A NEW COMBINED METHOD WITH HIGH SECURITY FOR DIGITAL IMAGES STEGANOGRAPHY BASED ON IMPERIALIST COMPETITIVE ALGORITHM AND SYMMETRIC ENCRYPTION ALGORITHM

Mohammad Tahghighi Sharabyan¹, Hamid Ghorbani²

¹Department of computer engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran
²Department of computer engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran
Author Correspondence: Iran, +989123412834, m.hamid.ghb@gmail.com

Abstract: - Today, with the growing expansion of information and communication technology, the world, through digital data, is moving to the digital world and communications. Meanwhile, the role of internet as a public communication channel is becoming more and more important in the world of communication every day. In addition, maintaining security and creating confidential communications are of particular importance regarding the general structure of this communication channel. Cryptography and information steganography are two important issues in security systems. Both encryption and steganography techniques are not effective for high security information alone, but combining these two methods can greatly improve the confidentiality and security of confidential information. Recently, new hybrid algorithms have been proposed using cryptography and steganography. However, in these methods, attempts have been made to increase the security of censorship by using random factors and hidden keys, most of these methods are broken by examining the statistical components of the images. In this paper, a high-security hybrid approach is proposed to digital images steganography based on the Imperialist Competitive Algorithm and Symmetric Cryptography Algorithm. The proposed method, by considering the Imperialist Competitive Algorithm, creates a high quality, high-security image. Prior to data insertion, symmetric encryption of information takes place, and then encrypted information is embedded in the cover image. The results of the implementation of the proposed method show that in addition to enhancing the image quality of the steganography, it is more secure than other methods.

Keywords: Security, Encryption, Steganography, Imperialist Competitive Algorithm, Digital Images.

1. Introduction

Regarding the advances in Information and Communication Technology (ICT), much of the information is stored electronically. As a result, information security and protection against unauthorized access has become a major issue. Encryption and steganography are techniques used to secure information. Encryption makes information unintelligible, so that the user cannot decrypt without a decryption key. Steganography is a digital technique for concealing information in a cover media such as text, audio, image. Besides, these two techniques can be combined and provide a higher level of security [1]. The main difference between encryption and steganography is that the purpose of the encryption is to hide the contents of the message, not the message in general, while the purpose of the steganography is to conceal any sign of the existence of the message. In cases where the encrypted data exchange is problematic, there must be a hidden connection. Table 1 describes the differences between steganography and cryptography. Therefore, information steganography is a way to move
the information in the form of an overlapping agent with the highest degree of security accuracy between the points in question, so that even if along the way, information was accessed by unauthorized persons, there would be no access to hidden data. In fact, steganography is the science and art of embedding information in a carrier medium which is rising due to the significant advances in digital communication. The main purpose of steganography is security to mean inability in proving the existence of the message. Images are the most important media used especially on the internet, and human perception of the changes in images is limited. Images are a kind of appropriate cover media for steganography; many of the existing methods use common methods for image steganography, which attacks to crack the secret message is discussed in this case. In this paper, we present a high-security hybrid approach for digital image steganography based on Imperialist Competitive Algorithm and Symmetric Cryptographic Algorithm. In this method, firstly, the use of symmetric cryptographic techniques before steganography and, secondly, the steganography of information encoded by the Imperialist Competitive Algorithm. Applying symmetric cryptography in the proposed method for achieving security is used, while Imperialist Competitive Algorithm is used to enhance the quality of the image steganography. Therefore, in the proposed method, in addition to hiding information, encryption is also done.

Table 1: Comparison between steganography and encryption

<table>
<thead>
<tr>
<th>Background</th>
<th>Steganography</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host files</td>
<td>Image, sound, text, and so on</td>
<td>More text files</td>
</tr>
<tr>
<td>Hidden files</td>
<td>Image, sound, text, and so on</td>
<td>More text files</td>
</tr>
<tr>
<td>Result</td>
<td>Stego file</td>
<td>Encrypted file</td>
</tr>
<tr>
<td>Type of attack</td>
<td>A file analysis aimed at finding out whether or not the file is stego</td>
<td>Decrypt</td>
</tr>
<tr>
<td>Goals</td>
<td>Preservation of a secret message</td>
<td>Maintain the contents of a secret message</td>
</tr>
<tr>
<td>applications</td>
<td>Used to provide information security</td>
<td>Used to provide information security</td>
</tr>
<tr>
<td>Provide security services</td>
<td>Confidentiality, identification, authentication</td>
<td>Confidentiality, data integrity and authentication identify undeniable</td>
</tr>
<tr>
<td>Specific technology problems</td>
<td>Key distribution</td>
<td>Key Distribution, Decoding Law Enforcement</td>
</tr>
</tbody>
</table>

2. Related works

In this section, we study and evaluate hybrid methods for maintaining confidential information using cryptography and steganography. In [2], in addition to using the LSB substitution technique as an essential step, edge detection is also used. Research [3] uses a fuzzy logic and image processing techniques to develop an unobservable image steganography plan for development. The proposed scheme uses fuzzy data transformation of hidden data. Image processing techniques are used for implementing pixel classification and fuzzy techniques to select pixel coatings during latent data substitution. In another stage, by Genetic Algorithm, the values of pixels are adjusted so that the parameters of RS are satisfied normal image conditions [4]. This method works in the first step, like the simple LSB method, and embeds the bits in the host image. In the next step, by using the genetic algorithm, the pixel values are adjusted so that the value of the RS parameters in the normal image conditions is true. In [5], the author used the AES-based algorithm, in which the encryption process is a unique bit or the use of a pixel-based image set with a 128-bit key, which changes for each set of pixels. The keys are used independently on the transmitter and receiver side, based on the development process of the AES key. In the article [6], authors propose a way to hide information inside the image using the LSB and MSB substitution technique, which is as follows: (Public key and private key) are encrypted according to the RSA algorithm and the secret messages, and then the information is embedded in the carrier pixels by the LSB and MSB method. Therefore, the image is used as a cover for insertion of cached information. This process ends with low value bits by replacing a much smaller amount of pixel values with encrypted bit bits. In the authors’ study [7], a scheme of combining cryptography and steganography has also suggested secrecy of super-secret information that increases the level of security which is used to securely exchange private information between executives or governments. This method offers two levels of security: the first is the cryptographic process, and the second is to increase the level of steganography security to hide the information. In the first stage, the message was sent and converted to a cipher image using the first process of encryption. Then, in the second step, this encoding image is converted to an intermediate text using the second encryption process. The middle encrypted text or
information is included inside a cover image using the cryptographic process. In [8], a new secure communication protocol is presented by a combination of steganography and cryptographic techniques, which is based on the LSB method and the Boolean function in the development of crypto scopes. The used cover media focuses on black and white images, and Boolean functions are used to encrypt and control pseudo-random increase or reduce LSB. In this paper [9], an irreversible plan to hide a serial image is presented in a cover image that can improve the visual quality and the security of the image steganography. This is achieved by a hybrid cryptographic design, including the Noise Sight Field Function (NVF) and the optimal chaos based on the encryption scheme. Gaba and Kumar have provided a technique for steganography called Encrypt-Stego-Compress in which preprocessing of text is done before hiding it behind a cover image [10]. In preprocessing, the text is compressed for the first time and then modified using a key. The processed text behind the cover image is hidden using a domain-based conversion based on steganography. DCT is used to convert the cover image to the frequency domain. Table 2 provides a comparative study of the methods presented for image steganography.

Table 2: A comparative study of the methods provided for Image steganography

<table>
<thead>
<tr>
<th>Field used</th>
<th>Carrier object</th>
<th>Method used</th>
<th>Adaptive</th>
<th>Encryption before insertion</th>
<th>Compression</th>
<th>Parameter Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place</td>
<td>Image</td>
<td>Combined Edge Detector</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Method [2]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>Fuzzy domain transfer and pixel classification</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Method [3]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>Genetic Algorithm</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Method [4]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>Based email</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Method [5]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>LSB and MSB replacement</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Method [6]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>RSA algorithm and LSB technique</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Method [7]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>LSB and Boolean function</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Method [8]</td>
</tr>
<tr>
<td>Place</td>
<td>Image</td>
<td>Optical visual noise and optimal chaos</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Method [9]</td>
</tr>
<tr>
<td>Frequency</td>
<td>Image</td>
<td>Text preprocessing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Method [10]</td>
</tr>
</tbody>
</table>

3. Imperialist Competitive Algorithm

In Imperialist Competitive Algorithm, N countries are considered for the solution of the optimization problem, each of which is represented by a vector and represents a point in the N-dimensional space. From these points, the points that have the lowest cost according to the optimization function are considered colonizers and the rest are considered as colonies. For each colonist, at first, the normalized cost is calculated as follows:

$$C_i = \frac{C_i - C_{\text{norm}}}{\max[C_i]}$$

(1)

where $C_i$ is the i-th imperial cost, $\max[C_i]$ is the greatest cost between imperialists and $C_{\text{norm}}$ is the normalized cost of this imperialist. With the cost of normalized, normalized relative strength of the imperialist is calculated as follows and based on which colonial countries are divided between imperialists:

$$P_n = \left[ \frac{C_n}{\sum_{l=1}^{N_{\text{imp}}} C_l} \right]$$

(2)

Thus, the first number of colonies of an imperialist will be equal to:

$$N \cdot C_n = \text{round}(P_n \cdot N_{\text{col}})$$

(3)

where $N \cdot C_n$ is the first number of colonies in an empire and $N_{\text{col}}$ is the total number of colonial countries in the population of the primary countries. With the primitive state of all empires, the Imperialist Competitive Algorithm begins. Figure 1 shows the movement of the colonies towards the imperialist country.
Figure 1: The general idea of the movement of the colonies toward the imperialist

As is shown in Figure 1, we have for $X$:

$$x \sim U(0, \beta \times d),$$

(4)

Where $\beta$ is a number greater than one and close to $2$. $\beta = 2$ can be a good choice. The existence of coefficient $1 < \beta$ makes the colonial country be closer to the colonial country as it moves in different directions. To increase the search area around the colonial, an angular deviation which equals $\theta$ and follows a randomly distributed distribution, is added to the main vector:

$$\theta \sim U(-\gamma, \gamma),$$

(5)

$\gamma$ is a parameter that controls the range of angular deviation and is considered $\frac{\pi}{2}$ in the experiments. The next step is the colonial competition. At this stage, the weakest colony is selected from the weakest empire and is given to a strong empire (not necessarily the strongest empire). Of course, the chance choosing a stronger empire is higher. Eventually, when an empire lost all its colonies that empire is out of the list of empires and is given as a colony to other empires in colonial competition. The evolution process is in a loop that continues until a stop condition is met.

4. Description of the proposed method for digital image steganography

In this section, we propose a method for digital images steganography based on the Imperialist Competitive Algorithm and information encryption. The proposed method has two parts. The first process of encrypting confidential information is symmetric and the second is the process of embedding encrypted information in digital images based on Imperialist Competitive Algorithm. To enhance the security of confidential information, the first is to encrypt confidential information, then the encrypted information is embedded in digital images. Embedding the Lowest Bits (LSB) is a known mechanism for implementing data steganography methods. In the proposed method, LSB method is used to insert confidential data.
4.1 Encryption of confidential information

In this section, confidential information is encrypted symmetrically. Confidential information is text-based, and this information is first converted to an array of bits, then encryption is performed. In the proposed method, text encryption is used with symmetric key. The proposed method first converts the secret text into an array of characters and then to bits, and then encrypts the data bits using symmetric encryption and with 128-bit keys. In the proposed method, first, confidential information is converted into an array of characters and then converted into an array of bits. The key length for encryption of information should be ideal; if the key length is longer, the security is better and the speed is lower, and vice versa, if the key length is lower, security becomes lower and cryptographic information speeds up. In the proposed method, the 128-bit key length is considered. After selecting the key length, the bit array is applied to the 128/2 range. The bit array is divided into 64-bit length; this is for confidential information encryption. At each step of encryption, XOR is applied; performing the XOR operation is in such a way that, after dividing the array of bits into 64-bit, the two parts of the bitmap array, which is 128-bit, is performed by the XOR's encryption key (which is 128-bit). After encrypting the first part of the array, This time, half the second part of the array is performed with the half of the first part of the array with the XOR key. This operation continues until the array and encryption operation are completed. In the proposed method, the XOR operator is used for the convenience of encryption and decryption [11]. How to perform text encryption is shown in Figure 3:

Figure 2: The process of embedding information in the cover image
Embedding the encrypted information in the cover image

After encrypting confidential information with an array of encrypted bits, the process of embedding the bits in the host image using the Imperialist Competitive Algorithm; the XOR operator and the LSB technique are performed. As we said, the LSB technique is one of the steganography methods that hide the secret message inside the bits of the bits directly in the host image to prevent unauthorized access. Therefore, the most important advantage of LSB is that, with the change in bits, the human eye cannot see that change. The Imperialist Competitive Algorithm acts as a key to embed information. The main idea of the problem of steganography is raised as a search and optimization issue. The purpose of this project is to find the direction and the starting point in the cover image to hide the confidential information so that the PSNR of the steganography image is maximized. As can be seen in Figure 4, to apply the Imperialist Competitive Algorithm to cover image capture, each country is considered as a 128-bit array. The initial value of each country (128-bit votes) is random. After the algorithm is executed, the country value changes.

Figure 4: Displaying the country for embedding confidential information

In the proposed method, we want to embed confidential (encrypted) data into digital images (cover image). The image dimensions are 512 × 512. Embedding information in the cover image pixels is done by the XOR operator. The XOR operator is used to easily embed and extract information in the proposed method. To insert information in the cover image, it acts as any pixel of the cover image of 8 bits. To insert information in LSB1 and LSB2, each pixel of the cover image, first, the first bit of the country with the fourth bit of the first pixel of the cover image is performed by the XOR operation, then the bit value obtained is again performed with the first bit of the encrypted information array of the XOR operation. Then the bit value obtained in LSB1 is inserted in the first pixel of the cover image. The same method is done to insert information in LSB2. The same procedure is used to insert the rest of the confidential information bits in the cover image pixels. The process of embedding confidential information in a pixel of the host image is expressed in Figure 5.
After entering the confidential information in the host image blocks, the PSNR value is calculated between the original image and the hiding image. The greater value for PSNR shows the high quality of the steganography images. For all countries this is done and the PSNR value is calculated. The high PSNR value is chosen in the proposed method as the best image steganography. After the information is inserted, an update of the Imperialist Competitive Algorithm is performed. The fitness function is one of the most important steps in choosing the best country with high PSNR. While the Imperialist Competitive Algorithm aims to improve image quality, it can be a suitable choice of signal-to-noise ratio (PSNR) test.

5. Results of the proposed method implementation

To evaluate the proposed method, standard images are used to cover the gray scale with dimensions of $512 \times 512$ (pixels). Also the encrypted text information is used for embedding. Implementation of the proposed method has been done using MATLAB software. In order to measure the quality of the image steganography, the quantitative metric PSNR (the first case of the peak signal to noise ratio) criterion is used, which is calculated according to equation 6. In the PSNR relationship, MSE is the mean square difference between the corresponding pixel values in the cover image and the hiding image. The PSNR unit is decibel (dB).

$$\text{PSNR} = 10 \log_{10} \left[ \frac{(255^2)}{\text{MSE}} \right] (dB)$$

(6)

Where $B_{ij}$ and $A_{ij}$ are gray pixel values $(i,j)$ of covert images and steganography, $X$ and $Y$ are the length and width of the cover image.

$$\text{MSE} = \sum_{i=1}^{X} \sum_{j=1}^{Y} \frac{(A_{ij} - B_{ij})^2}{XXY}$$

(7)

Figure 6 shows cover images for steganography. The proposed method has been applied to both images and the PSNR value for the cover image and steganography image has been calculated. The cover images are gray and each dimension is 512 by 512 pixels. Most steganography techniques use these images for implementation. Figure 7 shows a portion of the secret information for encryption. This information is encrypted using the symmetric method and then embedded in the cover images using the Imperialist Competitive Algorithm.
Steganography and cryptography achieve separate goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message (Lou and Liu, 2002). Furthermore, steganography provides more confidentiality and information security than cryptography since it conceals the mere existence of secret message rather than only protecting the message contents. Therefore, one of the major weaknesses of cryptosystems is that even though the message has been encrypted, it still exists.

Even though both cryptographic and steganographic systems provide secret communications, they have different definitions in terms of system breaking.

Hello dear how are you my name is Muhammad Fayaaz. I belong to Odigam i am doing my project.

A cryptographic system is considered broken if an attacker can read the secret message.

However, a steganographic system is considered broken if an attacker can detect the existence or read the contents of the hidden message. Moreover, a steganographic system will be considered to have failed if an attacker suspects a specific file or steganography method even without decoding the message.

As a result, this consideration makes steganographic systems more fragile than cryptographic systems in terms of system failure. Additionally, steganographic systems must avoid all kinds of suspicion in order to achieve security and not be considered failed systems.

The embedded capacity used to embed information is two bits (25%) of 8 bits of pixels; that is, two pixel low bits are used. Table 3 and 4 show the PSNR value for a steganography image with a 25% embedding capacity. The high PSNR value depends on the amount of information and the capacity to embed information in the host image. Whatever the amount of confidential information is smaller, the insert of information in the images is not high and the PSNR value increases. Therefore, if the capacity is low, the PSNR is likely to increase.

Table 3: Experimental Results of the proposed method for different images

<table>
<thead>
<tr>
<th>Capacity %</th>
<th>Embedding capacity</th>
<th>PSNR Lena</th>
<th>PSNR Baboon</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>2</td>
<td>58.241</td>
<td>58.3401</td>
</tr>
</tbody>
</table>
Table 4: PSNR value of the proposed method

<table>
<thead>
<tr>
<th>Image</th>
<th>Embedded capacity in percent</th>
<th>The average value of PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>25%</td>
<td>58</td>
</tr>
</tbody>
</table>

For Table 4, the Lena image, which has been steganography, has a capacity to embed a value of PSNR = 58. This value shows the quality of the steganography image. Table 5 shows that the proposed algorithm is better than all the methods compared. In reference [12], the authors have proposed a new method for sharing serial images based on the threshold design \((K,n)\) with additional steganography and authentication capabilities. In [13], a plan is proposed to improve the authentication ability that prevents dishonest participants. The proposed design also defines the order of embedded bits to improve the quality of the steganography image. In [14], a picture sharing scheme is presented with the combination of steganography and authentication based on the remaining Chinese case (CRT). In [15], a picture sharing scheme is presented using the optimal pixel setting process to enhance the image quality and the various conditions of the authentication bits. The quality of the resulting steganography image in the proposed method is higher than other methods. The results of the implementation in this article are as follows: Capacity in pixel space depends on the number of bits assigned to each pixel to display the color. The type of image is very effective in achieving the desired results in steganography. Given the low effectiveness of the LSB bit in the appearance of the image, in most of the proposed methods, data insertion in these bits is used. Data hiding in pixel space should be done in random situations based on an agreed key between the transmitter and the receiver. As Table 5 shows, the proposed algorithm is better than all compared methods.

Table 5: Comparative performance of the proposed method with different steganography algorithms

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>39.19</td>
<td>41.58</td>
<td>39.84</td>
<td>43.54</td>
<td>58.34</td>
<td></td>
<td>PSNR value</td>
</tr>
</tbody>
</table>

The goal of the proposed method is to increase the PSNR value by considering the high embedding capacity. Therefore, the balance between the embedding capacity and the PSNR value should be maintained. (This can be achieved with the method of embedding and using the appropriate method). Figure 8 shows the graph of the PSNR values for Baboon and Lena images. The PSNR values of our proposed method, with 25% embedding capacity, show more embedding capacity than other methods.

Figure 8: PSNR values for different images
Figure 9: Histogram of the original image (left) and steganography (right) for the image of the bubble

Figure 10: Original histogram (left) and steganography histogram (right) for Lena image

The histogram is a graph of the gray levels in the image. The histogram plotting provides a general description of the appearance of the image. A bunch of hidden attacks is based on the histogram analysis of the steganography image. In these methods, the more histograms of the steganography images are closer to the histogram of the cover images, the likelihood of detecting confidential information in steganography images decreases and vice versa. In Figures 9 and 10, histograms are steganography and cover images for Baboon and Lena images are depicted. As shown in this figure, no significant changes have taken place in the histogram of cover images after embedding confidential information. Therefore, the proposed steganography method retains the histogram characteristics of the cover image after embedding confidential data.

Figure 11: Cover image (left) and steganography image (right)
In order to verify the visual quality of the steganography images generated by the proposed algorithm, we put together the main image and the steganography image, which shows the distortion and error between the main cover image and the steganography image are visually intuitive and perceptual. As can be seen from Figures 11 and 12, the quality of the steganography image is not significantly different from the original image, showing the high quality of the steganography image.

6. Conclusion

In this paper, we propose a secure method for the secrecy information steganography using the Imperialist Competitive Algorithm and symmetric cryptography in the location area. In the presented method, first, the confidential information was encrypted, then the encrypted information in the cover images was embedded using the Imperialist Competitive. Embedding information in the image pixels was done by considering the LSB method. The results indicate that the use of the proposed scheme increases the security of confidential information and improves the quality of the steganography image and also renders it resistant to attacks. Steganography image is visually recognizable from the corresponding host image. That the proposed algorithm can create a high-quality hidden image and the demand for embedded capacity by satisfying users are satisfactory. Our proposed method is simple and practical for steganography applications. According to the implementation results, the use of cryptographic and steganography configurations can be of great help in increasing the efficiency of security systems. Our next task is to focus on improving the efficiency of the proposed method, especially by using other meta-heuristic algorithms such as Firefly Algorithm, Queen Bee Honey Algorithm.

REFERENCES