Cryptography based on Color Substitution

Devyani Patil
SIES GST, Navi Mumbai, India.

Vishakha Nayak
SIES GST, Navi Mumbai, India.

Akshaya Sanghavi
SIES GST, Navi Mumbai, India.

Aparna Bannore
SIES GST, Navi Mumbai, 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 plaintext into ciphertext. In all traditional substitution techniques, characters, numbers and special symbols are substituted with other characters, numbers and special symbols. 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.

General Terms

Encryption, Decryption, Block Cipher, Play Color Cipher, Security and Algorithm.

Keywords

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

1. INTRODUCTION

Information Security which refers to protecting information in potentially hostile environments is a crucial factor in the growth of information-based processes in industry, business, and administration. 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. Intruder activities in recent times have created a need for inventing stronger and more secure algorithms. 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.

2. LITERATURE SURVEY

2.1 Existing Cryptographic Systems

1. Traditional Symmetric-Key Ciphers

In Symmetric-key ciphers, the sender sends the plaintext which is encrypted using a shared secret key. The receiver decrypts it using the same shared key. 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 and decrypts n-bit block of ciphertext using a k-bit key. DES and AES are examples of this type of cryptography algorithm. Modern Stream Ciphers process the message bit by bit (as a stream) and typically have a (pseudo) random stream key [7].

3. Asymmetric-Key Cryptography

This system is based on personal secrecy. Unlike symmetric key cryptography, this has distinctive keys: a public key and a private key. Public key of the receiver is used for encryption while the private key of sender is used for decryption. RSA 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 very vulnerable to chosen plaintext attacks. There is also a new timing attack that can be used to break many implementations of RSA. The RSA algorithm is believed to be safe when used properly, but one must be very careful when using it to avoid these attacks. A well-known attack on RSA can break the RSA in 953 milliseconds of length ‘n’ with 180 digits, where n is the product of two unequal prime numbers [6][10].

One of the most extensively used cryptographic method, DES, was also broken and announced by electronic Frontier Foundation in July 1986 [12]. A newly discovered technique known as biclique cryptanalysis helps attackers to remove about two bits from 128-, 192-, and 256-bit keys and recover AES secret keys up to five times faster than previously possible [2].

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

3.1 Diagrammatic representation

We propose a cryptographic substitution method called Color coded cryptography which modifies the “Play Color Cipher” [3]. 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 centre 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.

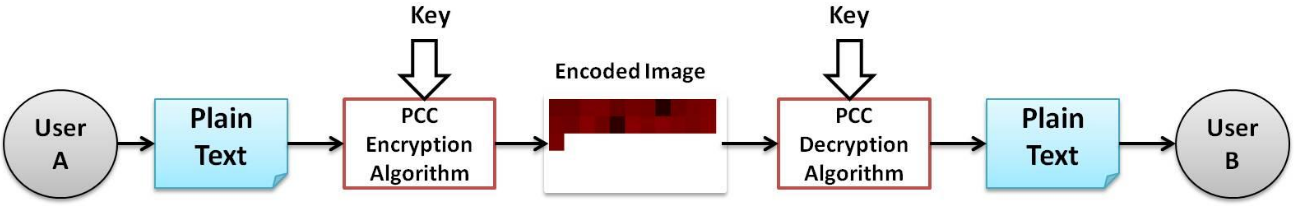

Fig 1: Block Diagram

3.2 Advantages of proposed system

Each character (available on the keyboard) 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 is resistant against problems like Meet in the middle attack, Birthday attack and Brute force attacks [3].

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. [3]

4. DESIGN AND IMPLEMENTATION

4.1 Algorithm

4.1.1 *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.

4.1.2 *Decryption*

1. Add the ASCII value of every 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 block’s 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.

4.2 Implementation

Fig. 2 describes a diagram for the working of this concept.

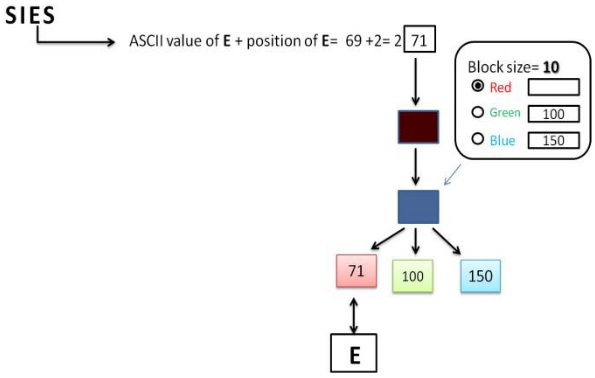

Fig 2: Representation of the working

4.2.1 *Encryption*

1. Conversion of character to color block

The user selects a color channel (R, G or B) and gives the values for remaining channels between the range 0-255. The character is converted to its ASCII value and assigned to the selected channel. Also, a block size 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.

2. Generation of the key

The color channel selected and the size of the color block forms the key.

3. Generation of an image

All the characters are converted to color blocks and then a single image is generated by putting together all the color blocks.

4.2.2 Decryption

1. Block size and the selected channel

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

2. Extraction 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 message

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. After extracting all such characters, the original message is retrieved.

4.3 Technologies used

1. C#.net

C# is an object-oriented programming language encompassing strong typing, essential, declarative, efficient, class-based, and component-oriented programming disciplines. C# is a well-designed and type-safe that allows C Sharp developers to build a wide array of secure and robust applications that run on the .NET Framework. It combines the high productivity of rapid application development languages and the raw power of C++. It includes an interactive development environment, visual designers for building windows and web applications, a compiler and a debugger. It has complete access to the same rich class libraries that are used by session tools such as visual basic.net and visual C++.net [8][9].

5. APPLICATION

This system of cryptography can be used for authentication of login systems.

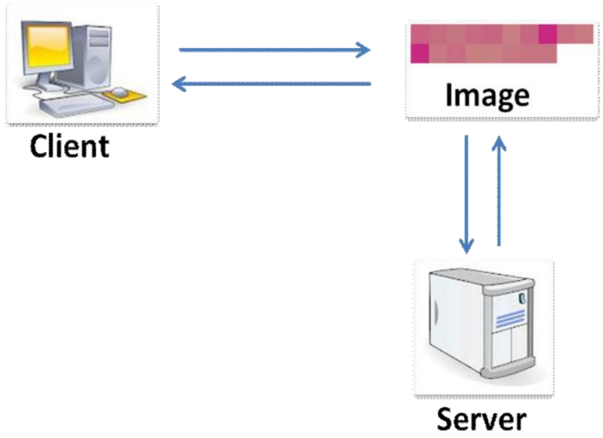

Fig 3: Color coded cryptography for Login-Authentication system

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.

6. CRYPTANALYSIS

Considering the application of Login authentication system which uses the proposed cryptographic system, the length of the key, which is a mathematical function of timestamp (stored at the time of registration) and user's date of birth, is a decimal number with maximum of 28 digits. The key can be any combination of 0 to 9 numbers. Thus, the maximum number of keys can be $(10)^{28}$. Thus, if we perform one encryption per micro second it takes:

$$\frac{10^{28}X10^{-3}}{365X24X60X60} = 3.17 \text{ X } 10^{17} \text{ years}$$

For color substitution, only 3 parameters (RGB) have been used where, each channel has a color-shade range of 0-255. Maximum number of color combinations is 1,67,77,216 in decimal. It will be very tiring to try out all possible combinations. Hence it is safe to conclude that the brute force attack is not possible. Also, there are 18 Decillions of colors in the computer world. Thus, if man in the middle, known plain text, known cipher text attacks is considered, it will not be possible to guess or decrypt the plain text just by obtaining the color image.

7. 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. The cryptanalysis carried out on this experiment shows that 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 future, the figures, tables, images, etc can be included in the plaintext for conversion and hence the scope of the algorithm can be increased. To generate a stronger cipher, the number of parameters (like alpha, gamma correction etc.) can be increased for generating the color to get 18 Decillions of color combinations. With small changes, the same algorithm can be used for languages other than English as well.

8. ACKNOWLEDGMENTS

We would like to express our sincere gratitude to the teaching faculty at SIES GST whose timely inputs and suggestions, helped in the completion of the project. We would also like to thank the Library and Computer Centre Departments of our college for allowing us to carry out our research. Finally, we are thankful for having been given this opportunity to learn something new about the world of technology.

9. 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): 698-703.

[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 2nd 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/fips46-3.pdf