In this chapter, we address the proposed steganography algorithm that hybrid of text and image for steganography enhancement. Describes the design of the proposed algorithm, show the detailed approaches used for embedding and extraction process. Following that, explains how the implementation of the proposed system algorithm for embedding, extracting and its relation to the proposed architecture. Lastly, summarizes made.

5.1 INTRODUCTION

Steganography enhancement of hybrid text and image for the hiding purpose, specifically on the security and robustness of the proposed system that's based on the Discrete Wavelet Transform (DWT), where focuses on how to enhance the security communication and robustness of the secret data by combining text and image of the hiding techniques approaches such as text, Ciphertext, biometric data and embedding and extracting.

The process of combining of text and image Steganography aims to utilize the application of hiding information. That implemented in real time to achieve the design objectives for the purpose of security and robustness, we decoupled the message embedding and extraction processes from the host image manipulation process. Steganography methods are usually used to accomplish the process by these methods,
the first method is embedding that used to insert the secret message into the host object and the second method is used to retrieve the inserted message.

Informally, the data flow in the steganography architectural design occurs as follows. Let divide the steganography architectural design into various steps, the first step intends to select it as a cover object and secret message. Next, the package manipulation unit determines the secret message to be used in the payload, sending in the corresponding embedding unit. After embedding, the stage object manipulation unit takes the stage object and injects it back into the suite. The extraction process is starting sending it to the corresponding extraction unit, and returns it to the stack after inspection [1, 2].

This process of combining text and image for the steganography purpose, exactly when we intend to use it on the security and robustness of the proposed system, the implementation is based on the Discrete Wavelet Transform (DWT), where focuses on embedding and extracting the secret messages such as text, Ciphertext, biometrics data to enhance the security of communication and robustness of the secret data by combining text and image of the hiding techniques approaches through image processing techniques as Discrete Wavelet Transform (DWT). The unifying models Fig.5.1 illustrate the overall view of the system.

![Fig 5.1: Hiding Secret Message scheme.](image)
Based on this observation, trying to satisfy multiple securities communication at a time is expected to greatly increase the effective and efficient of the encryption, decryption of the ciphertext, biometrics data and hiding techniques. The previous critical survey of existing approaches; we have identified several crucial attributes of a data hiding technique that may be used in guiding the design of a good security and robustness in term of search effectiveness and efficiency: encrypting, decrypting, encoding and decoding of the secret messages [3, 4].

5.2 STEPS OF THE PROPOSED APPROACH

To show the efficiency, security and robustness performance of our scheme, executive tests have taken place for the steps of the proposed system. In this section, we will discuss in detail the overall view of combining text and image as secret information of the introduced hiding data scheme. It is composed of the following processes: process of embedding secret messages such as (text, ciphertext, text, image and biometrics), detected and extract secret message processes.

Predicting the design of the combining text and image as steganography tool that Alice and Bob would be used to share their hidden messages, we considered the main requirements for the design of our proposed approach as shown in fig. 5.1. The proposed system must intercept and perform modifications of data in the form of a secret message that should be transferred to particular payload. It must host steganographic methods for a variety of applications for the purpose of security and robustness approaches. The design should be deployable in multiple ways to fulfill the desire of our proposed system.

To achieve the design objectives, we decoupled the message embedding and extraction processes of combining text and image from the packet manipulation process in the discrete wavelet transform algorithm. Steganography enhancement methods usually desire to implement in individual function, therefore we decided to implement them as individual functions, that can be linked together to perform the core of the proposed system such as choosing the secret message as text, text, image, ciphertext and biometric data, the embedding process as individual parts to perform and the extraction process as the individual part to be performed. As a result, the combining text and image steganography requires implementation of at least one pair of functions, one for embedding the message and one for extracting it.
The ultimate design goal relates to the different embedding and extraction points established in the combining text and image Steganography framework.

The process of ciphertext of a cryptographic system consists of the secret message (plaintext), encryption, ciphertext, keys, and decryption. To ensure securing messages, the essential of cryptography is used to transform the secret information and covers the message that is being communicated over a public channel. The encryption process has been achieved when the sender applies the transformation of the message or plain text to get the transformed message or the Ciphertext. Evaluating the Ciphertext must not reveal the corresponding plaintext. An important property of this transformation is that it must be decrypted, but unless a particular secret is known to get the plaintext directly from the Ciphertext. This secret is called as the key. Finally, the inverse transformation on the recipient is referred to the decryption [5, 6, 7]. The detail references of the process of cryptography discussed in chapter 2.

**5.2.1 Embedding Function process**

The block diagram of our proposed method in fig 5.1, shows how to hide the secret message such as text/ ciphertext/ text-image/ biometrics in a wavelet domain transformation steganography as the discrete wavelet transform. Wavelets described as small waves that divide data into various frequency components to transfer each component with different resolution that is matched to the scales. It was established in contrast to the problems of Fourier Transform (FT) that provide a uniform localization of time and frequency domain to extract data from the signal effectively. The main reason of using frequency domain Steganography is for analyzing signals and it is very secure, hard to detect, flexible and has different techniques for manipulation of its coefficient values [8].

The wavelet transform (WT), where \( W(a, b) \) the wavelet coefficient of the function \( f(t) \), and \( \psi(a, b) \) the products of the inner performing with collection of analysis of a time function with finite energy of wavelet \( \psi(t) \). The discrete wavelet transform is defined as follows.

\[
DWT = W(a, b) = \int_{-\infty}^{+\infty} f(t)\psi_{(a,b)}(t) dt
\]  

\[
\psi_{(a,b)}(t) = a^{-\frac{1}{2}}\psi\left(\frac{t-b}{a}\right)
\]  

We proposed the method, where the host image of a different size is transformed into wavelet coefficients using the various levels of DWT as illustrates in in Fig.5.2.
The wavelet family such as Haar-DWT [9] has been used in order to use the wavelet to transform effectively. A 2-D Haar-DWT contains of two steps, the first one used as a horizontal operation and the second used as the vertical one. Step 1: At first, test the pixels from left to right in horizontal direction. Then, calculate the operations of addition and subtraction on neighboring pixels. The sum of neighboring pixels should be Stored on the left and the variable on the right. This process should be repeated until all the rows are processed. The sum of pixels is representing the low frequency part (L) while the pixel differences denote the high frequency part of the original image (H). Step 2: text and scan the pixels from top to bottom in vertical direction. Calculate the operations of addition and subtraction on neighboring pixels and then the sum of neighboring pixels should be Stored on the top and the most varied on the bottom as illustrated in Figure 5.2. This process of operation should be repeated until all the columns are processed. Finally, we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image, adapted for the purpose of high security, good visibility, and no loss of secret message [10 - 12].

For instance, if we describe the DWT in a simple and fast transformation approaches that translates an image from the spatial domain to its frequency domain. Unlike the standard Fourier transform which represents a signal either in spatial domain or in frequency domain, DWT is able to provide a representation for both spatial and frequency interpretation. Now it becomes much more popular in some areas [13 - 15]. The Haar DWT [16 - 18] is the simplest of all wavelets and is adopted in this in most of the research because of its features as given below:
PROPOSED APPROACH

- Haar wavelets are orthogonal, symmetric and the simplest.
- The minimum support property allows arbitrary grid intervals.
- Boundary conditions are easier than other wavelet-based methods.
- Haar DWT works very well to detect the characteristics like edges and corners.

<table>
<thead>
<tr>
<th>x1</th>
<th>x2</th>
<th>x3</th>
<th>x4</th>
<th>y1</th>
<th>y2</th>
<th>y3</th>
<th>y4</th>
<th>z1</th>
<th>z2</th>
<th>z3</th>
<th>z4</th>
</tr>
</thead>
<tbody>
<tr>
<td>x5</td>
<td>x6</td>
<td>x7</td>
<td>x8</td>
<td>y5</td>
<td>y6</td>
<td>y7</td>
<td>y8</td>
<td>z5</td>
<td>z6</td>
<td>z7</td>
<td>z8</td>
</tr>
<tr>
<td>x9</td>
<td>x10</td>
<td>x11</td>
<td>x12</td>
<td>y9</td>
<td>y10</td>
<td>y11</td>
<td>y12</td>
<td>z9</td>
<td>z10</td>
<td>z11</td>
<td>z12</td>
</tr>
<tr>
<td>x13</td>
<td>x14</td>
<td>x15</td>
<td>x16</td>
<td>y13</td>
<td>y14</td>
<td>y15</td>
<td>y16</td>
<td>z13</td>
<td>z14</td>
<td>z15</td>
<td>z16</td>
</tr>
</tbody>
</table>

Original image  Calculation on Row  Calculation on Columns

\[
Y_1 = \frac{(x_1 + x_2)}{2} \quad z_1 = \frac{(y_1 + y_5)}{2}
\]
\[
Y_1 = \frac{(x_3 + x_4)}{2} \quad z_5 = \frac{(y_9 + y_{13})}{2}
\]
\[
Y_1 = \frac{(x_1 + x_2)}{2} \quad z_9 = \frac{(y_{1} + y_5)}{2}
\]
\[
Y_1 = \frac{(x_3 + x_4)}{2} \quad z_{13} = \frac{(y_9 + y_{13})}{2}
\]

Fig 5.3: An example of Haar DWT with size of 4x4

This Fig. 5.3 mentioned above is the idea of performing Haar DWT is quite simple. For instance, the original size of the input image is N x M, so when we try to filter in horizontal direction and down sampling procedure, the size of images will be reduced to (N x M / 2). And further filtering and down sampling in vertical direction, four images of size (N/2 x M/2) can be obtained. The Steps of the embedding scheme proposed [19, 20].

5.2.2 Embedding algorithm

Input: \( f \) indicates as a host image of size of \( M_1 \times M_2 \). \( W \in \{-1, 1\} \) be the text, text image, and biometrics and shared secret key.

Output: Stego Image

Processing

1. Initialize the key pseudo-random number and secret key.
2. Produce the detail coefficients of the host image \( f \) (Wavelet decomposition).
3. Generate a random key an embedding process used to produce a traversing order for visiting the two pixels.

4. If the secret message length \( \leq \) the key
Then
Embed the secret message into the details wavelet coefficients
\[
f_{k1,I}(m, n) \leq f_{k2,I}(m, n) \leq f_{k3,I}(m, n)
\]
where \( f_{k1,I}(m, n), f_{k2,I}(m, n), f_{k3,I}(m, n) \) are coefficients, \( k1 \neq k2 \neq k3 \in \{H. V. D\} \) and \( f_{k1}(m, n) \) is the \( K \)th detail image element in the level \( L \)th resolution of the host image and \( \{H. V. D\} \) represent the horizontal, vertical and detail coefficients.

5. Apply the inverse discrete wavelet transform (IDWT) at a various levels, such as L3, L2 to obtain the stego image.
This embedded steps illustrated in Fig.5.4.

---

**Fig 5.4:** Embedding and Extracting Secret message scheme (a) Embedding, (b) Extracting.
5.2.3 Extracting Function process

An extraction function process is a module in the form of a removes stenographic content embedded in cover payload. Unlike embedding functions, as implied by the definition, extraction functions do not necessarily modify the stego images when retrieving the message. On the other hand, it is also conceivable to produce extraction functions that exploited already-existing payload data to communicate a secret message, thus minimizing the amount of information actually needed for transmission.

The a hidden message can be extracted without removing the steganographic content, the key challenges when producing extraction functions differ from the ones of embedding functions. The algorithm used for extracting the hidden messages are shown below

5.2.4 Extracting algorithm:

**Input:** Host image, stego image and shared secret key.

**Output:** Secret message (hidden message) and Host image.

**Processing**

1. Apply Lth level of the product Discrete Wavelet Transform (DWT) to the stego image.
2. Find the locations by using the shared key where the secret message was embedded in each level of resolution.
3. Sort the coefficient details and estimate the secret message bit value.
4. Find the closest quantized value using the same constant Q.
5. Compute the extracting threshold for the embedding in different locations.
6. If the Secret message is extracted by various locations, then it is estimated as common bit value, else the Secret message extracted bits are restructured by the key and we obtain the secret message.

The extraction process aim is to estimate and obtain reliability of the original image for a possible distortion version of the Stego image. The extraction process can be carried out by reversing the embedding procedures that are generating the similar random permutations of each embedding subchannel as the encoding by using the same user-provided key and given the correlation coefficient between the given and extracted one to get the output as the host image and the Secret message, Fig.5.5 illustrated in extracting process.
5.2.5 Quantization process

The quantization processes determine the strength of the secret message signal embedded in the wavelet coefficient. The wavelet coefficient in the middle process such as $f_{k_2, l} (m, n)$ must be quantized to embed to secret message, the value range between $f_{k_1, l} (m, n), f_{k_3, l} (m, n)$ bins is divided into the width that using the following equation:

$$\Delta = \frac{f_{k_3, l} (m, n) - f_{k_1, l} (m, n)}{2Q - 1}$$  \hspace{1cm} (5.4)

Where $Q$ is the user-defined variable and $f_{k_2, l} (m, n)$ is quantized to the nearest value.

To enhance the embedding strength of the secret message and an attacker doesn’t determine the key and secret message where the wavelet decomposition kept secret and quantization is unknown $[21]$.

The experimental result shows the performance and the efficiency of the proposed method, where the executive tests have taken place. We perform simulation on a various images with different variable parameter size and embedded the secret message.

A Steganography algorithm can be evaluated in a number of different ways. The algorithm has been implemented in JPEG and Bitmap (color and grayscale) images. They were resized to different sizes such as 256×256 from the center of the original images. We could measure the relative complexity of the algorithm in the form of the amount of data to be embedded, and how secured the secret information should be, and how robust the algorithm.

Considering the differences between the original and hidden data are slightly smaller to the human being perception. Therefore, the differences might be mathematical or perceptual that should be obvious from the context, whether the results of authentication of image processing techniques are required for both quantitative performance measures and visual inspection.

Here we deal with various experimental evaluation methods and their results Original and stego of image data such as quality measures. It covers the experiments based on Least significant Bit (LSB), Discrete cosine transform (DCT), and Discrete wavelet transform (DWT) techniques, which is implemented on Various standard images to determine the differences between the original and hidden data $[22, 23, 24]$. 
5.2.6 Evaluation of Image Quality Measurement

In the objective measures of the Image Quality is to calculate the difference between the original and the stego image by a predefined function. These measures are widely used in the literature. The approach image quality would be given to calculate the mean values and variances of some small regions in the image, and then compare them between the original and the hidden data image. There are many objective quality measuring methods which have been developed for image quality evaluation in last two decades. They are based on numerical measures of image quality and computable distortion measures [25-26].

The quantitative of Image Quality measurement of images is commonly measured by The Mean Square Error (MSE), Peak Signal to noise ratio (PSNR), Normalized correlation (NC), and Normalized Cross–correlation. The MSE, PSNR and NC are most commonly used Objective quality measures for image quality evaluation. Because they are simple to calculate, have clear physical meanings and are mathematically convenient in the context of optimization.

The Mean Square Error (MSE) is one of the most commonly used performance measures represents the cumulative squared error between the embedded and the original image. For an image of size N x M, it can be defined as

\[
MSE = \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{j,k} - x'_{j,k})^2 \tag{5.5}
\]

Where X (n, m), X’ (n, m) are original and embedded image respectively.

Peak Signal to noise ratio (PSNR)

\[
PSNR = 10 \log_{10} \left( \frac{2^n - 1}{MSE} \right) = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \tag{5.6}
\]

It represents the cumulative squared error between the embedded and the original image.

Normalized Cross–correlation (NC)

\[
NC = \sum_{j=1}^{M} \sum_{k=1}^{N} x_{j,k} \cdot x'_{j,k} \tag{5.7}
\]

The combination of text and image for the purpose of hiding the information, in order to provide more security and to minimize the distortion of the stego image, a novel technique using the hybrid of text and image is presented in this section [27].

The main proposed combinational of text and image steganography possesses the following advantages.
• The data can be inserted into the host image is secured, so the security is increased.
• To split the image into parts makes the degree of protection double. The splitting strategy can be designed even more complicated to be unable to compose. Furthermore, to enhance the security and robustness that used to defeat the various attacks such as crops.
• The algorithm in the process of embedding and extraction of combining text and image steganography used Discrete Wavelet Transform in order to secure and robust the stego image.

5.3 SUMMARY
This chapter describes our proposed approach that combined text and image using Discrete Wavelet Transform (DWT) algorithm. This algorithm has special features such as analyzing image features, breaking down an image into the approximation, concentrated in time and space and suited to analysis of transient uses wavelets of finite energy. This chapter also describes the several method of embedding and extracting reliability models presented here and aspects related to algorithm process for security and robustness, it is concluded that the existing models and studied aspects are much more slanted towards implementation rather than design. The details of the experiments and result as per our proposed approach will be discussed in chapter 6.

References:


