Generation of a Novel Cryptographic Algorithm for Implementation of Play Color Cipher Substitution Technique

Rahul Patil¹, Sarvesh Mhatre² & Shreyas Mankar³
Prof. Maya Vargese⁴, Prof. Arlina Mascarneas⁵
¹,²,³Information Technology Dept., Universal College Of Engineering Vasai India,

Abstract: The emerging threats to information security are increasing at an alarming rate. The most influential and universal approach to counter such threats is encryption. Traditional encryption techniques use substitution and transposition. Substitution techniques map plain text into cipher text. In this paper, an innovative cryptographic substitution method is proposed to generate a stronger cipher than the existing substitution algorithms. This method emphasizes on the substitution of characters, numbers and special symbols with color blocks. This algorithm of substitution is based on Play Color Cipher. The cryptanalysis done on this will prove that the cipher is strong. This play color cipher helps the sender and the receiver to establish a secure connection when transmitting a file over a communication network.

Keyword – D , E , PCC , RSA

1. Introduction

Cryptography is a key technology for achieving information security in communications, computer system, 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 is a symmetrical system which implements encryption of text by converting it into colors. Each characters of the message are encrypted into a color block. Every characters will be replaced by a different color blocks. The inverse process is used to produce the original text from color blocks at the receiver side. The user types a message which is a plaintext. There will be three color channels i.e. R, G or B (Red, Green or Blue), out of which one channel needs to be chosen by user to encrypt the message. The user must specify the values for the remaining channels from the range 0-255. All the characters of the text are then converted to blocks of color formed by combining the values of R, G and B channels. An image is generated by combining all the color blocks of the message. The channel selected form the key. At the decryption (receiver) side, the image is divided into blocks. From each block, the pixel value of center position is extracted and then converted to a character. This is done for all blocks and the corresponding characters are extracted. Hence the original message is retrieved.

2. Literature Review

2.1. Image Encryption Using Advance Hill Cipher Algorithm

The Hill Cipher algorithm is one of the symmetric key algorithm that have several advantages in data encryption. But, the inverse of key matrix used for encrypting the plain text does not always exist. Then if the key matrix is not invertible, then the encrypted text cannot be decrypted. In the evolutionary matrix generation method the key matrix used for encryption is its invertible.

2.1.1. Advantages

• This scheme is fast encryption scheme which overcomes problem of encrypting with homogeneous background.
• This algorithm works for any image with different gray scale as well as color image.

2.1.2. Disadvantages

• Hill cipher can't encrypt the image properly if the image consist of large area covered with same color.
• If the key matrix is not invertible ,then the encrypted text cannot be decrypted.

2.2. Cryptography Based On Color Substitution

The threats to emerging information security are increasing at an alarming rate. The most influential
and universal approach to counter such threats in encryption. Traditional encryption techniques use substitution and transposition. Substitution techniques maps plain text into cipher text. This algorithm is based on color cipher.

2.2.1. Advantages
- Resistant against problems like Meet in the middle attack, Birthday attack and Brute force attacks.
- Encrypted in a lossless manner.

2.2.2. Disadvantages
- Vulnerable to brute-force attacks.
- Security on RSA relies on the difficulty of factoring large integer.

2.3. Secure Encryption And Decryption Using Play Color Cipher

In traditional encryption technique substitution and transposition is used. In substitution technique plain text is mapped into cipher text. In all traditional substitution technique plain text characters, numbers and special symbols are substituted with another characters, numbers and special symbol. In this new method an innovative cryptographic substitution is proposed to generate stronger cipher than the existing substitution algorithms.

2.3.1. Advantages
- Size of cipher text is small.
- Speed of transmission through the channel is fast.

2.3.2. Disadvantages
- Not much secured.

3. Proposed System

The proposed cryptographic substitution method is called Color coded cryptography which modifies the Play Color Cipher. This is a symmetrical system which is implemented by encryption of text by converting it into colors. Each character of the message is encrypted into a block of color. Every character will be substituted by a different color block. The inverse process is used to produce the original text from colors at the receiver side. The user enters a message which is the plaintext. A channel needs to be chosen from the three color channels i.e. red, green and blue (RGB). The user must specify the values for the R, G and B channels from the range 0-255. Also a block size needs to be specified. All the characters of the text are then converted to blocks of color formed by combining the values of R, G and B channels. A single image is then generated for all the color blocks of the message. The block size and the channel selected form the symmetric key. At the decryption side, the image is divided into blocks of the size specified in the key. From each block, the pixel value of the center pixel is extracted and then converted to a character. This is done for all blocks and the corresponding characters are extracted. Thus the original message is retrieved.

3.1. Block Diagram

![Figure 1. Block Diagram Of Play Color Cipher](image)

4. Algorithm

4.1. Encryption :-
1. Accept the input text file and the key.
2. Separate the input text into individual characters.
3. Input the block size, color-channel (R/G/B) and a color (RGB value).
4. Depending on the block-size (say n), divide the picture box into a grid of blocks, each of size n.
5. Add the ASCII value of every character with its position and put the value in the color-channel selected.
6. For the remaining 2 channels, put the value of the Color inputted by the user.
7. Draw the bitmap image.
8. Generate the Key.
9. Send the image to the receiver.

4.2. Decryption :-
1. Add the ASCII value of character with its position and put the value in the color channel selected.
2. For the remaining 2 channels, put the value of the Color inputted by the user.
3. Draw the bitmap image.
4. Generate the Key.
5. Send the image to the receiver.
6. Subtract the blocks position from that value.
7. Convert the resulting value into character and get the text.
8. Decrypt the text using the decryption process of the standard encryption algorithm used.
9. Get the original text back

5. Acknowledgements

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organization. I would like to extend my sincere thanks to all of them. I am highly indebted to my college for their guidance and constant supervision as well as for providing necessary information regarding the project & for their support in completing the project. I would like to express my gratitude towards my parents & members of my project for their kind co-operation and encouragement, which helped me in completion of this project.

6. References


