ABSTRACT

Cyber crime has become a dangerous threat to all the technical users and layman. Due to lack of skill on using the secured means in the data communication, many users as well as organizations are suffering. As we know that India is moving a step ahead in technical aspects, which is enhancing and improving the concept “Digital India”, but we must intensify the concept to “Secure Digital India” where we can see no data breaches, no malicious attacks and no cyber terrorism. Security in transmission through the public channels, storage of digital images has its importance in today's image communications and confidential video conferencing. Because of expanding use in sharing the images in the daily social life, it is essential to protect the confidential image data from unauthorized access. Advanced Encryption Standard (AES), a block cipher based algorithm is a well famous methodology making several advantages in data encryption. We are doing a hybrid approach for image security that combines both encryption of the image data and hiding the encrypted data into another image through steganography. The research helps layman to share the images into the public channels without getting compromised.

KEYWORDS : Cryptography, Steganography, Encryption, Decryption, AES, LSB, Hiding-Extracting, Cyber security, Image security, Cyber threats.

LIST OF FIGURES

TABLE OF CONTENTS

1. INTRODUCTION

Cyber Security is the body of technologies, whose processes and practices are drafted to protect networks. Apart from detecting the already existing threat, it also uses the intrusion prevention methods, in order to avert the upcoming threats.

In order to avert threat, virus or any unauthorized access into a network or a computer, we need to safeguard the network with a firewall and awareness of hacking. It is important to avert security breach which can cause diminution for an organization. Potential threats like loss, modification, unauthorized access, data leak must be prevented.

1.1 Cryptography

To corroborate the confidentiality, integrity and availability of information, it is vital to secure the information. One pivotal branch of information security is cryptography, the science of securing the data. Cryptography permits the original data to be converted into cipher data that can be sent over the unsecure channel. Fig.1. shows the representational diagram of the steps followed by sender and receiver using cryptography. Encryption is the procedure of transforming the native data into cryptographic data so that only intended recipient can decipher the data by applying decryption.

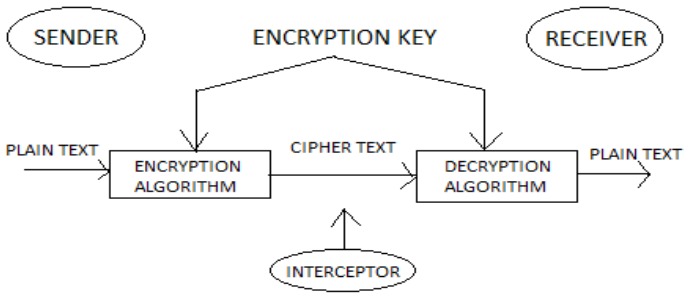

Fig. 1.1 Cryptography (Ref-2)

1.1.1 Symmetric / Secret Key Cryptography

The strategy of Secret key (same to sender and receiver) encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all side's encryption and decryption secret data. The original information or plaintext is encrypted with a key by the sender side also, the same key is used by the receiver to decrypt the encrypted data to obtain the plaintext. the key will be known only by the people who are legitimize to the modules of encryption/decryption. However, the technique pledges the good security for transmission but there is a difficulty with the distribution of the key. if one nab or explore the key he can get whole data without any difficulty. An example of Symmetric Key cryptography methodology is DES Algorithm.

1.1.2 Asymmetric / Public Key Cryptography

We can call this system as the asymmetric cryptosystem or public key cryptosystem, this uses two keys which are mathematically associated, use separately for encrypting and decrypting the knowledge. During this technique, once we use the private key, there are not any possibilities to get the info or just discover the opposite key, all keys are needed for the technique to run. The key used for encryption is stored public, ergo it’s called public key, and therefore the decryption key's stored secret and called private key. An example of Asymmetric-Key Algorithms is RSA.

1.2 Steganography

Steganography is the branch of information security that enables the information hiding. It is the art and science of hiding the data within a cover in order to avoid disruption, modification and disclosure etc. Steganography differs from cryptography in the sense that it keeps the existence of information secret while cryptography keeps contents of information secret. Fig.2. describes the steganography process. Embedding is the process

Also, it will be a powerful mechanism which enables people to communicate without interferes of eavesdroppers even knowing there is a style of communication in the first place.

1.5 Motivation for the work

As technology expanded, users started migrating information into digital form. It is difficult to secure these digital data from hackers while sending or receiving files from another person over the internet. So we need some secure method to communicate that's the main reason for developing this tool. This proposed tool will eliminates user effort of using different tools.

Cyber Threats

The below listed cyber threats have been mainly used to compromise the image data that is been sent in the public medium. The increase in the number of attacks lack of security in image security has motivated us to do research on this domain.

♦ Keylogging: Also familiar as Keystroke logging. It is the method when a attacker records the key-storks while the victim is unaware of it. It can be done via malicious application which is specifically coded for these purposes. This is a kind of spyware, where attacker spies to collect the keystrokes of Usernames and Passwords.

♦ Sniffing : Monitoring and capturing the packets passing through a network and analyzing it. It is also called WireTapping. Sniffing is important to study the packets. To secure ourselves, we must use encrypted network and SSL is recommended (Secure Socket Layer) in the web address. Email Traffic, FTP passwords, Web Traffics, Chat sessions, Cookies, DNS traffic etc can be sniffed. Sniffing can help attackers to perform ARP Poisoning, Spoofing Attacks, DHCP Attacks, etc.
Some of the most popular Sniffing tools are WireShark, SmartSniff [4].

♦ MITM: “Man In The Middle Attack” is an attack in which attacker enters the field of communication by sniffing and spoofing methodology and secretly relays and alters the communication between two parties who believe that they are directly communicating to each other. The elemental strategy is to disconnect the single connection between server and client, alter between both the networks and use the cookies and other info to harm. In order to safeguard from MITM, end-to-end encryption, SSL etc. are introduced.

1.6 Problem Statement

The aim of the project is to ensure image security by first encrypting the target image with an modified version of AES algorithm and then using steganography to hide the encrypted image in a bigger image, which is then sent to the destination.

1.7 Organization of the thesis

The introduction gives a brief about the work domain and the basic knowledge on the project. The next chapters are explained as below -

Chapter 2, Literature survey gives the usage algorithms and the methods that are been used in the system. Along with the existing methods of Encryption and Steganography.

Chapter 3, Methodology provides the system architecture and the module division of the system with the explanantion of each module in brief.

Chapter 4, Design of the project produces the structure chart and other UML diagrams of the project.

Chapter 5, Experimental analysis produces the results that are obtained in the system for various inputs. Along with the software and hardware requirements. The sample code of the system is also present in this chapter.

Chapter 6, Conclusion is given in justification to the work done in the project that is accomplished by the system with a future work note.

2. LITERATURE SURVEY

The significance of network security is increased day by day as the size of data being transferred across the Internet. This issue pushes the researchers to do many studies to increase the ability to solve security issues. A solution for this issue is using the advantage of cryptography and steganography combined in one system. many studies propose methods to combine cryptography with steganography systems in one system. these methods were deceased in previous surveys available on the topic. This survey was published in 2014, it aims to give an overview of the method proposed to combine cryptography with steganography systems. In this survey, the authors introduced 12 methods which are combined steganography and cryptography and made a comparative analysis. This comparative has been implemented on the basis of the requirements of security i.e. authentication, confidentiality, and robustness. Another survey was published in 2014, this survey presented many steganographic techniques combined with cryptography, AES Algorithm, Alteration Component, Random Key Generation, Distortion Process, Key Based Security Algorithm.

There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for the security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together.

2.1 AES Algorithm

Advanced Encryption Standard is a symmetric block cipher encryption algorithm that uses a single key to encrypt the data.

Encryption Process