CHAPTER I
INTRODUCTION

This chapter presents the background of the study; including the rationale, theoretical framework, conceptual framework, the problem, hypothesis, assumption, scope and limitation and the importance of the study.

1.1. Rationale

Nowadays the need for information security becomes so inevitable due to the rapid applications development on computer network and internet technology. There are specific informations need to be secured since they are valuable resources [3]. Security consists of some policies, rules, protocols and standards that help the organization to meet its objectives. Organizations need security to protect their assets from illegal and unauthorized access, also people in their personal life need to keep their private documents, family albums, and also confidential films. Physical security and access control are the solution but they are not enough to secure the data. Electronic data are still easy to access, steal or copy via networks. Therefore security system and methods are needed to keep them safe and secure [4].

Digital images are attractive data types with widespread range of use. There are many researchers who are interesting to protect the content against previewing, manipulation and copying. In many applications such as military image databases, confidential and top secret video conferencing, medical imaging system, cable tv, and online personal photograph album, security is significant and essential. The wide application of images in industrial process turns it into a resource and asset, so it is important to protect the confidential/top secret image data from unauthorized access. Most of today encryption algorithms are based on textual data, but images are different from text [4]. An idea for image encryption is to consider a 2D image as a 1D data stream and encrypt this stream with any textual based cryptosystem [3][4] and VEA. This approach is usually suitable for text, and sometimes for a small bit rate audio, image and video files that are being sent over a fast dedicated channel [7].

One method for securing it is by using mosaicing. However, it is hard to recover the image perfectly. For overcoming this problem cryptosystem may be used. However, since the size of image is greater than text, then for encrypting image, more time is needed compared to text.

1.2. Theoretical Framework

This research proposes new approaches to modify the method for obtaining secure mosaic with more secure and robust. The improvement of this study combined with soft encryption (also known as selective bitplane) can also reduce the time computation regardless of the boundary of input in the previous research [8].

The idea of the proposed method for mosaicing is applying cryptography instead of blurring method and minimizing the area of the mosaic using image processing. For reducing the time and memory needed by the process, the combination of selective bitplane [1] based cryptosystem and AES [3] is introduced. To achieve stronger security, the mosaic has also message on it embedded using method Modified Dynamic Cell Spreading [13]

For investigating the visibility of the proposed method proposed method compared to blurred images, investigating by people is conducted as well as for investigating the invisibility of the embeded image.

1.3. Conceptual Framework/Paradigm

This study introduces new method proposed to achieve the optimal objectives. There are several processes to be conducted, they are the image preprocessing, encrypting with soft encryption, embedding the message into mosaic. There are some parameters analysed related to the previous studies for securing the information. Those parameters and criterions are

a. Data source,
b. Image processing; including: cropping image, edge detection, selecting area the most needed.
c. Cryptography; including: generating plaintext, key generating, encrypting selective bitplane.
d. Steganography; including: random number generating, bit stream generating, and embedding the message.
e. Performance of cryptography; including: memory usage and time computation.
f. Performance of robustness of the steganography; including the values result of MSE, PSNR for the theoretically objective criterion, and the invisibility between the mosaic and stego-mosaic for the subjective one.

1.4. The Problem

The problem identified is that recently the mosaic until this time can be carried out by blurring the signal on the image such as lowering the probability to recover the original one. In order to overcome the problem, recently cryptography is introduced as a method for mosaicing. One method for mosaicing image using cryptography is conducted in [12]. But, this method still has drawback because it needs large computation.

1.5. Objectives and Hypothesis

Due to those problems, then this objective of this research is for decreasing the computation while maintaining the strength of mosaicing process.Thus, the mosaic can be read only by the authorized party.

The hypothesis for securing a mosaic with minimum computation is implemented using cryptosaic. Cryptosaic is a method for generating a mosaic by encrypting the object which will be procesessed by applying selective bitplane encryption which is frequently called as Soft Encryption (SE) [1]. This method is used to reduce the encryption computation because by applying SE it is not necessary to encrypt the whole pixels. Morover, for decreasing computation, it is conducted process edge detection based on cropping method.

For strengthening the security level in implementing SE, AES [3] is used instead of RC4 in [12]. AES is stronger than RC4 and this has been discussed in [14].

Furthermore, the key seed for decrypting ciphertext will be inserted into the mosaic.

1.6. Assumption

The assumption proposed in this study is that no problem occurs during the process (such as interrupted running time).

1.7. Scope and delimitation

This thesis discusses the implementation of the cryptosaic algorithm and the scope this study are:

a. The format image to encrypt is in JPG and to embed is in Bitmap.
b. There are three categories of images as input to process.
c. The time performance of processing image will not be considered.
d. The image size is 500x313 pixels.
e. The cropped image is in large (50..100) x (50..100) pixels, with addition 10 pixel.
f. The key length is 128 bit.

1.8. The importance of the study

This research can be used for securing confidential information (such as military and health infomation), since it proposes a method for securing data partially with less computation while maintaining the security strength.