Secure Encryption and Decryption using Play Color Cipher

Priyanka V. Deshmukh[1] Netra R. Bujad[2] Prof. Sachin Sonawane[3]
[1,2,3]Atharva College of Engineering, Mumbai University,Mumbai, India

Abstract— The threats to information security areincreasing at very rapidly. The most effective and universal approach to counter such threats is encryption. In Traditional encryption techniques substitution and transposition is used. In Substitution techniques plaintext is mapped into ciphrtext. In all traditional substitution techniques plaintext characters, numbers and special symbols are substituted with another characters, numbers and special symbols. In this new method an innovative cryptographic substitution is proposed to generate a stronger cipher than the existing substitution algorithms. This method focus on the substitution of characters, numbers and special symbols with color blocks. This algorithm of substitution is based on Play Color Cipher. This is a symmetrical system which is implemented by encryption of text by converting it into colors. Each character of the plaintext is encrypted into a block of color. Every character will be substituted by a different color block. To produce the original text inverse process is used using color block.

Key words: Information security, plaintext, play colorcipher, encryption, decryption, color block

I. INTRODUCTION

Encryption techniques are used widely in security of data. Malicious users are also ready to attack on encryption algorithm security. Different types of attack can apply on the algorithm, but when an algorithm develops it is also ready to defend against attack. Encryption algorithm is based on number of substitution and transposition. When a substitution algorithm is developed strong then it normally uses number of substitution and transposition, but it is easy to break. When for encryption an algorithm process on data then it uses one of the approach block cipher or stream cipher. In block cipher it uses a block of plaintext for encryption and gives a block of cipher text in return. Where in stream cipher it continuously takes plaintext character one by one and gives cipher text[2].

The power of cipher text is dependent on encryption and confidentiality of key. In past years many researchers trying to modified algorithms to fulfill need of security[1].Play color cipher is a new substitution technique. Each character (capital and small letter, number (0-9), symbol on keyboard) in plaintext is substituted with a block of color from 18 decillion of color. At the receiving end the cipher text block (in color) is decrypted in to plaintext. In play color cipher we need to transmit key for security of algorithm. It use RSA algorithm for key transmission which is a public key algorithm. Play color cipher uses same way of encryption as we use in the play fair cipher. [2]

A. Need

Widespread transmission over various communication networks has forced the security of multimedia data to be a critical issue and also a source of attraction for many researchers. If we want to secure any type of data then we have various ways like, encryption algorithm, digital signature and authentication protocol. While there are a lot of traditional techniques to protect plaintext, most of which use traditional approach in which plaintext is replaced another letter or any symbol which can be cracked easily by attackers. When a substitution algorithm is developed strong then it normally uses number of substitution and transposition, but it is easy to break.

B. Applications

The 'Play Color Cipher' is evolving into a standard means of substitution technique. Cryptography is a key technology for achieving information security in communications, computer systems, electronic commerce, and in the emerging information society. The security of cipher text is completely dependent on two things: the power of the cryptographic algorithm and the confidentiality of the key. In recent past many researchers have modified the existing algorithms to fulfill the need in the current market, yet the ciphers are vulnerable to attacks. This project proposes such a technique which is resistant against problems like Meet in the middle attack, Birthday attack and Brute force attacks. The size of the plain text is also reduced by 4 times when it is encrypted, in a lossless manner. The space occupied by the cipher text in the buffer is very less; hence transmitting through a channel is very fast which subsequently brings down the transportation cost[1].

II. REVIEW OF LITERATURE

A. Existing Cryptographic Systems

1) Traditional Symmetric-Key Ciphers

Symmetric-key ciphers use the same secrete key on both sender and receiver side. These ciphers consist of Substitution and Transposition ciphers. A Substitution cipher replaces one symbol with another. Transposition cipher re-orders the symbols[1].

2) Modern Symmetric-Key Ciphers

In symmetric-key modern block cipher n-bit block of plaintext encrypts and decrypts n-bit block of ciphertext using a key of k-bit. DES and AES are examples of this type of cryptography algorithms. Modern Stream Ciphers process the message bit by bit (as a stream) and typically have a (pseudo) random stream key [1].

3) Asymmetric-Key Cryptography

This system is based on personal secrecy. Unlike symmetric key cryptography, it has two distinctive keys: a public key and a private key. Public key of the receiver side is used for encryption while t h e private key of sender side is used for decryption. RSA is the most widely used asymmetric key algorithm. The security of RSA depends on the difficulty of factoring large integers [1].

III. DESIGN AND IMPLEMENTATION

A. Algorithm

1) Encryption[1]

1) First accept the input text file and the key.
2) Separate the input text file into individual characters.
3) Input the block size of key, color-channel (RGB) and a color (RGB value).
4) Depending on the block-size, divide the picture box into a grid of blocks.
5) Add the ASCII value of each character with the position and put the value in the color-channel selected.
6) For the remaining two channels, put the value of the Color given by the user.
7) Draw the bitmap image using all values.
8) Generate the Key using all values.
9) Send the image to the receiver side.

2) Decryption[1]

1) Add the ASCII value of each character with the position and put it in the color-channel selected.
2) For the remaining two channels, put the value of the Color as given by the user.
3) Draw the bitmap image using all values.
4) Generate the Key using all values.
5) Send the image to the receiver side.
6) Subtract the block's position from that value used.
7) Convert the resulting value into the respective characters and get the original text.
8) Decrypt the text using the decryption process of the standard encryption algorithm used.
9) Get the original text back using the decryption process.

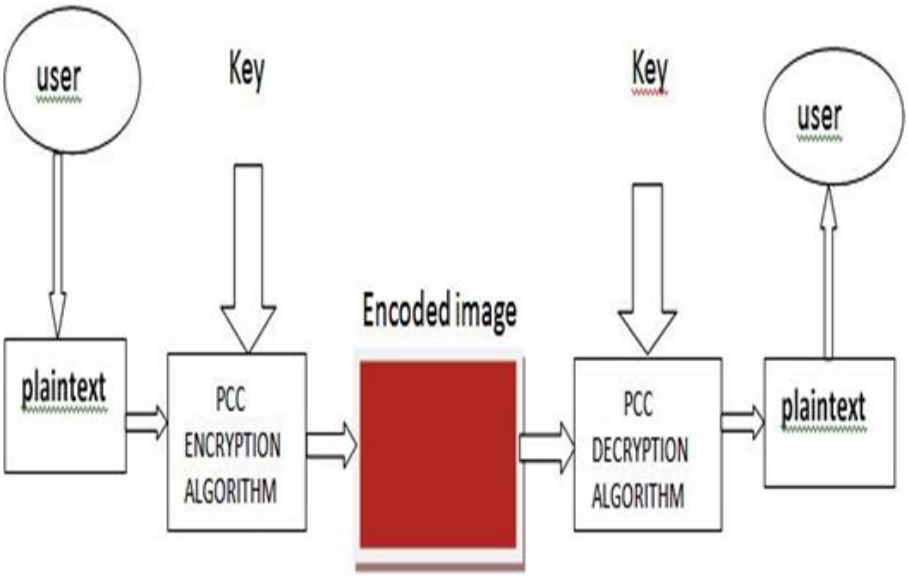

Fig. 1: Block diagram of play color cipher

B. Implementation

The fig.1 describes a diagram which shows working of this concept.

IV. REPRESENTATION OF THE WORKING

A. Encryption

1) Conversion Of Character Into Color Block

The user selects a color channel from R, G or B and gives the values for remaining channels between the range 0-255. The character is then converted to its ASCII value and it is assigned to the selected channel. Also, a block size which is greater than 0, is specified by the user. A color block of the specified block size is then formed by combining the values of all three channels given by the user[2].

2) Generation Of The Key

The color channel which is selected and the size of the color block together forms the key[2].the character in the plaintext is mapped and its positional value and ASCII value together form unique value that substitute in one of the three channels i.e. R G B. Other two channels take any random values and together form key followed by the channel number i.e. 1, 2 or 3[1].

3) Transmission Of Key

Key is transmitted using RSA Public key encryption algorithm [4]

4) Generation Of An Image

All the characters are converted into color blocks and then a single image is generated by putting together all the color blocks[2].

B. Decryption

1) Block Size And The Selected Channel

The block size and the color channel are taken from the key.The key is generated using block size and channel there for block size and channel that is used for encryption can be regenerated using the key[2].

2) Extraction Of Pixel Value From The Image

The received image is divided into blocks whose size is specified in the key. A center pixel and its 4-nearest neighbor pixels from each block are taken and the most common pixel value is selected from all the values. This is done to improve the robustness of the algorithm in case noise is present[2].

3) Retrieval Of The Message

From the pixel value which is selected, the component value of the selected channel is extracted (R, G or B component) and it is considered as an ASCII value. This ASCII value is then converted to its corresponding character. After all such characters are extracted, the original message is retrieved[2].

V. CONCLUSION

This paper gives a brief introduction about the Encryption Algorithm implemented using play color cipher. The article provides a new method for protecting confidential information using colors. By implementation of this algorithm, we will propose a way of Encryption and Decryption.

REFERENCES

[1] Devyani Patil, Vishakha Nayak, Akshaya Sanghavi, Aparna Bannore, Cryptography based on color substitution, Volume 91 – No.16, April 2014.
[2] Pritha Johar, Santosh Easo, K K Johar, A Novel Approach to Substitution Play Color Cipher, Volume 1 .Issue 2, October 2012.
[3] Seyed Mohammad Seyedzadeh , Sattar Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, 2012.
[4] Cryptography and Network security by Stallings" RSA Scheme" -Page Number-286.