Efficient Approach of Image Hiding

Haval Muhammed Sidiqi, Prof. Dr. Muzhir Shaban Al-Ani

ABSTRACT— In the End, the thesis was covered an efficient method of construction a secure image hiding approach in digital images. The digital image steganography process has been achieving the improvement of constrained intensity of human visual system (HVS). Image steganography method was utilized image as cover media for hiding secret message. The major principles necessities for a steganography framework are to be untraceable while augmenting the measure of the data is going to embed into spread unique image. The proposed encoding of restricted image based on chaos approach, in which the image was distributed into various sorts then interchange these parts to generate the new form of depiction. The next step was applying discrete wavelet transform, so the facsimile data was prepared to be concealed. The performance measurement has been applied in this approach to find peak signal to noise ratio (PSNR) and mean square error (MSE) between embedded and extracted image. The obtained results indicated that this approach leading to more secure approach comparing to other methods. The archived values of PSNR is in between 38.7447 and 59 depending on the size of the secret image.

Index Terms— Chaotic Approach, DWT, Data hiding, Image Steganography, Image processing, Spatial Domain, Security.

1 INTRODUCTION

Hence, the promotion of utilizing Internet to send and receive data one of the best principle reasons of data innovation and correspondence has been the security of data [1]. Cryptography was formed as a method for hiding and securing the security of information and many different techniques have been established to decode and decrypt information in order to hide the message secret [2]. Unfortunately, sometimes not enough since the embedded message has been detected yet. The host can extract secret message easily, also the priority is protecting the encrypted message; secret from detection [3]. The method has been used to implement embedding data in audio, image and video, so called Steganography [4]. The object called cover object when by using steganography methods has been embedding secret information in a in such a way that existence of secret information was untraceable [5]. The most main requirement in digital image steganography schemes is imperceptibility and clearly [6]. The digital image, an audio file, or a video file is able to be inserted secret message into the original object [7]. The process of hiding secret information was known as payload, it might be a plain text, an image, a video file or a sound. Steganography techniques are grouped into two strategies methods spatial domain embedding and frequency domain embedding [8]. Cover image will be converted into bands (frequency components) after applying one of the discrete cosine transform (DCT), fast Fourier transform (FFT) or discrete wavelet transforms (DWT) then the data was encrypted on the bands coefficients [4], the technique called frequency domain [9]. Spatial domain spread image is the most broadly utilized information concealing strategy [10]. However, the attackers are able to detect secret message when the hiding technique created by least significant bit (LSB) Techniques [11]. Due to, high embedding capacity and low complexity chaotic approach was noticed in many fields [8]. Chaotic is a novel methodology in non-direct countless elements in genuine frameworks, both man-made and common, are being researched [13]. The Image steganography method is approximately used procedure to protected information used for hidden communication [14]. Such as featured tagging, military agencies copyright protection [12]. Steganography studies how to conceal restricted information and design a better (secure and fast) stego-image algorithms, and stegoanalysis endeavors to find security weaknesses of existing algorithms and studies whether or not they are vulnerable to some attacks [15]. Encryption is always for the purpose of protection, security of information and the reasons for the encryption are much more, including the interchange of confidential data between certain companies, certain government departments, and others. On the other hand, when you want to hide information, we include the information inside a medium and under a certain cover. So, the message does not appear to the primary mediator (image or video) due to an entire restriction [16]. The process was unsuspicious communicating beyond the sights. Therefore, one is able to say that the basic difference between encryption and information concealment is that when encryption or cryptography is known, the third party might know that there were two-way communication (two people or two) but cannot understand the information because it is encrypted [17]. In the case of steganography, the third party was not able to disclose the encrypted data or the connection between the two beyond, because an intermediary has been fulfilled to hide this connection altogether [18]. The process of embedding and extracting are defined in figure 1. A graphical representation is shown below [19] Embedding process is a transmitting secret image in to cover image in such a way that the expenses of the embedded message undetectable and the stage-image is going to be obtained from secret image inside the cover image. Extracting process finds out of the secret image.

Haval Muhammed Sidiqi: University of Sulaimani Polytechnic, College of Informatic, Department of Database, KRG Iraq .
Prof. Dr. Muzhir Shaban Al-Ani2: University of Human Development, College of Science and Technology, Department of Information Technology.

www.ijstr.org
Figure 1: Steganography Process

2 RELATED WORK

Steganography was enrolled to secure data by restricting information through Steganography techniques. Both of Cryptography and steganography methods has been used to protect from illegal access in multimedia processing. Thus, the crucial method for protection of information from attaches, copying and altering is image encryptions [22]. The field has embedded methods of cryptography and steganography which has already got resemblance and differences. Cryptography is used to encrypt messages so that they cannot be detected. In cryptography the message exists. On the other hand, steganography hide the details which refers to the existence of secret message by embedding the authentic message in another [23]. Over the last current years there are several various different steganography technique have been proposed. Analysis of statistical properties of the channel’s noise is a most of methods can be used for extract secret message from attaches [25]. Lately, many algorithm of steganography for two-color binary images have been proposed [24]. Covert channels, character arrangement, digital signatures are examples of detected secret data in steganography [26]. TsungYuan and Wen-Hsiang [18] was used to change tracking technique to propose a new steganography algorithm for hiding data in Microsoft Word documents. Sinha and Singh. [22] Was used the digital signature of the image to propose a technique to encrypt an image for secure transmission. It enables the recipient of a message to authenticate the sender of a message and verify that the message is intact. Kisik et al. [23] was proposed algorithm divides a bitmap image into bit plane images from LSB-plane to MSB-plane for each pixel, and considers each bit-plane image as a binary one which hides a secret message into bitmap images and palette-based images. K.Sakthidasan [24] was proposed A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images, The bigger key space, smaller iteration times and high security analysis applied in the system such as key space analysis, statistical analysis and sensitivity analysis.

3 METHODOLOGY

3.1 APPLIED ENVIRONMENT

A proposed system environment was implemented by using Visual Studio as IDE (Integrated Development Environment) and MATLAB as the graphics library. The application of the proposed system has been testified the image color (naturel image.bmp.jpg) shown in figure 2. , Mona Lisa has been used as a secret message and after steganography the corresponding stegoimage.

Figure 2: Simulation Environment

3.2 SECURE IMAGE ENCRYPTION

The chaotic approach was going to be shown in figure 3 by using the proposed method to encrypt the secret image and then embedded into the cover image after applying DWT technique. In this study, encrypted image achieved from cutting and replacing the positions of the original secretes image coefficients to mix up the relationships between the cipher-image and the plain-image [18].

Figure 3 chaotic method.
The chaotic approach is used to shuffle the positions of the image pixels in the spatial-domain. It is preprocessed to be suitable for the color scale image encryption, and the shuffled image is encrypted by the preprocessed signal pixel by pixel [21].

### 3.3 Proposed Approach

The proposed scheme was shown in figure 4. The stego Image consists of two stages. The first stage was the encoding stage, applying discrete wavelet and embedding. The second stage was extracting secret image and decoding. The quality measure is measured by PSNR and MEAN Square Error.

![Figure 4 Architecture of proposed system](image)

The load secret image is encrypted by the chaotic approach. After loading the secret image, we must create two loops to go through all rows and columns (actually each pixel) and get the red, green, blue (RGB) values from the secret image and store into array...

1. **Load Secret Image:**
   - After loading the secret image, we must create two loops to go through all rows and columns (actually each pixel) and get the red, green, blue (RGB) values from the secret image and store into array...

2. **Secret image encryption:** was done through three steps, first step the values of the pixels of secret image divided into four parts and shift between them, top with bottom and left with right. The second step has obtained image from first step then distributed into eight parts and replacing between parts. The last step has obtained image from second step then might be split into sixteen parts and going to be replacing one another. Each part of secret image might be encrypted by the strategy delineated.

3. **Apply discrete wavelet transform (DWT) to secrete image:** The DWT represents the signal in dynamic sub-band decomposition. Generation of the DWT in a wavelet packet allows sub-band analysis without the constraint of dynamic decomposition. It has become a powerful tool for signal processing and finds numerous applications in various fields.

4. **Load Cover Image:** The size of cover image is a 512 x 512. The original image has been load by creating two loops to go through all rows and columns (actually each pixel) and get the red, green, blue (RGB) values.

5. **Determine Maximum Coefficient (RGB):** In this stage the maximum coefficient for the cover image has been determined by finding the pixels to go through all rows and columns.

6. **Embedding process:**
   - Merge the most pixel values from the secrete image with the maximum values of cover image and get the stego image. The process is done by using the equation 3.
     
     \[ \text{Stego} = \text{Cover} + \text{Secret} \]

7. **Extraction Process:** Extracting each pixel of secrete image from stego image is going to be implemented by using equation 4.

8. **Secret image Decryption:** The process is going to be implemented as inverse of step 2.

9. **Performance Measurement:** Let us considered the original image \( P(i,j) \) and the stego image \( S(i,j) \). Regarding to this assumption, both peak signal to noise ratio (PSNR) and mean square error (MSE) are given below:

\[
\text{PSNR} = 10 \log_{10} \frac{L^2}{\text{MSE}} \quad (3)
\]

\[
\text{MSE} = \frac{1}{HW} \sum_{i=1}^{H} \sum_{j=1}^{W} (P(i,j) - S(i,j))^2 \quad (4)
\]

### 4 Result and Discussions

The illustration of proposed scheme efficiency after extracting secrete image in the spatial domain of stego image and return back to the secrete image; the schemes are implemented on the natural picture as a cover image and Mona Liza portrait has been taken as a secrete image instance. The results have been compared with the corresponding base embedding and extracting methods. Table (1) presents the comparison results between PSNR and Time when the size of each cover image and secrete image have been changed.

In the proposed approach, the embedded secrete image have to be unsuspicious to human eyes and enough robust to some image processing operations. Before insertion, the secrete image color system (RGB) is converted to encrypt color image by cutting and shifting the pixels values after that the embedding operation start by inserting into the histogram of the color values is calculated to find out the high pixel values in the host image. The process is an undertaking of encoding RGB information. The actual color displayed depends on the actual RGB colorants used to display the signal. Table (1) presents the comparison results between the cover image before and after embedding and secret image before and after extraction based on PSNR, MSE and the time.
<table>
<thead>
<tr>
<th>Cover IMAGE</th>
<th>PSNR</th>
<th>MSE</th>
<th>TIME/sec</th>
<th>Secret Image Size</th>
<th>PSNR</th>
<th>MSE</th>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>38.7447</td>
<td>35</td>
<td>3</td>
<td>256 x 256</td>
<td>26.9590</td>
<td>132</td>
<td>Without Section</td>
</tr>
<tr>
<td></td>
<td>38.7447</td>
<td>35</td>
<td>3</td>
<td>256 x 256</td>
<td>26.9920</td>
<td>131</td>
<td>First Section</td>
</tr>
<tr>
<td></td>
<td>38.7447</td>
<td>35</td>
<td>3</td>
<td>256 x 256</td>
<td>26.9920</td>
<td>131</td>
<td>Second Section</td>
</tr>
<tr>
<td></td>
<td>38.7447</td>
<td>35</td>
<td>3</td>
<td>256 x 256</td>
<td>26.9920</td>
<td>131</td>
<td>Third Section</td>
</tr>
<tr>
<td></td>
<td>45.1544</td>
<td>8</td>
<td>2</td>
<td>128 x 128</td>
<td>20.9056</td>
<td>133</td>
<td>Without Section</td>
</tr>
<tr>
<td></td>
<td>45.1544</td>
<td>8</td>
<td>2</td>
<td>128 x 128</td>
<td>20.9056</td>
<td>133</td>
<td>First Section</td>
</tr>
<tr>
<td></td>
<td>45.1544</td>
<td>8</td>
<td>2</td>
<td>128 x 128</td>
<td>20.9384</td>
<td>132</td>
<td>Second Section</td>
</tr>
<tr>
<td></td>
<td>45.1544</td>
<td>8</td>
<td>2</td>
<td>128 x 128</td>
<td>20.9384</td>
<td>132</td>
<td>Third Section</td>
</tr>
<tr>
<td></td>
<td>51.1750</td>
<td>2</td>
<td>1</td>
<td>64 x 64</td>
<td>14.9178</td>
<td>132</td>
<td>Without Section</td>
</tr>
<tr>
<td></td>
<td>51.1750</td>
<td>2</td>
<td>1</td>
<td>64 x 64</td>
<td>14.9841</td>
<td>130</td>
<td>First Section</td>
</tr>
<tr>
<td></td>
<td>51.1750</td>
<td>2</td>
<td>1</td>
<td>64 x 64</td>
<td>14.9841</td>
<td>130</td>
<td>Second Section</td>
</tr>
<tr>
<td></td>
<td>51.1750</td>
<td>2</td>
<td>1</td>
<td>64 x 64</td>
<td>15.0177</td>
<td>129</td>
<td>Third Section</td>
</tr>
<tr>
<td></td>
<td>59</td>
<td>1</td>
<td>0.6</td>
<td>32 x 32</td>
<td>9.2039</td>
<td>123</td>
<td>Without Section</td>
</tr>
</tbody>
</table>
The figures 5 and 6 shows PSNR and MSE similarity between difference size of secrete images after extraction and decryption. Figure 5 is an illustration of Peak Signal to Noise Ratio (PSNR) which one is able to determine the resemblance between the various sorts of the given instances. The given pixels demonstrate that when the capacity of the embedded hidden image is increased, the PSNR value of the embedded image is almost acceptable. In order to evaluate the performance of the proposed algorithm in comparison to other algorithms, thus, the researcher just enhanced a predictable result.

![PSNR graph](image)

Figure 5 PSNR of Secret Image after extract

Figure 6 is an illustration of Mean Square Error (MSE) of a restricted image after the extractions and works satisfactorily by the pixels. The similarities and the differences of the given ranges were various according to the MSE illustration. Although MSE provided merit results in evaluating quality of certain distorted images.

![MSE graph](image)

Figure 6 MSE of Secret Image after extract

The embedded capacity used to embed information of pixels; that is, start from 256 x 256 ends to 32 x 32 is used. Table 2 show the PSNR value for a steganography image with 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>
<thead>
<tr>
<th>Size of Secrete Image</th>
<th>PSNR of cover image</th>
<th>MSE of cover image</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 x 256</td>
<td>38.7447</td>
<td>35</td>
</tr>
<tr>
<td>128 x 128</td>
<td>45.1544</td>
<td>8</td>
</tr>
<tr>
<td>64 x 64</td>
<td>51.1750</td>
<td>2</td>
</tr>
<tr>
<td>32 x 32</td>
<td>59</td>
<td>1</td>
</tr>
</tbody>
</table>

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.

Table 3 shows, the proposed algorithm is better than all compared methods.

<table>
<thead>
<tr>
<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>59</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. In Figures 7 and 8, histograms are steganography and cover images before and after embedding are depicted. As shown in this figure, no significant changes have taken place in the histogram of cover images after embedding confidential information.

Figure 7 is a histogram of a graphical representation of a tonal distribution image which was illustrated the image cover before it was taken into the process of encrypting its data to be a stego image.
Figure 8 is the illustration of a histogram stego image compare to the original one that covered previously; thus, the tonal and the synthesized image distribution noticeably differs from original histogram of the cover image.

Figure 8 Histogram of the Stego image

5 CONCLUSION
Another key thing to remember, millions of images and videos are circulating over Internet and other transmission media. Due to, the specialists must determine a method of restricting and encrypting them to be more secure and protected. To hide confidential information steganography can be effectively used. This paper presented an efficient novel approach for image steganography which provided improvements to the current available steganography algorithms which is immune to external attacks. The proposed approach focuses on the pre-processing stage such as payload encryption and embedding area selection, in addition to steganography. A comprehensive review of previous work in digital image steganography was discussed and classified into three main categories based on the embedding strategy. These three categories are: spatial domain methods, frequency domain methods and adaptive methods. Advantages and disadvantages of algorithms within each category have been highlighted in this work. Eventually, the achieved results indicated that the value of PSNR after retrieving the embedded image ranging between 38.7 to 59 depending on the size of secrete image.

6 REFERENCES


