CHAPTER I
INTRODUCTION

1.1 Background

Maintaining privacy in personal communications is something everyone wants, so information and data security is one of the important factorize in communication technology. The over whelming advances in digital data-sharing methods have brought tremendous potential to both security and protect confidential data from unauthorized acceptance. Accordingly, the development of security systems are critical to ensuring data security while moving through the Internet. There are many fields of security technology that deal with protecting confidential data. The most important of these techniques are encryption and information hiding[1].

Then combine cryptography and steganography in one system with the aim increase security and that all the information (message) inserted into the media images could not be opened easily by unauthorized persons. The cryptography converts messages and information confidential to a shape that cannot be read unless by using a secret key, then the information is retrieved by the same key. The form of encrypted message (untidily) raises doubts for revealing their content, which attract the hackers to tamper the message that they could not decrypt, While The steganography is about inputting the information into media files where it is neither observed nor detected and its existence cannot be recognized, but it look as ordinary files where the overall form of the carrier file is maintain[2].In steganography was used method least signification BITS (LSB) technique, because it is easy, simple and uncomplicated method for embedding, in which pixel values are processed directly and produce a slight change in the coat data that cannot be perceived by the human senses and the drawback of this algorithm is that if you use an 8 bit pixel example, LSB can drastically change the main elements. the colour of the pixel. This can show a marked difference from the cover image to the stego image, so that it indicates the state of the steganography.

Research conducted [3]indicates that a new system for document images has been proposed for hide signature based on Beta Elliptic modeling, with the aim of

hide the Beta Elliptic signature as secret data in the host document image. The method is subdivided into two main blocks: embedding steganography and extraction steganography. To identify the embedding positions in the host document image, the Binary Robust Invariant Scalable Keypoints (BRISK) detector is applied. By pre-possessing the signature, the Beta Elliptic signature is transformed into a series of hidden bits. Binary Transformation and Huffman Compression are comprised of the pre-possessing. The sequence obtained is added in the first less significant bit (LSB) to the embed positions in the host document image. The experimental results achieved on three types of standards, L3iDocCopies, Tobacco800, and standard grayscale test images indicated that we outperformed related business solutions in terms of human Visual System (HSV), Peak signal-to-noise ratio (PSNR), and Structural Similarity Index Matrix(SSIM).

In the development of information technology, one of the main ideas is security. Some things that must be met when the message is sent to the recipient are confidentiality, integrity, availability, authenticity, and nonrepudiation. These five computer security concepts protect messages sent to the receiver by sending the messages delivered safely without less than one bit of data. Confidentiality is a term used to prevent access to information by an individual or an unauthorized system. Integrity in terms of information security means data couled not be modified without being detected.

1.2 Research Problems

The problem: with the improvement of correspondence today, everyone would wish to send information or an email without fear that an illicit person will read the message. Whereas each person must be protected themselves from undesirable spying, duplicating and robbery. Where main constraint of today is for computer communication is protecting data, especially when it comes to various secret data such as sensitive documents or files, military maps etc. Which is reason in endeavour to find ways to keep data confidential, safe and not share it with others.

Steganography has advantages in the aspect of hiding messages where the hidden message is not visible in the form of certain codes such as cryptography,

because in steganography the message is entrust to a cover image. The problem is how so that the message can be deposited on the cover image without seeing a decrease in the quality of the cover image, and what methods are appropriate so that the message that is deposited does not reduce the quality of the cover image. The next problem is how to design a Graphical User Interface (GUI) that is easy to use by a user even with steganography, the GUI must be able to display images, sent text, extracted text and display three menus and one execution button, namely open image, create. Encode image, save image and get massage.

Therefore, to overcome the problems, the research questions as follows:

1. When integrate the two technologies into one system, is that will provide the necessary security?
2. Will the inclusion of a secret message deteriorate the quality of the carrier's image?

1.3 Scope of Research

This thesis is committed in terms of objective coverage of the subject by the proposed system and is to take advantage of modern techniques of encryption and Steganography. Where the scope of the research are involving of encryption algorithm using substitution cipher and RSAtechnique, whereas Steganography using LSB technique. Will be used an image like cover in this search, where you can hide a large amount of data in the image.

1.4 Objectives and Benefits.

For the sake send and retrieve a confidential image safely on the Internet and to certain that no third party will note that the secret image exists. Then propose a hybrid data security technique by integrating encryption algorithms and steganography.

1. The main objective in this thesis is to provide resistance against visual attacks.
2. Enhance the security of the data for secure data transmission over an open channel, with no detectability.

3. Give a higher degree of protection to confidential data and to avoid raising arouse suspicion about the transmission of secret message and to achieve privacy.

The benefits

1. Reducing piracy, reducing the chances of attacking confidential data.
2. No access to confidential data, only the persons concerned can read the confidential data.
3. The data arrival the other party without change.

1.5 Originality of The Research

With great technological progress, the development of various means of communication, and the world's reliance on sending different types of data through networks. We need to keep information secure more than ever. The paper[2]presented a method based on the use of both encryption and steganography whereby the secret image is divided into two parts, and each part is hidden in a different image cover. After that, the resulting stego images are encrypted. It is true that the capacity in this way is high, but sending encrypted images bring the attention of the hacker. The table (1, 1) shows some related research. In this research, the proposed system uses both steganography using LSB and cryptography using substitution cipher and RSA. To provide a double layer of security, with keeping on the main function of each. Steganography hides message in some other digital media. Cryptography, furthermore, obscures the content of the message. Where the public key using in both technologies. All this to improve data security.

TABLE 1.1 RELATED RESEARCH

No	Name	Title	Conclusion
1	Zenati et al (2020)[3]	SSDIS-BEM: A New Signature Steganography Document Image System based on Beta	The experimental results achieved on three forms of benchmarks, l3idoccopies, Tobacco800, and regular grayscale test photos, showed

		Elliptic Modeling	that in terms of Structural Similarity Index Matrix (SSIM), Peak Signal to Noise Ratio (PSNR), and Human Visual System (HSV), we have outperformed related work solutions.
2	Rashid et al (2016)[4]	Analysis of Steganography Techniques using Least Significant Bit in Grayscale Images and its Extension to Colour Images	The sequential Least Significant Bit (LSB) method of substitution for any possible pixel position is studied in this paper. Image quality is computed by the statistical tests. Demonstrate these measurements that the message replaced in the eighth bit (least bit) has the least visual and statistical impact on the quality of the image.
3	Hutapea (2018)[5]	Watermarking Method Of Remote Sensing Data Using Steganography Technique Based On Least Significant Bit Hiding	The Mean Squared Error value of stego images is less than 0.053 for all three data compared to the original image. Visually, the result of the encoded image is similar to the original. This means that in remote sensing satellite images, information can be protected with steganography techniques using the LSB algorithm.
4	Malathi and Gireeshkumar (2016)[6]	Relating the embedding efficiency of LSB Steganography	Combined with the F5 algorithm and matrix embedding, the LSB method is applied to an image's

		techniques in Spatial and Transform domains	spatial and frequency domains. As a performance metric, Peak Signal to Noise Ratio (PSNR) and the Mean Squared Error (MSE) were used to compare the various LSB techniques. This paper shows that MSE and PSNR provide better results for LSB techniques with Matrix embedding.
5	Younus and Hussain (2019)[7]	Image steganography using exploiting modification direction for compressed encrypted data	With respect to imperceptibility by PSNR of 55.71 dB, the payload of 52,400 bytes and the robustness, the empirical results indicate that the proposed scheme is more effective compared to the old steganography schemes.

1.6 Structure of Research

Chapter1 (Introduction): this chapter contains the clarification about General introduction around the thesis, the existing problem statement, Limitations, objectives, significance.

Chapter2 (Literature Review): background about cryptography and Steganography and a detailed explanation of the literature review.

Chapter3 (Methodology): will be explain on the selected techniques and algorithm that has been used in the research.

Chapter4 (Results): this chapter explains the implementing and results of the experiential work.

Chapter5 (Conclusion): this chapter summaries conclusion about proposed paradigm.