The rapidly proliferated information and the growth of digital technologies by information hiding in multimedia has enhanced the access to digital data. It enables to the reliability of the techniques and achieves the efficient storage, transferring, faster. The processing of digital forms and accomplishes to make the illegal production and redeployment of digital media easy and undetectable. Hence, it poses a novel challenge for researchers. Securing the communication of intellectual property and providing protection for digital data in distributed system have drawn a lot of attention now a day [1].

Steganography is an important branch of information hiding that falls under the umbrella of security system, which is the state of the art of safely hiding secret messages in an innocuous carrier that has a dynamic tool and the capability to adjust new advanced technology. It literally means “covered writing” as derived from Greek [2] which is described techniques such as `Least Significant Bit (LSB), Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT) used to imperceptible convey information by communicating secret messages in an appropriate multimedia carrier, such as text, image, audio, video and also at the network packet files.

The aim of security and robustness of steganography used in such a way that the third party (Warden) cannot discover and extract the existence of the hidden messages, and the secret key used as an extra security between the sender and
recipient in which is indiscernible to a detector unless the secret key is known. It can trace its origin as far back as 440 B.C. in histories written by Herodotus [2, 3].

In the modern information age, as digital media text, images, audio and video provide sufficient redundancy, security and robustness for information hiding, expanded to Internet data shared, digital signatures, Biometrics, Bioinformatics and spread spectrum communications to fulfill the desire of secret hidden communication [2, 4]. Steganography and cryptography is very alike methods to maintain the data in a confidential manner. The cryptography differs from its specific objectives, where the content of a secret message is unintelligible to eavesdroppers and studies how to protect the content of messages. However, in Steganography, the very existence of such a message is camouflaged and study methods to make messages imperceptible by concealing a secret message within harmless messages [5].

On the other hand, Biometric-based system [6, 7], are becoming very popular because of their ability to identify and verify the physiological or behavioral characteristics of personality and differentiate between a legitimate user and an unlawful user. The embedded steganography in a biometric data gives another way to protect the biometrics data against illegal utilization. Meanwhile, it should be as a means to eliminate some of the attacks to a biometric system.

Watermarking, as opposed to Steganography, another sub-discipline in information hiding, which attempt to hide copyright messages into a medium with a high level of robustness to against possible attacks, thus watermark enables the identification of copyright violation or an accumulation of evidence for prosecution. It is always associated with its own while steganographic systems just hide any information. Steganographic communications are usually point-to-point while watermarking techniques are usually one-to-many [2, 8, 9].

Finally, the goal of steganography is to conceal messages in a digital form within a cover-object, especially with an innocent cover-object such as a common image, in such a way that the third party does not even suspect or identify there is a hidden message exists within the innocent cover-object.
1.1. **THE PROBLEM INVESTIGATION**

This study is focused on the enhancement of steganography techniques by combining text and image through the major factor of steganographic algorithm methods such as security and robustness. It is based on steganography transform domain technique such as Discrete Wavelet Transform (DWT) which meets the requirement of imperceptivity, security and robustness.

There are three major factors to consider when designing any steganographic algorithm. These factors are the “capacity, security and robustness” [10]. The embedding and extracting strategies are most of the existing methods of steganography where no consideration of the preprocessing steps, such as encryption and robustness. They depend on the encryption algorithms which obviously can be applied to the robustness and security that required for steganography. Besides, most of the research on enhancement of steganographic methods of combining text and image through a various techniques in spatial domain based steganography such as Least Significant Bit (LSB) and transform domain based steganography such as Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT) [11]. These techniques are arguing that the strength of the combined system relies on the cumbersome computation and the length of the key or the difficulty of the reverse computation of a one way function of the hidden data.

We limited our research work to steganography technique system for combining text and image data in frequency or transform domain, such as Discrete Wavelet Transformation (DWT). However, DWT is preferred because; it provides both simultaneous spatial localization and frequency spread of the secret message within the host object and fulfills both security and robustness. The techniques and limitations of the existing method will be described in detail in chapter three.

The challenge arises when steganography applications become in demand for many government and private organizations, especially when it comes to the term of security and robustness of the secret data. These challenges will be described in chapter five for designing the proposed system.

The performance of essential measurement of the existing methods is implemented to compare, develop and determine specific algorithms for the technique of Discrete Wavelet Transformation (DWT) with other techniques as Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) in appropriate uses methodology for steganography to promote security and robustness approaches.
1.2. MOTIVATION AND OBJECTIVE

We address a modern digital steganography that have many different ways to hide information that involves digital media and techniques: images formatted, written text, text image and biometric data. The methods of steganographic evolution system for security and robustness have received a lot of particular attention [12, 13]. Focusing on the limitation of security and robustness of the information hiding in the existence of the message is noticeable and has motivated us. This is the foundation of various factors of steganography of new techniques that exploit contemporary technology in addition to metrics to measure their performance needs to develop [14].

The challenge lies in providing the best solution for robustness against attacks, increasing the difficulty of destroying a Stego image from an image and providing a high visual quality of the Stego image. The problem of text and image steganography has been addressed using a number of different techniques, such techniques as spatial and transform domain that categories according to the embedding domain of the cover image “spatial and transform” domain methods. The spatial domain methods are the easiest and simplest steganography techniques. However, they have a low information hiding capacity, and the hidden data can be easily erased by image compression. The transform domain approaches [15] On the other hand, insert the hidden data into the transform coefficients of the image cover, embedding more information and yielding more robustness. Most of the combinations of text and image steganography methods use one transform to embed the data. Usually these methods have either good robustness against attacks or good security. This method of combining text and image has motivated our research through the need for more robustness better security of visual imperceptibility steganography.

Objective of the Proposed:

- To study a methodology for steganographic data hiding.
- To study and develop the efficient Steganography techniques using transform domain approaches.
- To develop a novel of combining Text and image steganography to find a solution for enhanced security (High Security) and to ensure the robustness of a high volume of data that can be hidden reliably in images (Robustness).
- To compare effectiveness of steganography techniques.
- To design and develop the steganography system should be enhance.
The performance of embedding and extracting algorithm has been assessed and analyzed. The proposed algorithm is developed to enhance the techniques for the both issues security and robustness. The efficiency of steganography algorithms is compared and achieved with other wavelet domain algorithms. Since the main novelty of our approach resides in the way the DWT are exploited to hide the secret message where we tested on the various mixed images.

This research work presents a system that develops intelligent steganography algorithm to improve the system performance of combining text and image for more robustness better security of steganography techniques.

1.3. SIGNIFICANCE OF STUDY

The steganography in every few years has to enhance and re-invent itself by new technologies and new applications in the acclaimed research area. Due to the growth of the steganography applications in the World Wide Web has also made the government intelligence, police agencies and private sectors anxious. Therefore, the common reaction is to try to develop techniques to restrict the strength. This application of steganography enhancement schemes of combining text and image has brought new threats, and focus us to invent new protection mechanisms and also received attention from the research community.

In this work the combination of text and image steganography algorithms has been implemented in the various formats such as JPEG, Bitmap in the color and gray scale images with various types of contents Images. They were resized to $512 \times 512$ from the center of the original images. The experimental work of steganography enhancement was performed by embedding and extracting methods. The unnoticeable visual difference after embedding is a good indicator of the proposed method. We used various types of secret messages to be concealed into the host images like text, ciphertext, text image, and biometrics. Several kinds of distortion including unintentional attacks such as JPEG compression, filtering, and noising as well as intentional attacks such as cropping, rotation were performed on the stego images.

For the performance of the proposed method, we have focused on the security, invisibility and the robustness. We tested the performance of the present algorithms such as LSB, DCT and DWT on these standard images with various quality measurements like MSE, PSNR and NC.
1.4. **RESEARCH CONTRIBUTIONS**

In this research, we focus on the important issues of information hiding that related to the enhancement of steganography techniques by combining text and image for both security and robustness aspects. The following list specifies the main contributions of this work:

1. The Scientific issues in the scope of digital Steganography (Combining text and image) surveyed and systematically summarized [16].
2. An extended of digital steganography is presented in order to clarify the advantages of the proposed method over the other existing methods. [17, 18].
3. The existing related combining text and image steganography approaches are classified [19].
4. A novel of combining text and application-friendly approaches to digital steganography is proposed [20].
5. Several methods for the steganography extensions providing applicability such as embedded and extract with the basic algorithm, as LSB, DCT and DWT [21-23].
6. The algorithms of embedding and extracting also work well in Discrete Wavelet Transform (DWT) technique, which are widely proposed and used [24].
7. Both security and robustness and performance aspects of the proposed approaches are analyzed to survive against various geometrical attacks [25-27].
8. Experimental results are generated for a number of text and image sequences to demonstrate the performance of the proposed methods.
9. A novel type of digital steganography base on the combination of text and image through the techniques of Discrete Wavelet Transform (DWT) to consider security, impeccability and robustness of the proposed system.

1.5. **ORGANIZATION OF THE THESIS**

The content of the thesis is organized in seven chapters as follows. In Chapter 2, we serve to review some basic theory of information hiding (steganography) that is necessary for a better understanding of this work, including watermarking, cryptography, biometrics hiding, steganalysis and state-of-the-art of combined text and image steganography and outline of the thesis. The references selected which are used to compose this chapter and the list of related publications had been given. In chapter 3, some important related work describes the steganography processing techniques. In chapter 4, introduces a novel description about study area and data
details of steganography algorithms based on discrete wavelet transform for robustness and security Steganography. In Chapter 5, we describe the design of the proposed technique. This chapter also describes the details of our proposed system of combining text and image steganography approach. The core work of this dissertation is presented in chapter 6, where a novel combination of text and image algorithm are proposed and analyzed in terms of security and robustness, as well as a novel type of digital image processing of steganography where a given data hidden is disguised with other data. In Chapter 7, holds the conclusions and discusses some potential future directions regarding the presented work. Finally, graphs of the experimental results and glossaries are placed in the appendix of this dissertation.

References:


19. J.C.Judge,“Steganography:past,present,future,”SANSInstitutepublication


