for embedding (Wang et al., 2020). Despite that, LSB technique includes some disadvantages, including considerable degradation of the stego images once large amounts of hidden data are embedded. Also, it is the simplest approach for detection (Walia et al., 2018). This method can be improved by combining an optimization technique.

The performance of the steganography technique is primarily determined by three major indicators: quality (imperceptibility), security, and concealing capability (Mandal et al., 2022). Imperceptibility is the primary prerequisite for any steganography, it determines the strength of any stenographic approach, it is used to effectively hide a secret message inside the cover image. In other words, it cannot be noticed by the human eye or by statistical methods. The Peak signal to noise ratio (PSNR) and mean square error (MSE) are often used as measures of imperceptibility (Kadhim et al., 2019). Any steganography approach is considered secure and protected if the stego image is resistant to steganography attacks and cannot be detected or removed after the attacker discovers it (Alatawi & Narmatha, 2020). The capacity factor is defined as the number of embedded secret bits per pixel (bpp) (Evsutin et al., 2020).

Genetic Algorithms (GAs) are a class of heuristic optimization algorithms inspired by the theory of evolution, "survival of the fittest". It is dependent on the idea of generational propagation. The selection is made according to a fitness function, then substituting offspring that look weaker. Thus, GAs are algorithms that are basically population-based (Pandey, 2016). That means, rather than starting with one random answer, a genetic algorithm starts with a population of

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

solutions that serve as the system's foundation, then, every two individuals in this population get married. This marriage is done by crossover and mutation, and the resulted new individual is referred to as the offspring reflecting features of both parents. These offspring will become parents. After many generations of continuing this cycle, a genetic algorithm gets the global solution to the optimization problem by producing an ideal new offspring that improves the fitness function (Bäck et al., 2018).

Genetic algorithms are particularly advantageous for scanning an ample search space where an exhaustive search is impractical (Resende & Drummond, 2018). In steganography, GA can be exploited to search for the optimal position for embedding the indexes that are output from data mapping with the least distortion. This paper contributes to the field by proposing a steganography system that is very secure with high imperceptibility. By merging the two techniques, data mapping and GAs. the objective of using the combination of techniques is to hide a secret message in the cover image with minimum possible change and generate a very strong stego key.

The remainder of the paper is organized in the following manner. The second section, discusses some of the most recent studies in this field. Section 3, contains a detailed discussion of the proposed algorithm. In section 4, the results and discussions of the dataset are given. Finally, Section 5 draws conclusions.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

## 2. Literature Survey

In the spatial domain, there are numerous approaches for implementing image steganography techniques. The Least Significant Bit is the preferred technique for spatial domain image steganography due to its simplicity of usage. Simultaneously, it is the simplest approach of detection. In this approach, the quality of stego image gradually decreases with increasing capacity. Random embedding is used to overcome the shortcomings of sequential methods. This strategy is difficult to detect due to the character's random positioning, but it significantly increases the amount of distortion. Therefore, the optimizing the embedding complexity and enhancing security are necessary (Ibanez et al., 2018).

(Shehzad & Dag, 2017), employed the data mapping technique by dividing the secret message into bytes and divide the pixel byte into pairs of bits. The binary message bytes are grouped into pairs, and each pixel byte is divided into four pairs: the first pair includes 2nd and 3rd bits, the second pair includes 3rd and 4th bits, the third pair includes 4th and 5th bits, and the fourth pair includes 5th and 6th bits. The 7th and 8th bits are not clustered. To determine the matching pair, every message pair is compared to all pixel pairs. Once the matching pair is identified, the number of pixel pairs is saved in the LSB of that pixel. When no matching is detected, the third pair is replaced with message bits, and the LSB values contain the pair's number. However, this strategy is not secure, as the secret message can be acquired indirectly through the initial bit pairs. Furthermore, the result obtained is somewhat small at 35.19 DB with 2bpp.

In (Shah & Bichkar, 2018) a data mapping-based steganography technique is described. A quarter of an image is identified to hide 2 bits per pixel. The coefficient that results from the data mapping is embedded into the rest of the image using a linear congruential generator (LCG). Simultaneously, a genetic algorithm is utilized to modify the LCG

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

parameters. However, this technique is not sufficiently secure and hackable because LCG is not truly random and can be repetitive. Given enough cipher text, it can be broken.

(Wazirali et al., 2019) proposed a strategy for high-capacity/payload steganography that tries to boost imperceptibility by using several operations such as optimized pixel scanning order, flipping secret bits, circular shifting, and transposing secret data. This system made use of GA in order to identify the most optimal solutions. However, the technique in this study is somewhat highly complex due to the GA operations required to find the answer in a near-optimal manner.

(Swain, 2016) presented hybrid embedding systems to incorporate the advantages of many embedding schemes. Where used both techniques, PVD and LSB substitutions. Initially, it put the k-bit secret data into the block's upper-left pixel. The PVD embedding procedure was followed to the upper left base pixel and the remaining pixels along their horizontal and vertical edges. To improve only PSNR, or PSNR with high payload, two embedding strategies, Type 1 and Type 2, were proposed. While the proposed approach achieved a large embedding capacity, it lacked security and was susceptible to attacks via histogram analysis methods.

(Nosrati et al., 2015) proposed genetic algorithm-based technique is conducted for hiding secret message in a cover image, by "before embedding hiding strategies". This method ideally determines the right areas in the cover image to embed the secret information. It makes the fewest possible changes to the bits, which results in the histogram of the image being modified minimally. Segmentation is used in this genetic method to convert LSBs and secret messages to a set of blocks. After determining the optimal embedding locations, this algorithm embeds the secret blocks and generates the key file needed during the message extraction procedure. However, this study did not calculate the

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

degree of distortion introduced by this method, and the experimental outcome was limited to the histogram. As a result, the performance of this method cannot be measured.

(Shah & Bichkar, 2021) proposed a genetic algorithm-based payload data modification-based image steganography technique. A genetic algorithm controls the requirements for altering and modifying the payload data. The concept of a flexible chromosome is applied, in which the genetic algorithm interprets the chromosome value in a variety of ways and attempts to determine the optimal parameter that produces high-quality stego images. Due to the modification of the payload image at this point, the extraction process at the receiver may become cumbersome. For two bits per pixel, this approach has an average PSNR of 46.41 dB. This value is lower than the other comparable payload capacities approaches.

(Soleimanpour & Talebi, 2013) modified the score matrix technique and used GAs to optimize it. The major aim of employing these schemes is to discover a near-optimal pairwise LSB scheme based on GA. When a pixel from the carrier picture is identical to a pixel from the secret image, the score is T1, and when the pixels are different, the score is T2. T1 must be bigger than T2 in this case.

## 3. The Proposed System

This paper presents a new approach for enhancing the security of image steganography by combining two techniques, data mapping and GAs. Data mapping is an effective technique to embed the secret message in the cover image with minimum distortion. While GA is an optimization algorithm which has a clear advantage when searching and matching in a vast area is needed and a comprehensive search is impossible. The compression process is applied to reduce the large key size that results from the index key size. The proposed approach is shown in Figure 1.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

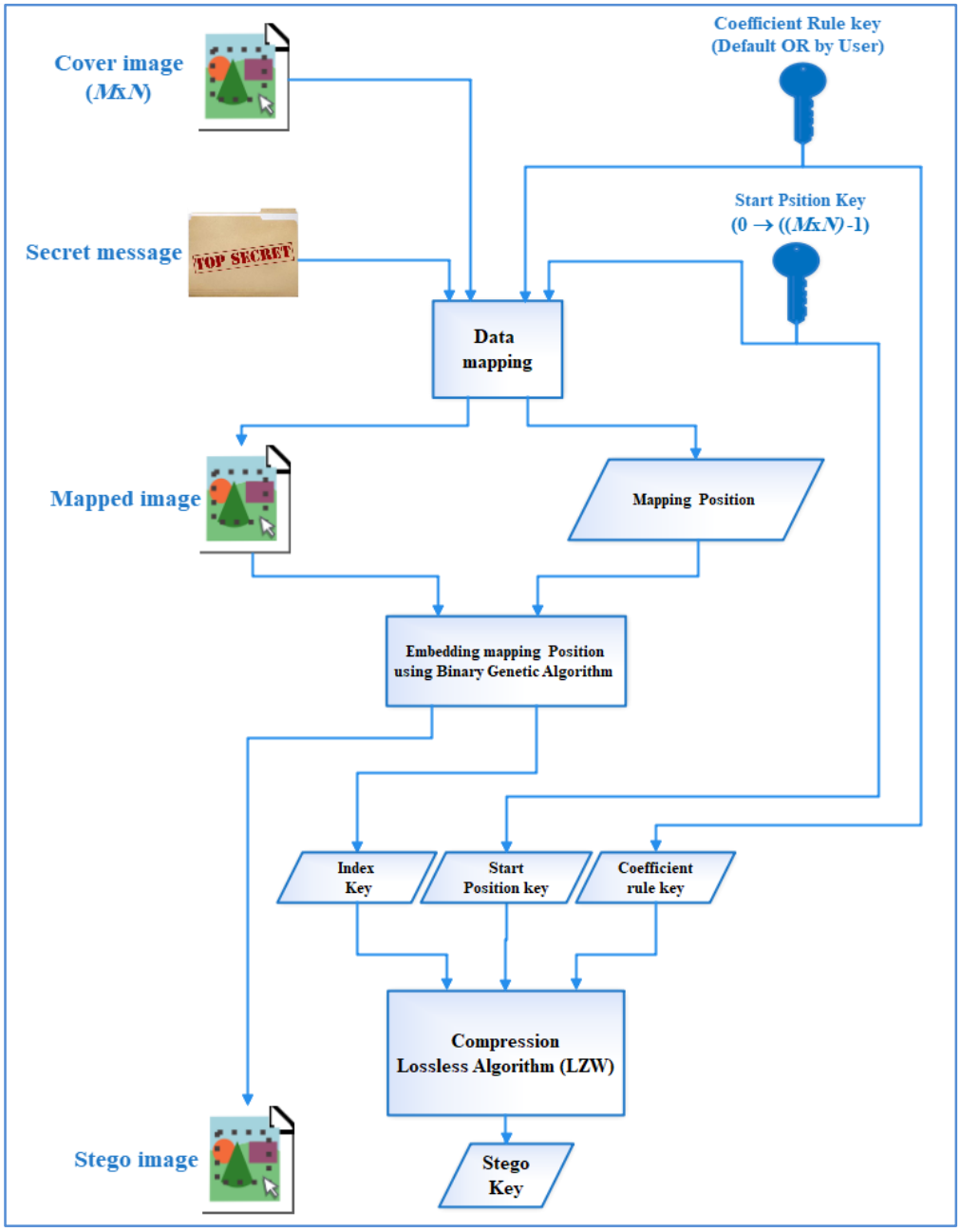


Figure (1): The proposed system

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

The proposed approach consists of four stages as described below:

### 3.1 Data mapping stage

It is the process of embedding the secret message in the image by matching each pair of secret message bits with a pixel of the cover image. The location of matching is called the (coefficient rule key). The value of the coefficients is shown in Table 1. The pixel where the data mapping process starts matching is called (start position key). If the cover image is *M*x*N*, then start position key equal (0→( *M*x*N* -1)), the user selects the start position value.

Table (1): Coefficient Rule Key (Default Key)

| Matching Position | Coefficient (Default Rule) |
|---|---|
| 010100** | 000 |
| 01010**1 | 001 |
| 0101**11 | 010 |
| 010**011 | 011 |
| 01**0011 | 100 |
| 0**10011 | 101 |
| **010011 | 110 |
| *101001* | 111 |

The first step in the data mapping stage is based on dividing the secret message into pairs of bits, then starting to embed every pair of bits from the secret message in a pixel of the cover image starting from (start position) start pixel. Based on the location of matching, corresponding coefficients are generated. Figure 2 shows the data mapping process; in the

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

case of embedding the secret message byte (11011110) in 4 image pixels (10010110, 11010000, 10010101, 00011011).

If there is no matching between the pair of bits of secret message and the pixel of the cover image, then this pair is embedded in two least significant bits of the pixel. Least significant bits represent feeble information and modify its lead to minimum distortion. Generally, it is possible to embed two bits of the secret message into each pixel without changing its value, resulting in less distortion in the stego image. Statistically, the data mapping technique succeeds by 88.76% in embedding the secret message without any pixel value change.

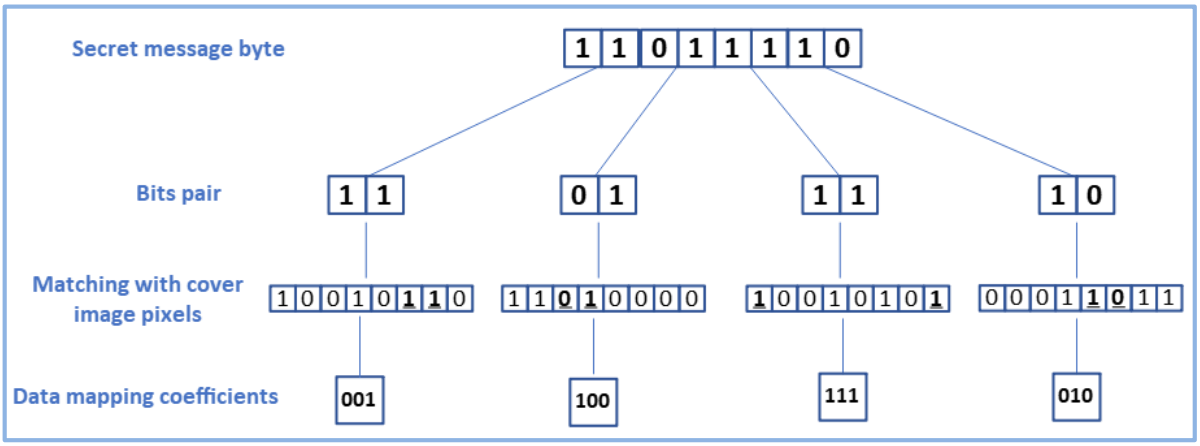


Figure (2): Data mapping process

3.2 Genetic algorithm stage

This stage aims to embedding the coefficients resulting from the data mapping stage into the rest of the cover image by genetic algorithm. As the coefficients have a value in the range 000–111, each coefficient requires three bits to be embedded. Finding the ideal match between the coefficient bits and the least significant bit of the rest pixels in the cover image is regarded as a search

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

and optimization problem.

The most important component in GA is the fitness function. In our proposed system, it is used to assign each individual a fitness based on how well it solves to find optimal matching between the coefficient and LSBs of pixels. PSNR is used as fitness function to measure the matching.

After certain generations, GA will get optimal matching. Then the bits of the coefficient are embedded in LSBs of the carrier image pixels and store the final chromosome, which represents the location of coefficients embedding in the stego image. Lastly, the final chromosome with the start position and coefficient rule forms the stego key.

### 3.3 Compression stage

The stego key consists of (Start position key, Coefficient rule key, and Index key) which is compressed before sending it to the receiver. The compression process is applied to reduce the large key size that came as a result of the index key size. Data compression is considered lossless if it is possible to exactly reconstruct the original data from the compressed version without any loss. When the original data of a source is so vital and cannot be afforded to lose any information, a lossless approach will be mandatory. In the proposed system using lossless compression is logical, where all bits in the stego key are important and have a specific role, it is irreplaceable.

In this work, Lempel-Ziv-Welch (LZW) is used where; it is one of the most popular and prevalent lossless compression algorithms, mainly due to its simplicity, high compression ratio, and time/space efficiency (Aldwairi et al., 2019). Using the LZW compression algorithm to compress the stego key is a convenient choice because the LZW algorithm achieves an excellent

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

compression ratio when compressing long text files containing repetitive strings (Ignatoski et al., 2020).

3.4 Extraction Process

This process is easier than the embedding procedure. It is the inverse of the embedding process as shown in Figure 3. The stego image, in addition to the stego key, are required as inputs to retrieve the secret message. Firstly, the stego key is decompressed and split into a coefficient position key, a coefficient rule key, and a start position key. Where the first 24 bits are the coefficient rule, the next 20 bits are the start position, and all the rest bits are the index key. The mapping positions are retrieved using the index key, and the secret message bits are retrieved using the start position.

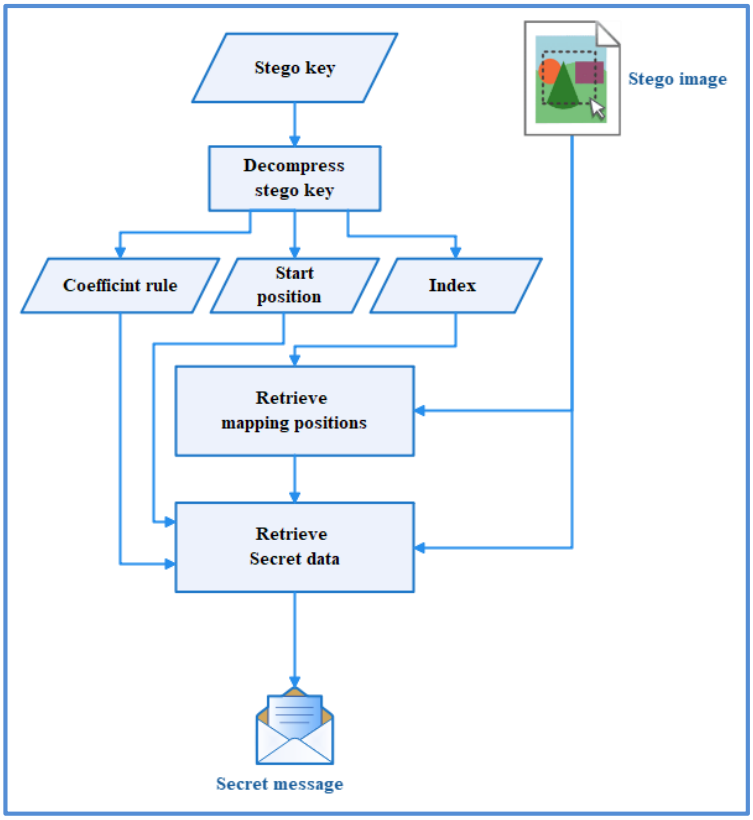


Figure (3): Extraction process

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

## 4. Experimental Results

The proposed algorithm is executed in MatLab R2021a. All studies are conducted on a PC equipped with a 2 GHz dual- Fig. 3. Extraction process core i7 processor 4th-generation and 16 GB RAM. All of the statistical data is averaged around twenty separate runs. The following examples of test images are taken from the USCSIPI Image Database (SIPI Image Database, n.d.).

To conduct the studies, a set of four carrier images with a grey level of 512x512 and 256x256 pixels are utilized, including (Pepper, Baboon, Jet, and Cameraman). Additionally, the proposed algorithm's performance is evaluated by using a secret message of Lena image in five different sizes. The sizes of the secret message are 8,192 bits, 12,000 bits, 20,000 bits, 32,768 bits, and 131,072 bits.

The GA parameters used in our experiment are listed in Table 2, the maximum GA generations number is set to 200. The improvement over the 200 generations with hiding 32,768 bits of the secret message is shown in Figure 4. The image indicates how the quality improves as the number of generations increases.

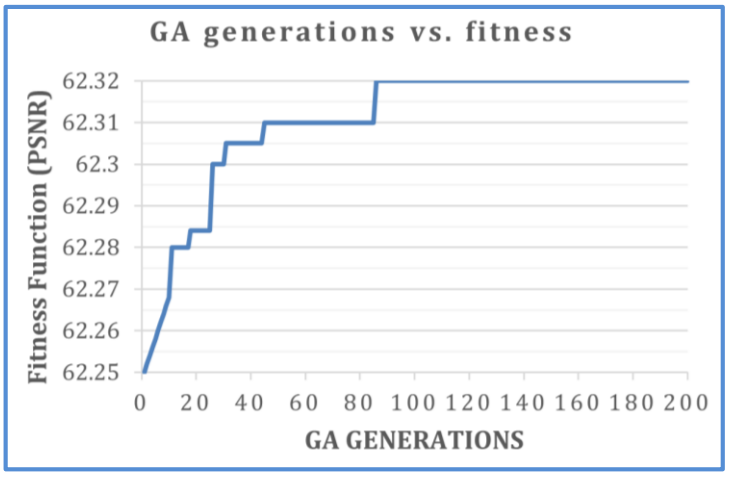


Figure (4): The evaluation of the PSNR over 200 GA generations

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

Table (2): Ga parameters

| Ga Parameter | Value |
|---|---|
| Population size | 200 |
| Crossover rate | 0.9 |
| Mutation rate | 0.1 |

Rather than setting the parameters of crossover rate and mutation rate, the test was conducted using a mutation rate of 0.05, 0.1, and 0.2 and a range of crossings between 0.1 and 0.9, as described in Figure 5. The crossover probability of 0.9 outperforms the other probabilities slightly, but the mutation rate of 0.1 outperforms the other probabilities.

The next section discusses the experimental results that evaluate the performance of the proposed system. The system's effectiveness is evaluated using imperceptibility analysis,

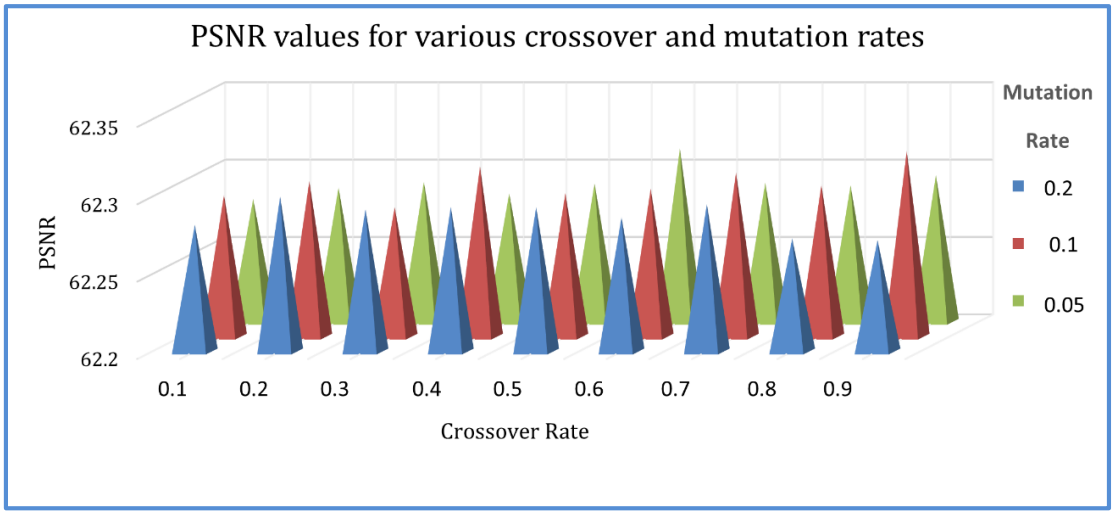


Figure (5): PSNR values for various crossover and mutation rates

visual and histogram analysis, and reversible analysis. Then the result of the proposed system is compared with previous work.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

4.1. Imperceptibility Analysis

Imperceptibility is the most important analysis to evaluate the power of the stenographic approach. It measures the effectiveness of hiding a secret message inside the cover image. The PSNR is used to measure the imperceptibility. PSNR evaluates the quality of stego-images and quantifies their distortion level. It compares the carrier and stego images and computes the variation in terms of pixel intensities. Decibel (dB) is used to express the PSNR ratio. A greater PSNR value indicates that the stego image has been subjected to less distortion, implying a higher quality. It is defined as shown in Eq. 1.

$$PSNR = 10 \times \frac{(255)^2}{MSE} \qquad (1)$$

Where MSE is an abbreviation for mean squared error. It is a commonly used statistical method for determining the difference between two images and is defined as as shown in Eq. 2.

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (x_{ij} - y_{ij})^2 \qquad (2)$$

Where W and H signify the image's width and height in pixels. $X_{ij}$ refers to the cover image pixel intensities of the $ij^{th}$ location, while $Y_{ij}$ refers to the stego image pixel intensities of the $ij^{th}$ location. A lower MSE value means a slight average difference between images, and conversely, the two identical images, MSE equals zero.

Table 3 shows the results of testing the system with different hiding capacities. The proposed system shows high quality performance Through different concealment capacities. According to (Armijo et al., 2020) the images with a PSNR value equal to 40

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

or greater are deemed to provide good quality and show a higher degree of similarity. The higher the value of PSNR, the better image quality is produced. The proposed system obtained a PSNR of 68.31 dB when 8,192 bits were hidden and a PSNR of 57.18 dB when 131,072 bits were hidden, as shown in Figure 6.

Table (3): The result of the proposed system with various hiding capacities

| Capacity (bits) | PSNR | | |
|---|---|---|---|
| | Baboon | Jet | Pepper |
| 8,192 | 68.32 | 68.20 | 68.41 |
| 16,384 | 65.21 | 65.34 | 65.29 |
| 32,768 | 62.17 | 62.45 | 62.34 |
| 65,536 | 60.13 | 60.39 | 60.24 |
| 131,072 | 57.08 | 57.28 | 57.19 |

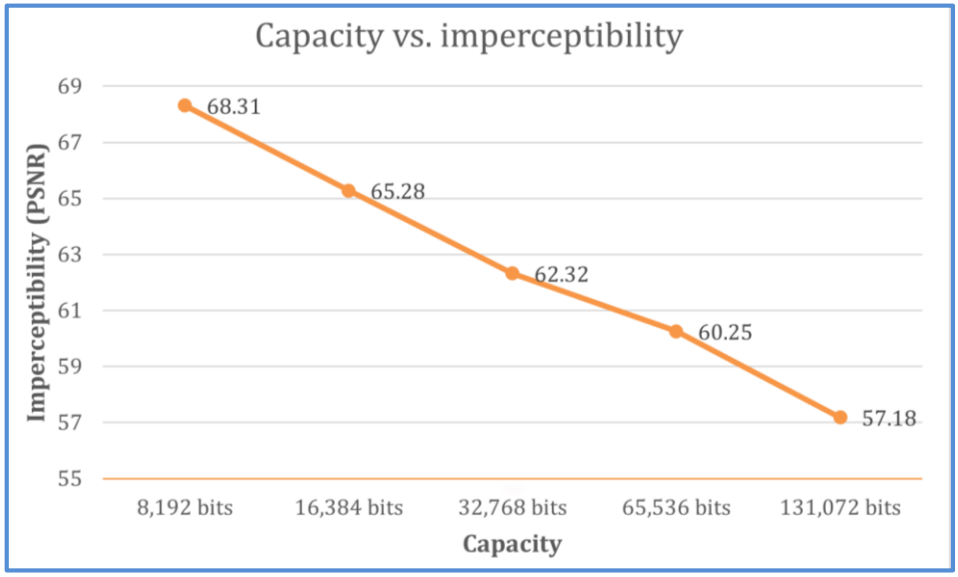


Figure (6): The relation between the capacity and imperceptibility

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

4.2. Visual and histogram analysis

The cover image and the stego image are analyzed visually using the human visual system (HVS). Grayscale images with a PSNR greater than 36 dB are indistinguishable by the human visual system (Saraireh et al., 2013). It is worth noting that the proposed method produces a stego image that is visually identical to the original image, as illustrated in Figure 7. Additionally, the histogram analysis is performed to compare the histograms of the cover images with the stego-images derived by the proposed system to ascertain the difference. As illustrated in Figure 8, the minimal difference in histograms between the cover and stego images. The proposed scheme of steganography is resistant to statistical attacks as the histogram will never reveal any secret pixels.

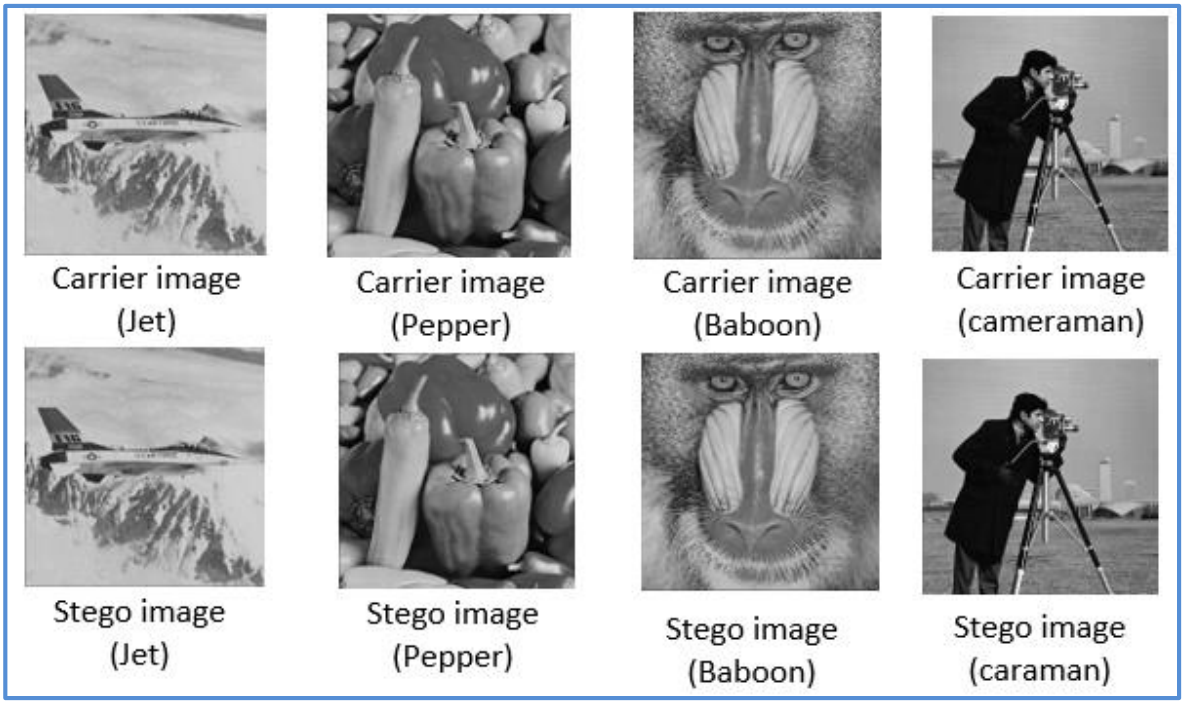


Figure (7): The Visual analysis for carrier and stego images

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

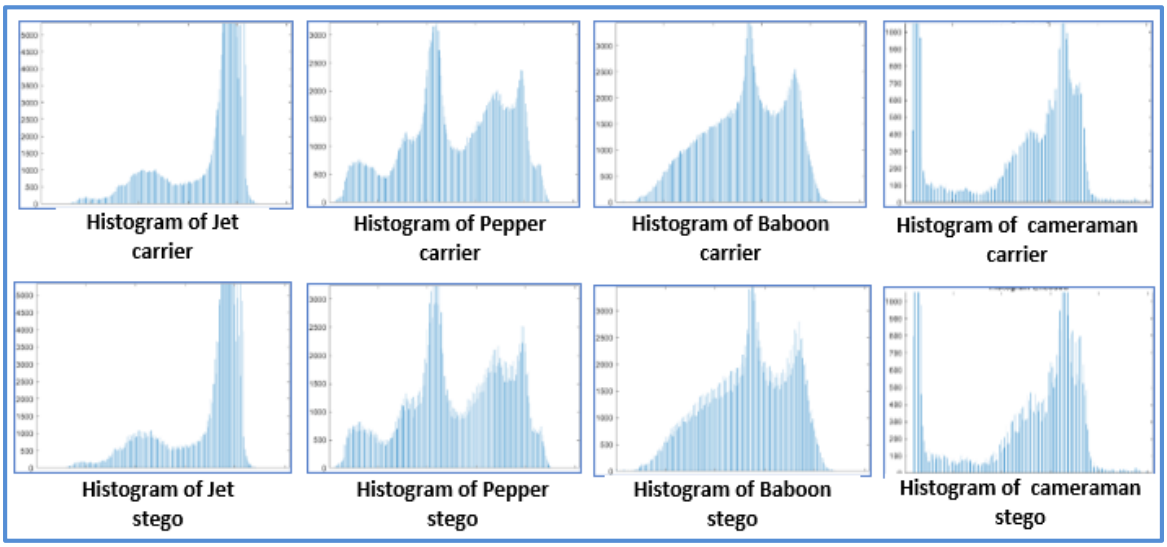


Figure (8): Analysis of histograms for carrier and stego images

4.3. Reversible analysis

The bit error rate (BER) is used to ensure that the proposed algorithm is a lossless and reversible process and verify an extraction process's effectiveness. It is defined as shown in Eq. 3:

$$BER = \sum_{i=1}^{n} (S_i \oplus E_i)/n \qquad (3)$$

Where: S refers to the secret message, E is the message after extracting, and ⊕ is the exclusive OR operation, and n is the total number of bits inserted (Rustad et al., 2022). The BER value falls between 0 and 1. The BER value should be 0 to ensure that the extraction process is entirely accurate. Table 4 shows the BER values for the secret message extracted from the stego image at different capacities. All of the images have a BER value of zero. As a result, we infer that the secret data extraction procedure is flawless for all capacities. There is no error in recovering the secret message from the stego image.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

Table (4): The BER values at various capacities

| Capacity (bits) | PSNR | BER |
|---|---|---|
| 8,192 | 68.31 | 0 |
| 16,384 | 65.28 | 0 |
| 32,768 | 62.32 | 0 |
| 65,536 | 60.25 | 0 |
| 131,072 | 57.18 | 0 |

4.4. Comparison with previous work

In order to evaluate the efficiency of the proposed system with other research methods, it has been compared with steganography techniques based on adaptive GA-based performance by using the same dataset. The performance of the proposed system is shown in Table 5, along with comparisons to other GA-based steganography systems. The proposed system achieves higher PSNR values when compared to the other methods.

Table (5): Comparison of the performance of the proposed system and GA-based systems

| Stego image | Stego image Size 512x512 | | | Stego image Size 256x256 | | |
|---|---|---|---|---|---|---|
| | (Soleimanpour & Talebi, 2013) | (Wazirali et al., 2019) | Proposed system | (Shah & Bichkar, 2018) | (Kanan & Nazeri, 2014) | Proposed system |
| Pepper | 53.22 | 59.08 | **60.18** | N/A | 54.28 | **56.26** |
| Baboon | 53.31 | 59.27 | **60.13** | 54.43 | 54.25 | **56.24** |
| Jet | 53.15 | 59.15 | **60.21** | N/A | 54.30 | **56.22** |
| Cameraman | 53.18 | N/A | **60.27** | 52.36 | N/A | **56.16** |

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

4.5. Security analysis

Since the secret message is embedded in a non-sequential way. Furthermore, the stego key consists of three keys (the start position key, the data mapping key, and the index key), and the stego key is long. As a result of that, the stego key is very secure and not guessable. At the same time, getting the secret message would be impossible without getting the stego key and distinguishing between its three parts.

## 5. Conclusion

In this work, a new method that combines data mapping and GAs techniques have been proposed to enhance the security of image steganography in the spatial domain. The system embeds the secret message by data mapping into a specific part of the cover image, then embeds the coefficients that resulted from the data mapping by GA into the rest of the cover image and generates the index key. The compression process is applied on the (start position key, coefficient rule key, and index key) to generate the stego key. Given that the secret message is embedded in a non-sequential way. Furthermore, the stego key is long. Therefore, the stego key is very secure and not guessable. The secret message cannot be recovered without obtaining all these three components of the stego key in their entirety and in the right sequence. The experimental results showed that the proposed system outperforms similar techniques when the imperceptibility is measured against other GA-based steganography systems. Moreover, the results proved that the distortion in the stego images is invisible to (HVS) system, and the histogram differences between the cover and stego images is negligible.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

**References**

[1] Alatawi, H., & Narmatha, C. (2020, September). The Secret image hiding schemes using Steganography-Survey. In 2020 International Conference on Computing and Information Technology (ICCIT-1441) (pp. 1-5). IEEE. **https://doi.org/10.1109/ICCIT-144147971.2020.9213764**

[2] Aldwairi, M., Hamzah, A. Y., & Jarrah, M. (2019). MultiPLZW: A novel multiple pattern matching search in LZW-compressed data. Computer Communications, 145, 126-136. **https://doi.org/10.1016/j.comcom.2019.06.011**

[3] Alsaidi, A., Al-lehaibi, K., Alzahrani, H., AlGhamdi, M., & Gutub, A. (2018). Compression multi-level crypto stego security of texts utilizing colored email forwarding. Journal of Computer Science & Computational Mathematics (JCSCM), 8(3), 33-42. **https://doi.org/10.20967/jcscm.2018.03.002**

[4] Armijo-Correa, J. O., Murguía, J. S., Mejía-Carlos, M., Arce-Guevara, V. E., & Aboytes - González, J. A. (2020). An improved visually meaningful encrypted image scheme. Optics & Laser Technology, 127, 106165. **https://doi.org/10.1016/j.optlastec.2020.106165**

**[5]** Bäck, T., Fogel, D. B., & Michalewicz, Z. (Eds.). (2018). Evolutionary computation 1: Basic algorithms and operators. CRC press. **https://doi.org/10.1201/9781482268713**

[6] Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security Journal: A Global Perspective, 25(4-6), 197-212. **https://doi.org/10.1080/19393555.2016.1206640**

[7] Bhuiyan, T., Sarower, A. H., Karim, R., & Hassan, M. (2019, July). An image steganography algorithm using LSB replacement through XOR substitution. In 2019 International Conference on Information and Communications Technology (ICOIACT) (pp. 44-49). IEEE. **https://doi.org/10.1109/ICOIACT46704.2019.8938486**

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

[8] 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**

**[9]** Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. IEEE Access, 8, 166589-166611. **https://doi.org/10.1109/ACCESS.2020.3022779**

[10] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66. **https://doi.org/10.1016/j.image.2018.03.012**

**[11]** Ibanez, A. L., Djamal, E. C., Ilyas, R., & Najmurrokhman, A. (2018, July). Optimization of least significant bit steganography using genetic algorithm to improve data security. In 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE) (pp. 523-528). IEEE. **https://doi.org/10.1109/ICITEED.2018.8534935**

[12] Ignatoski, M., Lerga, J., Stanković, L., & Daković, M. (2020). Comparison of entropy and dictionary based text compression in English, German, French, Italian, Czech, Hungarian, Finnish, and Croatian. Mathematics, 8(7), 1059. **https://doi.org/10.3390/math8071059**

[13] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326. **https://doi.org/10.1016/j.neucom.2018.06.075**

[14] Kalaichelvi, V., Meenakshi, P., Vimala Devi, P., Manikandan, H., Venkateswari, P., & Swaminathan, S. (2021). A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique. Journal of Ambient Intelligence and Humanized Computing, 12(7), 7235-7243. **https://doi.org/10.1007/s12652-020-02398-w**

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

[15] Kanan, H. R., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert systems with applications, 41(14), 6123-6130. **https://doi.org/10.1016/j.eswa.2014.04.022**

[16] Khan, M., Jamal, S. S., & Waqas, U. A. (2020). A novel combination of information hiding and confidentiality scheme. Multimedia Tools and Applications, 79(41), 30983-31005. **https://doi.org/10.1007/s11042-020-09610-1**

[17] Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital Image Steganography: A Literature Survey. Information Sciences. **https://doi.org/10.1016/j.ins.2022.07.120**

[18] Nosrati, M., Hanani, A., & Karimi, R. (2015, February). Steganography in image segments using genetic algorithm. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp. 102-107). IEEE. **https://doi.org/10.1109/ACCT.2015.57**

[19] Panah, A. S., Van Schyndel, R., Sellis, T., & Bertino, E. (2016). On the properties of non-media digital watermarking: a review of state of the art techniques. IEEE Access, 4, 2670-2704. **https://doi.org/10.1109/ACCESS.2016.2570812**

**[20]** Pandey, H. M. (2016). Performance evaluation of selection methods of genetic algorithm and network security concerns. Procedia Computer Science, 78, 13-18. **https://doi.org/10.1016/j.procs.2016.02.004**

[21] Qin, J., Luo, Y., Xiang, X., Tan, Y., & Huang, H. (2019). Coverless image steganography: a survey. IEEE Access, 7, 171372-171394. **https://doi.org/10.1109/ACCESS.2019.2955452**

[22] Resende, P. A. A., & Drummond, A. C. (2018). Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling. Security and Privacy, 1(4), e36. **https://doi.org/10.1002/spy2.36**

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications ( MECSJ )
Issues (59) 2021
ISSN: 2616-9185
www.mecsj.com

[23] Rustad, S., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. Journal of King Saud University-Computer and Information Sciences, 34(6), 3559-3568. **https://doi.org/10.1016/j.jksuci.2020.12.017**

[24] Saraireh, S. (2013). A secure data communication system using cryptography and steganography. International Journal of Computer Networks & Communications (IJCNC) Vol, 5, No.3. **https://ssrn.com/abstract=3668796**

[25] Shah, P. D., & Bichkar, R. S. (2018). A secure spatial domain image steganography using genetic algorithm and linear congruential generator. In International conference on intelligent computing and applications (pp. 119-129). Springer, Singapore. **https://doi.org/10.1007/978-981-10-5520-1_12**

[26] Shah, P. D., & Bichkar, R. S. (2021). Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure. Engineering Science and Technology, an International Journal, 24(3), 782-794. **https://doi.org/10.1016/j.jestch.2020.11.008**

[27] Shehzad, D., & Dag, T. (2017, August). A novel image steganography technique based on similarity of bits pairs. In 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC) (pp. 99-104). IEEE. **https://doi.org/10.1109/ICSGRC.2017.8070576**

[28] Shih, F. Y. (2017). Digital watermarking and steganography: fundamentals and techniques. CRC press. **https://doi.org/10.1201/9781315121109**

[29] SIPI Image Database. (n.d.). Retrieved September 27, 2021, from **https://sipi.usc.edu/database/database.php**

[30] Soleimanpour-Moghadam, M., & Talebi, S. I. A. M. (2013). A novel technique for steganography method based on improved genetic algorithm optimization in spatial

domain. Iranian Journal of Electrical and Electronic Engineering, 9(2), 67-75. **https://20.1001.1.17352827.2013.9.2.4.5**

[31] Swain, G. (2016). A steganographic method combining LSB substitution and PVD in a block. Procedia Computer Science, 85, 39-44. **https://doi.org/10.1016/j.procs.2016.05.174**

[32] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing. **https://doi.org/10.1088/1757-899x/518/5/052003**

[33] Walia, G. S., Makhija, S., Singh, K., & Sharma, K. (2018). Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map. Optik, 170, 106-124. **https://doi.org/10.1016/j.ijleo.2018.04.135**

[34] Wang, Y., Tang, M., & Wang, Z. (2020). High-capacity adaptive steganography based on LSB and Hamming code. Optik, 213, 164685. **https://doi.org/10.1016/j.ijleo.2020.164685**

[35] Wazirali, R., Alasmary, W., Mahmoud, M. M., & Alhindi, A. (2019). An optimized steganography hiding capacity and imperceptibly using genetic algorithms. IEEE Access, 7, 133496-133508. **https://doi.org/10.1109/ACCESS.2019.2941440**