Network Security Using StegoCrypt

Rudra J. Vivarekar
BE Computer
SSBT's COET Bambhori
Jalgaon, India

Yogita G. Motiramani
BE Computer
SSBT's COET Bambhori
Jalgaon, India

Nikita J. Kolhe
BE Computer
SSBT's COET Bambhori
Jalgaon, India

Darshana A. Mundada
BE Computer
SSBT's COET Bambhori
Jalgaon, India

***Abstract*—Information security plays a vital role in communication. The threats to information security have been incrementing at confounding rate. The most influential approaches used against such threats are cryptography and steganography. Cryptography and Steganography are two most popular ways to secure data transmission. However, combination of these two techniques results in appearing a highly secured method for data communication. In the proposed system for cryptography, the algorithm of substitution is based on Play Color Cipher and asymmetric RSA algorithm is used to make Play Color Cipher key in encrypted form. In steganography, encrypted key is hidden using multimedia steganography technique.**

Keywords— Play Color Cipher, Cryptography, Steganography

I. INTRODUCTION

Security is main concern regarding data transfer. Integrity of data is important factor for the both sender as well as receiver. In today's times, many techniques are used to ensure the same; those techniques are cryptography and steganography. A new technique proposed with combination of cryptography and steganography enhance with new secure feature for generating a new security system. Combination of this two techniques results in appearing a highly secured method for data communication.

A. Cryptography

Cryptography serves as an important tool for sending information securely in communication system. The cryptography basically takes place between the sender and receiver. The process involved in the communication between the sender and receiver is of two types, encryption and decryption. Encryption is a process where in the ordinary information also called as the plain text is coded into some unrecognizable form which is usually called the Cipher text. The decryption process starts with converting the cipher text which is in the unrecognizable form to ordinary information form to ordinary information that is plain text.

B. Steganography

Steganography is data hidden within data. Steganography techniques can be applied to image, a video files or an audio files. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from aiding in unauthorized viewing. Steganography must not be confused with cryptography. The main goal of steganography techniques is that it is difficult to detect the image and so saved from attack.

C. Play Color Cipher Algorithm

Play Color Cipher Algorithm is an innovative cryptographic substitution method. In this algorithm, each character i.e. small and capital letters, numbers, symbols are substituted using numerous colors in the world. The plain text is encrypted in color block and further this color block is used to decrypt and get the plain text at the receiver side.

D. RSA Algorithm

RSA algorithm is an asymmetric cryptographic algorithm. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The security of this algorithm is based on the difficulty of prime numbers. It allows the sender to encrypt the message using public key and decrypt the message using private key by receiver. So, the security will be high using RSA in public key encryption.

E. MSB Algorithm

MSB (Most Significant Bit) is an algorithm, which replaces the most significant bit in the input audio file to hide a sequence of bytes containing the hidden data. This is an effective technique used for message hiding using audio steganography.

The rest of the paper is organized as follows. Section II presents related work. A working of StegoCrypt is presented in section III. Discussion is presented in section IV. Finally, conclusion and result are given in the last section.

II. LITERATURE SURVEY

In this section we present history and related work of Cryptography, Steganography and its algorithms.

A. History

1) Traditional Symmetric-Key Ciphers: At sender and receiver side, the same secrete key used for Symmetric key

ciphers. Ciphers consist of Substitution and Transposition ciphers. In Substitution, cipher replaces one symbol with another. And in Transposition cipher reorders the symbols [1].

2) Modern Symmetric-Key Ciphers: In Modern Symmetric Key, a k-bit key is used to encrypt and decrypt the n-bit block of plain text. Examples of this type of cryptography algorithms are AES and DES. The message is processed bit by bit by Modern Stream Ciphers and typically have a pseudo random stream key [1].

3) Asymmetric-Key Cryptography: Unlike symmetric key cryptography, this technique have two distinct keys, a public key and a private key. For encryption, public key of sender is used and that for decryption, private key of the sender is used. RSA security depends upon the factoring of large integers [1].

B. Related Work

Ramesh Kumar, et.al uses bit plane method to hide data. A bit plane consists of bits corresponding to same significant level in all the elements. This method replaces the lowest 3 or 4 bits of the cover image to hide the data, hence, embedding data into the bit planes of the cover image. The message is encrypted before embedding in the cover file. A secret key is used for encryption, which is XOR with 2s complement of the message, hence results in encrypted text. An image is selected, which is converted into gray-scale. Numbers of bitplanes are selected and then the encrypted text is embedded into the selected planes of the cover file. Bitmap images are used to hide the data [2].

Ankita and Vishal introduces a new approach to substitute the LSB of RGB true color image. The proposed method, uses a secret key to hide information into cover image. The cover image is divided into three color matrices (Red, Green and Blue). The secret key is converted into 1D array of bit stream. Matrices are XORed with the secret key for finding the position to hide the given data. This process provides a new dimension for image steganography [3].

Mr.Vikas Tyagi et.al, discussed a technique based on the LSB (Least Significant Bit) and a new encryption algorithm. Before hiding the data in an image the application first encrypts it. Symmetric key encryption is used to encrypt the data and then the encrypted data is embedded using least significant bit technique (matching pixel) [4].

Ankita presents a model by combining cryptography and steganography techniques. In cryptography, Simplified Data Encryption Standard (SDES) algorithm is used to encrypt the secret message and then alteration component method is used to hide encrypted message in the cover image [5].

Rajkumar Yadav used combination of cryptography and steganography to enhance embedding capacity of a steganographic channel by preprocessing the secret data and applying encryption technique over it and compress the data before sending it to receiver using gray level modification (GLM) technique. Matrix encoding technique is used for encryption of the data. The proposed work technique is limited to textual data only. Here the concept of Scrambled Letters, Dictionary Module is also used [6].

III. PROPOSED SYSTEM

Proposed system consists of sender side and receiver side. At sender side, system takes input text from user. This text is substituted with color block by using Play Color Cipher algorithm. This algorithm accepts two keys known as starting address and increment value from the user which generates a color block which is a substitution for the message. Before transmission, the starting key and increment value is encrypted using encryption algorithm. These keys are hidden using multimedia steganography technique and it is sent to receiver via mail. At receiver side, user first recovers the hidden key. After recovering, user decrypts keys and generates plain text.

The working of StegoCrypt is as shown in Fig. 1.

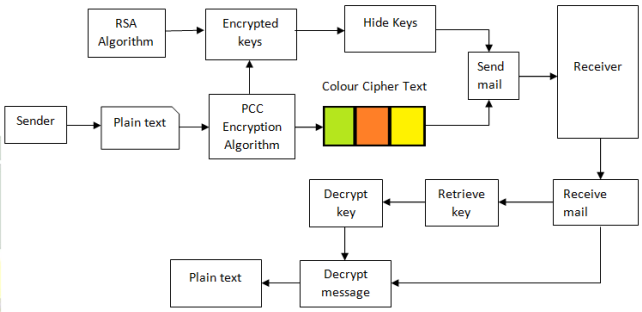

Fig. 1. A Block Diagram of StegoCrypt.

A. Algorithm

The Algorithm of the proposed system is as follows:

- Select Starting address Key1 such that Key1 <N Where: N =256*256*256*256 = 4,29,49,67,296,)
- Select Increment value Key2 such that (Key1 + (C * Key2)) <N

  Where: C - Number of characters in the plain text,

  N- Maximum number of colors
- Enter plain text
- Encrypt plain text using Play Color Cipher Algorithm for generating cipher text.
- Encrypt Key1 and Key2 using RSA Public key encryption algorithm.
- Hide the encrypted keys using audio steganography.
- Send hidden keys and encrypted message to the receiver side via Mail.
- Receiver receives mail and retrieve hidden keys and decrypt PCC keys.
- Using PCC algorithm decrypt cipher text into plain text.

IV. DISCUSSION

RSA uses 1024 bits as its key in asymmetric and that for symmetric, it is 80 bit key. In RSA, upto 2 keys can be used i.e. private and public keys. Earlier, Simplified Data Encryption System(SDES) was used which rolls its own encryption i.e. it

has keyless transmission. This type of transmission is not secure.

In this section, different algorithms are compared with Play Color Cipher algorithm as shown in Fig. 2.

Techniques/ Parameter	Caesar cipher	Play fair cipher	Hill cipher	**Play Color Cipher**
Key Type	Substitution	Substitution	Substitution	Substitution
Block Size	1	2	m	Equal to length of text
Key Size	Fixed Number	Fixed (25!)	variable	Fixed number
Attack Type	Brute-Force attack	Cipher text only (frequency distribution)	Known plaintext attack	Brute-Force attack, Man in the Middle, Birthday Attack
Algorithm Strength	Only 25 keys possible	26*26=676 diagrams possible	Hide single letter frequency distribution	256*256*256*256
Encryption & Decryption Process	Symmetric	Symmetric	Symmetric	Symmetric
Key Factor (Uniqueness) about the technique	Simple substitution with Alphabet	Use pair of letters and substitute with 5×5 matrix designed with key and remaining alphabets	Based on Linear algebra, Convert plaintext into matrix based on ASCII value	Letters substituted by color

Fig. 2. Comparison Table of Cryptographic Techniques [7].

V. RESULT

After executing, it is observed that, Play Color Cipher is appropriately converting plain text into cipher text with two encrypted session keys and further they are hidden in an audio file. Then these hidden keys and encrypted message reached at the receiver side via Email. At receiver side, hidden keys are retrieved and decrypted. Further cipher text is converted into plain text by reverse Play Color Cipher Algorithm.

CONCLUSION

The security is an essential concept of the digital data, it becomes more sensitive when the data is travelled through the untrusted environment. Here the untrusted environment can be any openly accessible network where anybody can use the network facilities. Using the combination of cryptography and steganography, the cipher has great potential as it eliminates major attacks like brute force, man in the middle, known plain text and known cipher text attacks. In proposed system, implementation of encryption-decryption scheme is done using symmetric and asymmetric techniques an steganography scheme for securing the transmission of data.

REFERENCES

[1] D. Patil and V. Nayak, "Cryptography based on color substitution," vol. 91, April 2014.

[2] B. Kumar and K.Suresh, "Enhanced approach to steganography using bitplanes," International Journal of Computer Science and Information Technologies, vol. 3, no. 6, pp. 5472–5475, 2012.

[3] A. Gangwar and V. shrivastava, "Improved rgb -lsb steganography using secret key." International Journal of Computer Trends and Technology, 2013.

[4] M. V. Tyagi and M. A. kumar, "Image steganography using least significant bit with cryptography." Journal of Global Research in Computer Science, March 2012.

[5] A. Agarwal, "Security enhancement scheme for image steganography using s-des technique," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, April 2012.

[6] R. Yadav, "Information security using blend of steganography and cryptography," Int. J. Comp. Tech. Appl., vol. 2, no. 6, Nov-Dec 2011.

[7] P. Poonia and P. Kantha, "Comparative study of various substitution and transposition encryption techniques," International Journal of Computer Applications, vol. 145, no. 10, July 2016.