CHAPTER ONE
INTRODUCTION

1.1 Introduction

As digital information and data are transferred over the internet and securing sensitive messages need to discover and developed more often than ever before, new technologies for protecting and securing the sensitive messages needs to realize and develop. Because cryptography and steganography methods always exposed to attacks by cryptanalysis and steganalysis respectively, so we constantly need to develop and look for new modes. Cryptography and Steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way, which hides the existence of communication [1]. On the other hand, cryptography is the enciphering and deciphering of data and information with a secret code so it cannot be understood [2].

The Steganography hides the message so it cannot seen. However, cryptography systems can be broadly classified into symmetric-key systems that use a single key, both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message, for instance, might provoke. Suspicion on the part of the recipient while an invisible message created with steganographic methods will not. However, steganography can be useful when the use of cryptography is illegal. Where cryptography and strong encryption are barred, steganography can avoid such policies to pass the message secretly.

However, steganography and cryptography differ in the way they are judged. Cryptography fails when the “enemy” is able to access the content of the cipher message, while steganography fails when the “enemy” detects that there is a secret message present in the steganographic medium.

When storing, transmitting, or merely using information, there is an increasing necessity to sustain **its security** and **integrity** and guard it against the unauthorized access. Security of data requires protecting data from access, modification, sharing or even viewing by unauthorized users, allowing only authorized users for such access. Sharing and receiving images on the network is increasing in large numbers. The security of the network is a major concern as the number of information that is being interchanged is increasing day by day. Therefore data security has gained more attention recently due to the rise in cyber espionage, and the massive increase in data transfer rate over the internet which resulted in more documents being exchanged in digital form, thus cryptography and steganography is chosen to enhance better security of information. Data is valuable, only, when it is correct and accurate. Data integrity is one step of data security, which also includes data confidentiality and availability. Data integrity means data correctness and accuracy,

which are based on the ability to prevent and/or detect unauthorized modification. Data integrity can be compromised in several ways. Each time data is replicated or transferred, it should remain unaltered. Maintaining data security is important for several reasons, it ensures recoverability and searchability, traceability and connectivity.

Cryptography approach for security of mystery information, where the information will be changed over into an in good spirits is one of the most secure cryptographic techniques, which will be then put off the beaten path into a picture. Scrambled mystery ciphertext encrypted with the Advance Encryption Standard algorithm which is composes of a series of fixed steps that should be followed to encrypt and decrypt the original message by the sender and the receiver respectively. The original message is called a plaintext, and the encrypted form is a cipher text (Nechvatal, Barker et al. 2000). The cipher text contains all of the original information of the plaintext. However, in an unreadable form, only the desired receiver can extract it by using a suitable secret key for decryption. The input of the AES algorithm consists of 128 bits (16 bytes) sequence. [3 Information is hided into a picture utilizing PVD steganography. So as to empower substantial measure of room of information and supporting great seeing nature of the spread picture, implanting is sent in name for by adjusting the subtle elements coefficients in roll out incredible improvement lands ruled over of Pixel Value Differencing (PVD). The thought of Double-Stegging is utilized and to alter the information into the picture with enhanced secrecy.

1.2 Statement of problems

Exchange of Information is one of the most challenging problems in today's technological world. In the transmission of secret data over the public network (Internet), a few cases reported that some privacy and important data has been stolen and altered from unauthorized or unintended parties. Data integrity and data security breaches have become a serious issue that requires urgent attention.

This project will focus in enhancing security by using the combination of cryptograpic technique Advanced encryption standard(AES) and steganographic technique pixel value different (PVD); prevent data to be unchanged during exchange of information.

1.3 Aim and objectives

The aim of this project is to secure and protect data using cryptographic technique Advanced Encryption Standard (AES) and steganographic technique Pixel Value Different

(PVD) and also to prevent message to be altered during the exchange of information from sender to receiver. This project will focus on the below objectives

i. Design two staging security system authentication to information integrity

ii. Implement the system in i using cryptographic (AES) and steganographic (PVD) technique

iii. To evaluate the performance of the developed system

1.4 Significant of the study

The significant of this study observed the weakness of the traditional network security solutions is that they lack a quantitative low embedding capacity and weak crytographics framework, to end this, utilization of cryptography and steganography technique will be administered in this projects to improved the security of information exchange. The system developed will focus on the the double staging protection algorithm of steganography and cryptography

1.5 Scope of the study

This project is limited to improve data hiding using pixel value different (PVD) steganography technique and data encryption using advanced encryption standard (AES) to prevent data integrity and security.

CHAPTER TWO

LITERATURE REVIEW

CHAPTER THREE

PROJECT METHODOLOGY

REFERENCES

[1] Rajyaguru, M. H., Combination of Cryptography and Steganography With Rapidly Changing Keys,International Journal of Emerging Technology and Advanced Engineering, Vol.2, No.10, 2012, pp 329-332.

[2] Manoj, I. V. S., Cryptography and Steganography. International Journal of Computer Applications (0975–8887), Vol.1, No.12, 2010,pp 63-68

[3] Chandra M. Kota and Cherif Aissi1, "Implementation o the RSA algorithm and its cryptanalysis", ASEE of Southwest Annual Conference on 2002, Houston, USA.