Color Cryptography using Substitution method

Manali Naik[1], Pushpanjali Tungare[2], Pooja Kamble[3], Shirish Sabnis[4]

[123]Student, IT, Rajiv Gandhi institute Of Technology, Maharashtra, India
[4]Professor, IT, Rajiv Gandhi institute Of Technology, Maharashtra, India

---***---

Abstract— *In world of computer network, threats come in many different forms. Some of the most common threats today are software attacks. If we want to secure any type of data then we can use encryption technique. All traditional encryption techniques use substitution and transposition. Substitution techniques map plaintext into ciphertext in which characters, numbers and special symbols are substituted with other characters, numbers and special symbols.*

In this paper, we are using an inventive cryptographic substitution method is to generate a stronger cipher than the existing substitution algorithms. This method focuses on the substitution of characters, numbers and special symbols with color blocks. This algorithm of substitution is based on Play Color Cipher.

Keywords— Play Color Cipher (PCC), Color substitution, Color block, Color code.

General Term--Encryption, Decryption, Block Cipher, Play Color Cipher, Security and Algorithm.

1.INTRODUCTION

Information security is the protection of information and minimises the risk of exposing information to unauthorised parties from disclosure, modification, and destruction of data. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The security of cipher text is totally dependent on two things: the power of the cryptographic algorithm and the confidentiality of the key. Many researchers have modified the existing algorithms to fulfill the need in the current market, yet the ciphers are vulnerable to attacks.

2. LITERATURE SURVEY

2.1Existing Cryptographic System

1. Traditional Symmetric-Key Ciphers

In symmetric key ciphers, plaintext is converted into cipher-text using a shared secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher-text. The Secret Key is shared by both, the sender and the receiver which they must have obtained in a secure fashion & should keep the key hidden.
These ciphers consist of Substitution and Transposition ciphers. A Substitution cipher replaces one symbol with another. A Transposition cipher re-orders the symbols [7].

2. Modern Symmetric-Key Ciphers

A symmetric-key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of cipher-text. The encryption or decryption algorithm uses a k-bit key.
A modern block cipher can be designed to act as a substitution cipher or a transposition cipher DES and AES are examples of this type of cryptography algorithm [7].

3. Asymmetric-Key Cryptography

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. In such type of cryptography user who wants to send an encrypted message can get the intended recipient's public key from a

public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.
RSA and Merkle–Hellman knapsack cryptosystem is the most commonly used asymmetric key algorithm. The security of RSA relies on the difficulty of factoring large integers [7].

2.2 Threats and vulnerabilities in existing systems

RSA is working on the base of multiplication of two prime numbers. Therefore, number factorization is a serious threatening against RSA and currently different kinds of attacks have indentified against RSA by cryptanalysis. Most attacks appear to be the result of misuse of the system or bad choice of parameters.
A well-known attack on RSA can break the RSA in 953 milliseconds of length with 180 digits, where n is the product of two unequal prime numbers [6] [10].

Substitution techniques like Caesar Cipher, Mono alphabetic Cipher, Play fair Cipher and Poly alphabetic Ciphers are not strong enough since they are vulnerable to brute-force attacks [7].

3. PROPOSED CRYPTOGRAPHIC SYSTEM

We propose a cryptographic substitution method which modifies the “Play Color Cipher” that is called as Color coded cryptography [3]. This system is based on symmetric encryption which is implemented by encrypting text into color image. 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 color block at the receiver side. The user enters a message which is the plaintext sender side. 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 between the ranges 0-255. Also a block size of color block needs to be specified.

All the characters of the text are then converted to color blocks formed by combining the values of R, G and B channels. A single image is then generated by combining all the color blocks of the message. The block size and the channel selected form the symmetric key.

At the decryption side, the received image is divided into blocks of the size specified in the key. From each block, the value of the centre pixel is extracted and then converted to a plaintext character. This is done for all blocks and the corresponding characters are extracted. Thus the original message is retrieved.

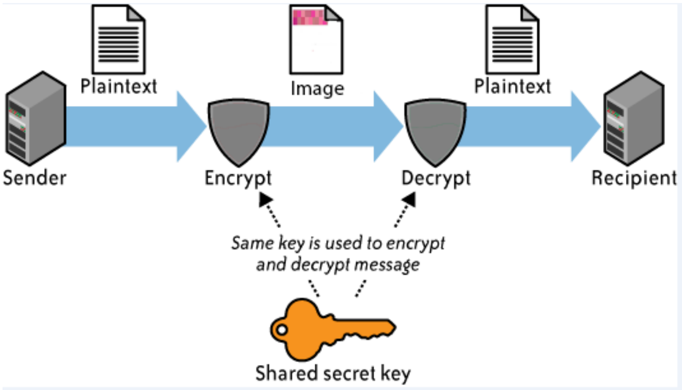

Fig 1: Block Diagram

3.2 Advantages of proposed system

Each character present in the plaintext is substituted with a color block from the available 18 Decillions of colors in the world and at the receiving end the cipher text block (in color) is decrypted in to plain text block. It prevents against problems like Meet in the middle attack, Birthday attack and Brute force attacks [3].

4. ALGORITHM

4.1.1Encryption.

- Accept the input text file and the key.
- Separate the input text into individual characters. Input the color-channel (R/G/B) and a color (RGB value).
- Depending on the predefined block-size (say n), divide the picture box into a grid of blocks, each of size n.

- Add the ASCII value of every character with key and put the value in the color-channel selected.
- For the remaining 2 channels, put the value of the Color inputted by the user.
- Draw the bitmap image.
- Generate the Key.
- Send the image to the receiver.

4.1.2Decryption

- Receiver receives the image and the key.
- Divide the color image into color blocks according to block size specified into the key.
- Get the value of individual color block and subtract the key from that value.
- Convert the resulting value into character and get the text.
- Decrypt the text using the decryption process of the standard encryption algorithm used.
- Obtain the original text back.

5. IMPLEMENTATION

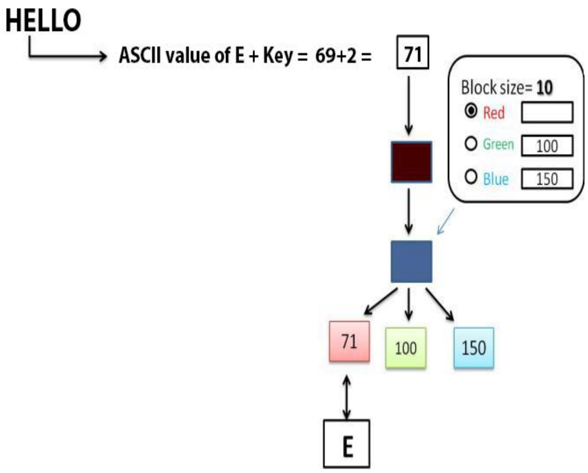

Fig 2: describes a working of this concept.

5.1Encryption

1. The user selects a one color channel (R, G or B) and gives the values for remaining two channels between the ranges 0-255. The character is converted to its ASCII value and assigned to the selected color channel. Also, a block size greater than 0, is specified by the user. Color is given to the color block of the specified block size is then formed by combining the values of all three channels.

2. Key Generation

The color channel selected and the color blocksize forms the key.

3. Image Generation

All the characters are converted to color blocks and then a single image is generated by combining all the color blocks of plaintext.

5.2 Decryption

1.Receiving image and shared secrete key

The block size and the color channel are extracted from the shared secrete key.

2. Extracting of pixel value from the image

The received image is divided into blocks of the size specified in the key. A center pixel and its 4-nearest neighbor pixels from each block are extracted and the most common pixel value is selected. This is to improve the robustness of the algorithm in the case of presence of noise.

3. Retrieval of the plaintext

From the selected pixel value, the component value of the selected channel is taken (R, G or B component) and considered as an ASCII value. This ASCII value is then converted to its corresponding character similarly for all other color blocks. After extracting all such characters, the original message is retrieved.

6. Technology used

1. C#.net

C# is an elegant and type-safe object-oriented language that enables developers to build a variety of secure and robust applications that run on the .NET Framework. You can use C# to create Windows client applications, XML Web services, distributed components, client-server applications, database applications, and much, much more. C# syntax is highly expressive, yet it is also simple and easy to learn. The curly-brace syntax of C# will be instantly recognizable to anyone familiar with C, C++ or Java [8] [9].

7. APPLICATION

This system of color cryptography can be used for authentication of login systems. During the registration process, the new user will enter his personal details and the password. The password is then encrypted into a color-coded image using the proposed color substitution algorithm. The image is then stored at the server. At the time of login, the user enters the username and password. Based on the username, corresponding image of the password is retrieved from server, decrypted and converted to text. This text is then matched with the password entered by the user. If it matches, the user successfully logs in. The key for encryption and decryption can be based on the parameters of the personal details entered by the user. Mathematical functions performed on the timestamp of registration and user‟s date of birth can generate a key. Thus, the need for storage of key is eliminated

8. CONCLUSION

Today's standard cryptographic methods are subject to a variety of attacks. An innovative approach presented and implemented in this paper makes information secure by color substitution. In future, the figures, tables, images, etc can be included in the plaintext for conversion and hence the scope of the algorithm can be increased

9. ACKNOWLEDGMENTS

We wish to express our sincere gratitude to Dr. U. V. Bhosle, Principal and Prof. D. M. Dalgade, H.O.D of Information Technology Department of RGIT for providing us an opportunity to do our project work on "Color cryptography using substitution method". This project bears on imprint of many people. We sincerely thank our project guide Prof. S. K. Sabnis for his guidance and encouragement in successful completion of our project synopsis. We would also like to thank our staff members for their help in carrying out this project work. Finally, we would like to thank our colleagues and friends who helped us in completing the project synopsis successfully.

10. REFERENCES

[1] Aditya gaitonde 2012. Color Coded Cryptography, International Journal of Scientific & Engineering Research, Volume 3, Issue 7.

[2] Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger, 2011, Biclique Cryptanalysis of the Full AES, Crypto 2011 cryptology conference, Santa Barbara, California.

[3] Prof. K. Ravindra Babu, Dr.S.Udaya Kumar, Dr.A.Vinaya Babu and Dr.Thirupathi Reddy, 2010. A block cipher generation using color substitution, International Journal of Computer Applications Volume 1 – No. 28.

[4] Sastry V.U.K, S. Udaya Kumar and A. Vinaya babu, 2006. A large block cipher using modular arithmetic inverse of a key matrix and mixing of the key matrix and the plain text. Journal of Computer Science, 2(9): 698703.

[5] Pritha Johar, Santosh Easo and K K Johar, 2012. "A Novel Approach to Substitution Play Color Cipher", International Journal of Next Generation Computer Application Volume 1- Issue 2.

[6] Johan Hastad, 1986. "On using RSA with low exponent in a public key network", Advances in Cryptology-CRYPTO "85, LNCS 218, pp. 403-408. [7] B.A.Forouzan, Cryptography and Network Security, 4th edition, 2008.

[8] Christian Gross, Beginning C# 2008 From Novice to Professional 2 nd edition, 2008.

[9] Jay Hilyard and Stephen Teilbet, C# 3.0 Cookbook, 3rd edition, 2007.

[10] Nguyen, H. Number Theory and the RSA Public Key Cryptosystem. http://cdn.bitbucket.org/mvngu/numtheory

[11] crypto/downloads/numtheory-crypto.pdf. Accessed on 25/9/2009.

[12] National Bureau of Standards "Data Encryption Standard" FIPS-PUB, 46, Washington, D.C., Jan 1977. http://csrc.nist.gov/publications/fips/fips46-3/fips463.pdf
.