Previous related enhancement techniques in the zone of combining text and image steganography are summarized in this chapter. The purpose of this chapter is not only to introduce some of the methods and techniques previously proposed for steganography, but also to understand some of the properties, general trends and limitations of these techniques approaches.

3.1 INTRODUCTION

Steganographic techniques have been proposed during the last few years for the variety of applications, LSB is called as a substitution technique in spatial domain that is one of the most used. The purposes of these techniques are used to replace the redundant amounts of a signal with a secret message; their main objective is to hide the data, even if it is a weakness against cover modification.

Now a day, the development and enhancement of new steganography techniques directed to improvements in the structure of secure and robust steganography systems. There are many different approaches in classifying steganographic systems. It is basically categorizes according to the kind of covers used for secret communication and the embedding process applied in the cover modifications. If we take attention towards the embedding process applied to the cover, it is becoming a challenging field over theses few years, since a huge amount of algorithms has been proposed on information hiding techniques. There are many recent researches focused on, embedding effectively where a proper amount of information should be embedded.
without giving any visual distortion. The efficiency of the embedding process should correctly and clearly extract the hidden messages from a media without returning to the original data, even though the media may have been modified by signal processing procedures.

We have to study several design trade-offs such as effectiveness vs. efficiency, capacity vs. correctness and quality degradation vs. robustness, etc. Besides, a good understanding of media representation, signal detection and signal processing is necessary for a designer to construct a well-rounded information hiding systems.

The main objectives of this research work is to enhance new computationally efficient and feasible techniques based on discrete wavelet transforms for a digital multimedia system of combining text and image steganography for the purposes of security and robustness approaches [1 - 3].

3.2 OVERVIEW

Information hiding is a relatively new research field. Detailed overview of previous algorithms, software and many applications for Steganography techniques can be found in [4-8]. An overview is discussing the variety of principles and mathematical ways to get the solution on information hiding [9].

The existing of a modern steganography in the field of information hiding can be shown as the main source for the novel of information hiding techniques. When they first launch the academic conference of the information hiding as an International Workshop on Information Hiding (IH), which has been conducted yearly since 1996. Another related conference is IS&T/SPIE Electronic Imaging Security, Forensics, Steganography, and Watermarking of Multimedia Contents (SPIE). In addition, two recent peer reviewed journals are IEEE Transactions on Information Forensics and Security and International Journal of Information Security. Since the proposed methods in this research work are applicable to steganography enhancement by combining text and image techniques, the overview of the enhanced techniques for steganography will be restricted to these techniques compare to discuss all the techniques of information hiding.

The information hiding techniques have three general processes to perform: a common process of generating a message to be embedded, the techniques to embed the message, and the techniques to extract the message.
A common process of generating a message to be embedded, where the data to embed is called a message, and the message length is called the payload. The message could be any digital data, counting with a unique identification for the distributed media, such as text, image, audio, data or the other way of copyright of the information. The decision of what information to embed is depending on its applications.

For security reasons, the encrypted message usually used a secret key to be shared between a sender and a receiver. The encrypted message is assumed to be a binary random sequence, and many statistical analysis in information hiding has been performed based on the assumption.

The embedding technique process is used to modifies the original cover-object in order to embed the message. The modification process can be performed in the techniques of spatial domain (identify the image by pixels) or transform domain (identified image by frequency waves such as DCT, DFT, DWT). The selection of domain in the field of steganography techniques is an important and depends on the type of application they required. For instance, the technique process for embedding in low frequency coefficients has a different result from the process of embedding in the high frequency coefficients. Because, the high frequency coefficients processes are more difficult to detect modifications especially, for the human visual system. Therefore, embedding by modifying the high frequency coefficients can achieve more imperceptible embedding rather than the ones in the low frequency coefficients.

For security reasons, the techniques for embedding process may be used as an extra security through the use of a secret key. The term cover object definition as the original medium before a message has been embedded. Meanwhile, stage object definition as the medium after the message is embedded process. The components of the stego-object are organized in a similar way of embedding processes used. This way of embedding will be achieved by performing a shared secret key. The extracted messages are different that depend on the specific applications. For instance, the verified message after extraction should be exactly similar to the original message that can evidence that the content of the stego object has not been modified since marked.

Each application of steganography enhancement by combining text and image using techniques has different requirements that depend on the objective of the application.
In general, there are four requirements for every application of steganography techniques, such as security, robustness, payload and transparency. The existing tradeoffs between those requirements, it is very challenging to design an algorithm that satisfies all of the four requirements. The tradeoffs between security and robustness have been dealt with in this research work.

The steganography technique for the Security purpose, focusing on merely detecting presence of a hidden message. Where, a third-party is supposed to know the distributions of cover objects and stego objects, and the embedding algorithms (not secret key). The Stego-objects of the cover-objects have to look like an innocent cover-object, even if they contain hidden messages. An insecure steganographic system, an adversary should not differentiate that a sender is sending an original cover-object or a stego-object. The security of steganographic systems with a cover object (C) and an object generated by an embedding algorithm (S) is quantified using relative entropy between \( P_{c} \) and \( P_{s} \). The system is called \( \epsilon \)-secure against passive adversaries if

\[
D(P_{c}\|P_{s}) = \sum_{x \in x} P_{c}(x) \log \frac{P_{c}(x)}{P_{s}(x)} \leq \epsilon
\]  

(3.1)

If \( \epsilon = 0 \), the stego system is called perfectly secure [10, 11].

The steganography technique for the robustness purpose, focusing on the requirement of the embedded message to survive against various types of attacks, such as image processing, filtering, resizing, rotation, and intended to remove the embedded message. To achieve robustness, the perceptually significant should consider placing for embedding, so that when removing the message of hidden data would be result in a significant perceptual distortion. Copyright protection application is an example that requires robustness.

The steganography technique for the payload purpose, focusing on the bits of the embedded message. The required payload ranges from a single bit to large bits of binary decision for a covert communication. Bit rate refers to the payload used to measure an embedding rate of the size of media. The steganography technique for the transparency purpose, focusing on the requirement of the embedded messages to be imperceptible. To achieve the transparency, perceptually insignificant places should be considered for embedding, which is in contrast to the robust embedding technique. It is easy to achieve transparency for a small amount to be embedded application, but the challenges arise for the huge amount to be embedded in the cover-object.
3.3 TECHNIQUES OF STEGANOGRAPHY

In this chapter, we will extend our research work to conduct grouping of combining text and image based embedded techniques. The proliferation of digital images and the redundancy of a high degree presented in a digital of an image, digital images as a cover-objects has been an interest of many researchers and increased for the purpose of steganography. Therefore, as stated earlier, we have limited our survey work for enhancement techniques by combing text and image steganography on the case of images being used as cover objects.

Now a day the materials available for the researches becomes confused, due to the fact that surveying many publications is not an easy and many approaches share common ideas, here we briefly explain the general fundamental methodologies of steganography for combining text and image approaches. These techniques In this section 3.3.1 we study the methodology and discuss an important of embedding techniques that can be categories into three main groups according to the embedding domain of the cover image: spatial domain, transform domain and model based techniques.

3.3.1 Steganography Enhancement Techniques

There have been a large number of Steganography Enhancement Techniques proposed in the literature. These techniques modify the cover images with different approaches as well as constrains. But all Steganography Enhancement Techniques share the important goal of secure, maximizing the capacity, robust and imperceptibility of the stego channel. In the most basic case the embedder operates by modifying image information like the least significant bit of the image pixels. It is limiting the modification to image block with certain variable level. In more complex Steganography techniques could use to obtain statistics, such as DCT and DWT based histogram. Alternatively, statistics could be modeled and then preserved.

Our goal is to provide a good understanding of how different approaches of steganography techniques are used to employ the redundancies in the cover object such as image for embedding a secret message. We categorize these algorithms into three categories.
3.3.1.1 Steganography Enhancement Techniques for spatial Domain

In a spatial domain the most widely known steganography algorithms are focused on modifying the embedding and noise of least significant bit layer of the image. It is known as the LSB technique that is an easy way to be given in image and audio [12, 13], that involves the manipulation of least significant bit (LSB) or Bitplane of the data and has a large impact compared to the other techniques. These common steganography approaches are easy to apply in multimedia [14, 15].

In the image perspective, the awareness of LSB techniques is to exchange the least significant bits of pixel value of secret messages. For instance, the value of a grayscale that range from 0 to 255, represented by 8 bits, as shown in figure 3.1 to embed more data into the cover-object, the least N bits are exchanged or replaced.

Fig 3.1: LSB Replace.

Least significant bits techniques, especially in an image will not identify any effect on the image. This is obvious observe by eye witnesses to various images of the same looking that

The visual appears unchanged after the LSB method is adjusted and the statistic of an image is also changing significantly. LSB manipulation software has been written for a variety of image formats and can be found in [16, 15]. These techniques typically achieve both high payload and low perceptibility and robustness; however, LSB technique has the fact that these methods are vulnerable and may be known to extract by unauthorized parties. These common tools are based on LSB Enhancement Techniques used in this group include StegoDos [1], S-Tools [17], Mandelsteg [18], EzStego [19], Hide and Seek [20], Hide4PGP [21], White Noise Storm [22], and Steganos [23]. The typical formats of steganography images used the method of lossless, so manipulation and recovery of the data can be directly used [24, 25].

We will discuss in detail some of the techniques that apply compression and encryption, providing better security of the hidden data, and statistical changes that could be used to detect stego images generated using the LSB method.

In the technique of LSB, the replacement of pixels by a secret message that to be sent.
STEGANOGRAPHY PROCESSING TECHNIQUES

The secret message bits are spread all over the image. This technique regularly uses to distribute the bits; accordingly half of the LSB’s will be modified.

For hiding information approaches. The LSB algorithm is used to change of pixels visited in a random, others used to modify the pixels in specific areas of images, [26]. Another approach for embedding the secret message in Steganography Enhancement Techniques for spatial domain [27], used as a statistically resemble for the common distortion process, for instance, scanner noise or digital camera noise, is introduced to pixels on a randomly. The distortion formed by a pseudo random noise generator through the use of a shared key. These embedding and extraction methods use to find a location and determines a sequence of locations that point to components in the cover-object.

The embedding algorithm procedures are used to modify the elements as a pixel in an image to hide the message and the extraction algorithm procedures are also used to recover the message by checking the same series of positions. The LSB enhanced techniques is involving of embedding and extracting algorithm. The LSB enhancement techniques in the process of embedding are consisting of choosing a subset of cover-elements and performing the LSB operation, which exchanges the LSB of the messages. One could also imagine an LSB operation which changes more than one bit of the cover, for instance by storing two message bits in the two least significant bits of one cover-element. The LSB enhancement techniques in the process of extraction, the stego-object is selected to extract and align to recover the secret message. The algorithm of LSB scheme obtained in 3.1 and 3.2. Where, \( l(c) \) is the length of the cover used in the embedding step, \( ci \) is the index of cover-elements, the stego-object by \( s \) which is again a sequence \( si \) of length \( l(c) \), the symbol \( j \) for such an index, \( ji \) is index of itself indexed by some set, we refer to the \( ji \)th cover-element we mean \( cji \). Stego key as \( k \), secret message as \( m \), length of \( m \) by \( l(m) \)

**Algorithm 3.1** Embedding process: least significant bit (LSB)

```plaintext
for \( i = 1, \ldots, l(c) \) do
    \( S_i \leftarrow C_i \)
end for

for \( i = 1, \ldots, l(m) \) do
    Compute index \( j_i \) where to store \( i \)th message bit
    \( s_{ji} \leftarrow c_{ji} \rightarrow m_i \)
end for
```
Algorithm 3.2 Extraction process: least significant bit (LSB)

\[
\text{for } i = 1, \ldots, l \text{ (M) do}
\]

\[
\text{Compute index } j_i \text{ where the } i \text{ th message bit is stored}
\]

\[
m_i \leftarrow \text{LSB} (C_{ij})
\]

\text{end for}

Another method used in least significant bit (LSB) steganographic such as TBPC. This method of LSB used for embedding and extraction by the determined locations of the elements pointed. It constructs a complete array tree as a master tree that represents the LSBs of the cover object. The cover object of LSBs will fill the nodes of the master tree from all directions as level by level, top to bottom and left to right. Denote the number of leaves of the master tree The TBPC embedding algorithm derives a bit binary string, called the master string, by performing a parity check on the master tree from the root to the leaves [28].

3.3.1.2 Steganography Enhancement Techniques for Transform Domain

In transform Domain steganography, where the embedding or extracting the secret message used in the spatial domain as LSB are modifying the values of image pixels directly for the embed process, but they are not robust, even if here is a slight change to the cover. An adversary can easily apply signal processing techniques to destroy the secret message entirely. In contrast to the spatial domain, these existing transform domain steganography, which modifies the frequency coefficient for information hiding after a proper transform such as the discrete wavelet transform (DWT), the discrete cosine transform (DCT) or the discrete Fourier transform (DFT).

In the early development of steganography systems, embedding a message in the method of transform domain is more robust, secure and reliable, in contrast to the embedding in time domain method.

Steganographic systems now days used to transform domain for the purpose of robustness. Thus, the transform domain methods designed to conceal the secret message in a significant part of the cover-object. This is a good way to protect the secret message made by an active adversary through various image processing techniques, such as compression, cropping… etc. However, they remain imperceptible to the human eyes. The approach of frequency or transform domain steganography are popular in literature. Discrete cosine transform (DCT) [29–31] as a vehicle to embeds information in images, where the image first divided into blocks of
a various algorithm method that are selected according to the block activity. Other schemes are based on a global image would be the use of discrete Fourier transform (DFT) [32-34] and discrete wavelet transforms (DWT), where Transformation can be applied over the entire image to be blocked throughout the image. However, a trade-off exists between the secret message added to the image and the robustness obtained.

For many methods of transform domain are used image format and may survive the transformation between lossless and lossy formats.

Here we will give an example of one of the transform domain techniques to demonstrate how the data can be concealed into the cover-object.

The Discrete Cosine Transform (DCT) of a sequence $s$ of length $N$ is defined to be

$$ S(k) = D[s] = \sum_{j=0}^{N-1} s(j) \cos \left( \frac{(2j+1)k\pi}{2N} \right) $$

$$ s(k) = D^{-1}[S] = \frac{1}{N} \sum_{j=0}^{N-1} C(j) s(j) \cos \left( \frac{(2j+1)k\pi}{2N} \right) $$

(3.2)

Where $C(u) = 1/\sqrt{2}$ if $u = 0$ and $C(u) = 1$ otherwise, the DCT has the primary advantage that $D[s]$ is a sequence of real numbers, provided that the sequence $s$ is real. In DCT of the two-dimensional in digital image processing is used as the "heart" of the most standard lossy digital image compression system used today.

$$ S(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} s(x,y) \cos \left( \frac{\pi u (2x+1)}{2N} \right) \cos \left( \frac{\pi v (2y+1)}{2N} \right) $$

$$ s(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v) S(u,v) \cos \left( \frac{\pi u (2x+1)}{2N} \right) \cos \left( \frac{\pi v (2y+1)}{2N} \right) $$

(3.3)

In the DCT of JPEG system [35, 27], the first procedures are used to convert the compressed image into the color space of YCbCr, then divide each color into $8 \times 8$ blocks of pixels. The DCT coefficients are divided in the process of quantization into some predefined quantization values and rounded to the nearest integer that can be scaled by a constant. The JPEG process is used to modify the effect of various spectral elements on the image [36]. In the decoding process, the DCT coefficients are multiplied by the quantization values for the encoding process. Then the inverse DCT is achieved to reconstruct the secret message.

The DCT general method of encoding a secret message is modulating the relative size of two of DCT coefficients within one image.
Algorithm 3.3  The encoding process of DCT-Stego

For \( i = 1 \ldots l(M) \) do

choose one cover-block \( b_i \)

\( B_i = D\{b_i\} \)

If \( m_i = 0 \) then

If \( B_i (u_1, v_1) > B_i (u_2, v_2) \) then

Swap \( B_i (u_1, v_1) \) and \( B_i (u_2, v_2) \)

end if

else

If \( B_i(u_1, v_1) < B_i(u_2, v_2) \) then

swap \( B_i(u_1, v_1) \) and \( B_i(u_2, v_2) \)

end if

adjust both values so that \(|B_i (u_1, v_1) - B_i (u_2, v_2)| > x b'_i = D^{-1}\{B_i\}\)

end for

create stego-image out of all \( b'_i \) [37].

The process of encoding for the DCT as an embedding process, the cover-image splits into 8×8 pixel blocks, each block encodes one bit of secret message. The embedding process select \( b_i \) as a pseudorandom block, \( i \)th as message bit to be coded by \( b_i \). Let \( B_i = D\{b_i\} \) be as DCT-transformed image block. \( (u_1, v_1) \) and \( (u_2, v_2) \) is the two indices of DCT coefficients, to ensures about the information that is stored in significant parts of the signal [38]. Since the constructed system should be robust against JPEG compression, the encode block of "1," if \( B_i (u_1, v_1) > B_i (u_2, v_2) \), otherwise a "0.", in the encoding process algorithm.

Algorithm 3.4 DCT- Steg decoding process

for \( i = 1, \ldots, l(M) \) do

get cover-block \( b_i \) associated with bit \( i \)

\( B_i = D\{b_i\} \)

if \( B_i (u_1, v_1) \leq B_i (u_2, v_2) \) then

\( m_i = 0 \)

else

\( m_i = 1 \)

end if

end for
The $|B_i (u_1, v_1) - B_i (u_2, v_2)| > x$ for some $x > 0$, is an algorithm that ensures by adding random values to both coefficients. The higher of $x$ is used to be more robust. Embedding and extraction algorithms are shown in Algorithms 3.1 and 3.2. The DCT coefficients of constant $x$ and location should be selected properly. This can be done by the method of JPEG for the purpose of robustness.

The disadvantage of the method mentioned above is that the Algorithm 3.3 does not reject the block of the image, then the DCT coefficients cannot be applied the desired relation without accruing damages to the image data contained in the specific block.

The related proposed method system in [39] presented about the disadvantage, which try to overcome the disadvantage of the above algorithm. The quantized DCT coefficients method has been used to be operated and store the information through the three coefficients relations in a block [33, 40].

The frequency domain steganography of Discrete Wavelet Transform (DWT) technique we will discuss more thoroughly later, especially in chapter 4 and five for the proposed method.

### 3.3.1.3 Steganography Enhancement Techniques for Model based approaches

In the previous discussion of steganography enhancement techniques, the obvious difference between spatial domain and frequency domain schemes is the convenient form of execution, these approaches can provide different functions to cope with various applications. The transform domains of steganography scheme's objective is to achieve a better balance between robustness, security and fidelity than the spatial domain schemes.

The steganography algorithms have enhanced the practice by combination of various techniques to operate the tasks to conceal a secret message into a cover-object. There are three stages make the steganography program a success, First, the redundant bits in a cover-object should be located before embedding a secret message. Second, decide which bits it should be used. Third, embed to the cover message should not be perceptible.

The model based techniques are used to model the statistical properties of an image and try to protect them in the embedding process, compared to the two previous techniques. In [33] discussed a method that separated the transforms image coefficients into two parts and replaces the perceptually unimportant element with the
coded message signal. AC DCT coefficients in the marginal statistics of quantized are modeled with a parametric density function. The non-adaptive arithmetic decoder is the cores of the embedding procedures which takes the message signal and decode it with respect to measured system prospects, which the coefficients in each histogram bin are modified with respect to embedding rules. The extraction process is the same as the embedding stage.

In another model based techniques [41] used the approach as data masking, in which the message take place and would be displayed the properties of an arbitrary cover-object. On the other hand, in order to secure a channel to achieve covertness, the preprocess is necessary for encrypted stream at the end points to remove randomness, so the stream defeats statistical tests for randomness and the stream is adjusted at the other end.

Other proposed in [42] as Invers Wiener Filtering used as a solution to remove randomness from cipher streams with images as a cover-object. The information hiding in halftone or dithered images scheme, that one bit represented in each image sample, embedded by flipping the image samples. In [43] use a variety of halftone connections to embed a secret message. It also embeds the secret message in halftone images by taking the local statistics in respect to be replaced.

In the additive spread spectrum method, that inspired by the spread-spectrum modulation technique in digital communication system. This technique affords more approaches for the purpose of security and robustness to a channel noise for digital aspects. The pseudo-random represented in additive spread spectrum method to keep a good perceptual quality since the value of each pseudo-random number is small and suitable to the data hiding application as the key is generated.

The spread spectrum can be operated in frequency and spatial domain, but a large percentage used in frequency domain for better performance [44]. They proposed that used the secret message to be placed in significant components of the content to survive common signal processing for the perceptually.

Quantization is other information hiding algorithms used to satisfy a distortion constraint and designed the reconstruction values from one quantizer that separated from the reconstructed points of every other quantized. The transmitted message is used as an index by quantizing the image data for embedding the information. In [45] use to embed a high volume of data through the method of quantization.
Another approach is used as feature extraction for the purpose of information hiding, where is used to embed the data by modifying the geometrical feature of the image that pseudo-randomly generated by a dense line pattern. Then a set of feature extraction in image is extracted [46]. The One kind of these information hiding schemes is used to embed the data without presenting any distortion to the cover-object as an image [47, 48]. The elementary idea in invertible embedding is to make the use of certain redundancy in the cover-object data. The process defined as the embedder compresses the redundant portion as the LSB of the image pixels, into a smaller size to preserve some place for the data to be hidden. The idea comes when the detector extracts the hidden data and expands the compressed redundant portion to reconstruct the original data. The similar way can also be extended to various image formats [49].

3.4 ADVANTAGES AND DISADVANTAGES OF STEGANOGRAPHY PROCESSING TECHNIQUES

3.4.1 Advantages

1. The main objective LSB technique is to hide the data. Even if it is a weakness against cover modification or vulnerable to some trivial attacks.
2. The advantages of the LSB are used to conceal the bits of a secret message directly into the cover-object in the Easy way.
3. Human-perceptible does not identify the modification of LSB due to the small changes to the cover-object.
4. The advantage of frequency domain over the spatial domain is a signal can be much more robust than embedding rules operating.
5. It can solve the problem which can be described with the embedding and encoding processes.
6. The transform domain used the techniques of compression to reduce the payload compare to the spatial domain.
7. In transform domain the sender knowing the coefficients before and after the process.
8. It solves problems with multiple solutions such as security, robustness payload and perceptibility.
9. Since the steganography embedding and extracting technique is used in various ways that can solve a multi way to hide the secret message for security purpose.

10. Steganography algorithm is a method which is very easy to understand and implement.

11. Like other security perspective techniques, the steganography algorithm can assure if the embedding algorithm is strong or secured.

12. Produce statistical distribution that is closer to the original cover-object.

3.4.2 Disadvantages:

1. The major disadvantage of LSB method is the way that can adjust the least significant bit of all the image pixels. So the hidden message will be destroyed by modifying the image quality a little bit.

2. The LSB technique is a weakness against cover modification.

3. LSB methods are vulnerable to extraction by unauthorized parties. An adversary can easily apply signal processing techniques to destroy the secret message entirely.

4. Small changes to LSB yield to total information loss of lossy compression systems.

5. The embedding capacity of the LSB is low.

6. Human being eyes are accurately very sensitive to the presence of a single bit of noise and can often detect it presents on an image file.

7. LSB coding is not very robust.

8. LSB level is limiting the modification to image block with certain variable.

9. The drawback of DCT Algorithm that does not reject the block of the image, then the DCT coefficients cannot be applied the desired relation without accruing damages to the image data contained in the specific block.

10. There is no absolute assurance that adversary can find a secret message and try to destroy it or add some harmful messages. It happens very often when the adversary identifies there is a hidden message in the innocent cover-object.
3.5 SUMMARY

The chapter gives an overview of different steganography processing techniques which have been proposed in the literature. Many flexible and simple methods exist according to the embedding domain of the cover image: spatial domain, transform domain and model based techniques has been discussed. However, covers and messages tend to have unique patterns. The simple techniques are used to be broken by the statistical properties of the channel's noise. Images and signals are used in various image processing such as quantization, filters, transformations, format converters. The general trend, advantage and disadvantages of theses technique approaches are described.

Steganography Algorithm based discrete wavelet transforms for robust and secure must be addressed when designing a steganographic system. So, these properties of algorithm which use to enhance the security and robustness will be highlighted in the next chapter.

References: