Securing Informative Text using Color Visual Cryptography

Anand Bali
M.H.S.S.C.O.E
Saboo Siddik
Polytechnic Road
Mumbai-08

Saud Ansari
M.H.S.S.C.O.E
Saboo Siddik
Polytechnic Road
Mumbai-08

Kalim Khan
M.H.S.S.C.O.E
Saboo Siddik
Polytechnic Road
Mumbai-08

Wasif Shaikh
M.H.S.S.C.O.E
Saboo Siddik
Polytechnic Road
Mumbai-08

ABSTRACT

The rising threats to information security are increasing at an alarming rate. The most powerful and universal approach to counter such threats is encryption. Conventional encryption techniques use substitution and transposition. Substitution technique change plaintext into cipher text. In all conventional substitution techniques characters, numbers and special symbols are replaced with other characters, numbers and special symbols. In this project, an innovative substitution method is proposed to generate a better cipher than the existing substitution algorithms. This method re-emphasizes on the substitution of characters, numbers and special symbols/characters with color blocks. This project is based on Play Color Cipher. The crypt-analysis is done on this will prove that the cipher is strong.

General Terms

Security, RSA, Color, Image

Keywords

Cryptography, security, encryption, decryption, substitution, Play Color Cipher

1. INTRODUCTION

Information Security which refers to protecting information in potentially hostile environments is a crucial factor in the development 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 rising information society. The security of cipher text is completely based on two things [1]:

i. Strength of the cryptographic algorithm and

ii. Confidentiality of the key

Due to malicious activities in recent times have created a need for developing stronger and more secure algorithms. In recent past years many researchers have modified the existing algorithms to carry out the need in the current market, yet the ciphers are vulnerable to attacks.

Cryptographic systems are used to provide secrecy, privacy and authentication in computer and communication systems. Encryption algorithms encipher the Plaintext, into unintelligible cipher text or cryptograms using a key [2]. Deception algorithm is used for decipher in order to restore the original information. In general, the enciphering and deciphering keys need not be identical (same). Eavesdropping is the interception of messages by monitoring a communication channel. The person who is trying to break (solve) a cipher without knowing the encryption or decryption algorithm and keys is called a cryptanalyst. According to William Stallings [2], Cryptographic systems are generally classified along three independent dimensions:

i. The type of operations used for transforming plaintext to cipher text: all the encryption algorithms are based on two general principles: Substitution, in this each element in the plaintext (bit, letter, group of bits are letters) is mapped in to another element and the transposition in which elements in the plain text are rearranged. Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

ii. The number of keys used: If both sender and receiver uses the same key, the system is referred to as symmetric, single key, secret key, or traditional encryption. If the sender and receiver each uses a different key, the system is referred to as asymmetric, two – key, or public key encryption [2][3].

iii. The way in which the plain text is processed: A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements, producing out put one element at a time, as it goes along.

The aim of this project is to provide secure communication between two parties. So, that secret message/data cannot be compromise.

The objective for developing this project is that, it can provide the security of data. It will also provide the transfer of data from one machine to another. Only the authorized user and administrator can access the application.

This project consists the following objectives:-

i. To achieve security based on cryptographic techniques.

ii. To explore techniques of hiding data using color cryptography.

The main objective of the project is to discuss the properties which help to transmit the secret message or information over a network without any modifications.

2. LITERATURE SURVEY

2.1 Existing Cryptographic System

There are following existing cryptographic techniques that used widely:

2.1.1 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 [4].

2.1.2 Modern Symmetric-Key Ciphers:

A symmetric-key block cipher encrypts an n-bit block of plaintext and decrypts n-bit block of cipher text 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 normally have a (pseudo) random stream key [4].

2.1.3 Asymmetric-Key Cryptography:

This system is based on personal secrecy of data. Unlike symmetric key cryptography, this has distinctive keys: a public key and a private key. Public key of the receiver is required for encryption while the private key of sender is used for decryption. RSA is the most widely used asymmetric key algorithm. The security of RSA relies on the difficulty of factoring large integers [4].

2.2 Threats and Vulnerabilities in Existing System

RSA is very vulnerable to chosen plaintext attacks. There is also a new timing attack that can be used to break RSA algorithm. The RSA algorithm is believed to be safer than other algorithms when used properly/carefully, but one must be very careful when using RSA to avoid 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 [5][6].

One of the most extensively used cryptographic method, DES, was also broken and announced by electronic Frontier Foundation in July 1986 [7]. 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 [8].

Substitution techniques like Caesar Cipher, Mono alphabetic Cipher, Play fair Cipher and Poly alphabetic Ciphers are not so strong enough since they are vulnerable to brute-force attacks [9].

3. PROPOSED SYSTEM

We propose a cryptographic substitution method called Color Coded Cryptography which modifies the “Play Color Cipher” [10]. This is a symmetrical system which implements encryption of text by converting it into colors. Each characters of the message is 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.

4. DESIGN AND IMPLEMENTATION

4.1 Algorithm

4.1.1 Encryption:

Step I: Accept the input text.
Step II: Separate the input text into individual characters.

Step III: Select one color-channel (R/G/B).

Step IV: Add the ASCII value of every character with its position and put the value in the selected color-channel.

Step V: For the remaining 2 channels, put the value of the color by the user.

Step VI: Draw the bitmap image.

Step VII: Generate the key

Step VIII: Send the image to the receiver.

4.1.2 Decryption:

Step I: Divide the received image into ‘n’ blocks

Step II: From each block color value subtract the key and block’s position

Step III: Convert the resulting value into character and get the text.

4.2 Flow Chart

4.2.1 Encryption

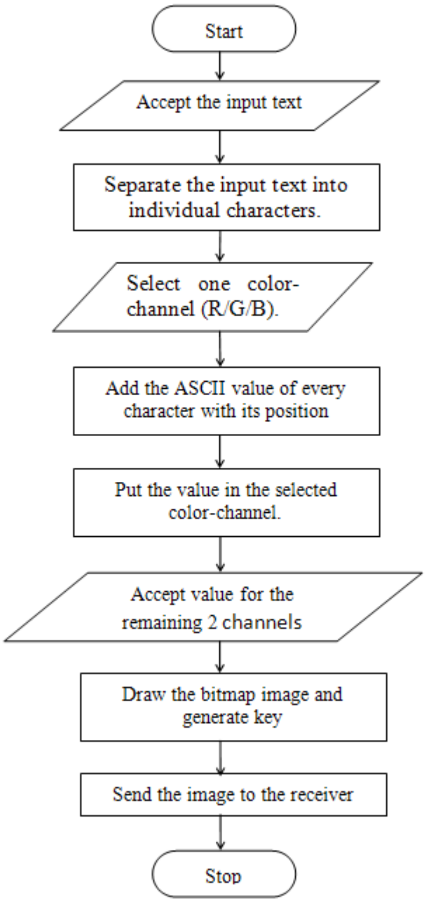
Start
Accept the input text
Separate the input text into individual characters.
Select one color-channel (R/G/B).
Add the ASCII value of every character with its position
Put the value in the selected color-channel.
Accept value for the remaining 2 channels
Draw the bitmap image and generate key
Send the image to the receiver
Stop

Fig 1: Flowchart of Encryption

4.2.2 Decryption

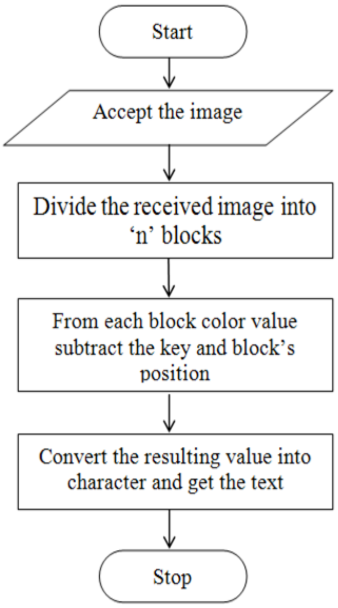
Start
Accept the image
Divide the received image into 'n' blocks
From each block color value subtract the key and block's position
Convert the resulting value into character and get the text
Stop

Fig 2: Flowchart of Decryption

4.2.3 Implementation

Fig 3 describes a working concept of proposed system

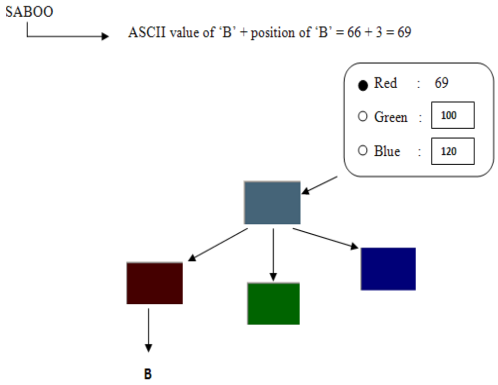

Fig 3: Representation of proposed system

4.2.3.1 Encryption

The user selects a color channel from given R, G or B and gives the values for remaining channels between range 0 to 255, it acts as a key. The input character is converted into ASCII value. This ASCII value and character position is assigned to selected channel. Now, from RGB values a color block is generated for that character. Like this all the characters are converted to color blocks and then single image is generated by placing together all the color blocks. Fig 1 shows the stepwise encryption process.

4.2.3.2 Decryption

The received image is divided into blocks. A center pixel from each block is extracted. From the selected pixel value, subtract the key which is used for encryption. Then subtract the position of block. Now the value is remain considered as an ASCII value. This ASCII values is then transformed back to its corresponding character. After extracting all characters, the original message is achieved. Fig 2 shows the stepwise decryption process.

5. CRYPTANALYSIS

Considering the application of this project which used the proposed cryptographic system. For color substitution only 3 parameters (Red, Green, or Blue) 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 [11]. It will be very tiring to try out all possible combinations. Hence it is safe to deduce that the brute force attack is not possible. Also, these are 16 millions 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.

6. FUTURE SCOPE

In future, the figures, tables, images, audio etc. can be included in the plaintext for conversion and hence the scope of the algorithm can be increased. With small changes, the same algorithm can be used for languages other than English as well.

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 topic shows that the cipher has great potential as it eliminates major attacks like brute force, man in middle etc.

8. ACKNOWLEDGMENTS

The co-authors of this paper express their gratitude to internal project guide or first author **Prof. Anand Bali** for valuable suggestions and constant encouragement for successful completion of the project.

The authors of this paper thanks to all other faculty and non-teaching staff members of our department for their support and peers for having stood by us to complete this project.

9. REFERENCES

[1] Maram Balajee, " UNICODE and Colors Integration tool for Encryption and Decryption", International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 3 Mar 2011.

[2] William Stallings, "Cryptography and Network Security, Principles and practice", 5th edition, 2008.

[3] R.L.Rivest, Shamir and Adleman, "A Method of Obtaining Digital Signatures and Public Key Cyryptosystems Laboratory for Computer Science", MIT Cambridge, 1978.

[4] B.A.Forouzan, "Cryptography and Network Security", 4th edition, 2008.

[5] Johan Hastad, "On using RSA with low exponent in a public key network", Advances in Cryptology- CRYPTO "85, LNCS 218, pp. 403-408 1986.

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

[7] 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 Accessed on 25/01/2016

[8] Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger, 2011, Biclique Cryptanalysis of the Full AES

[9] Debdeep Mukhopadhyay, IIT Kharagpur, http://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/FormalCrypto/slides/Introduction.pdf Accessed on 25/01/2016

[10] Prof. K. RavindraBabu, Dr.S.Udaya Kumar, Dr.A.VinayaBabu and Dr.Thirupathi Reddy, "A block cipher generation using color substitution",International Journal of Computer Applications Volume 1 – No. 28, 2010.

[11] Devyani Patil, Vishakha Nayak, Akshaya Sanghavi, Aparna Bannore, "Cryptography based on Color Substitution", International Journal of Computer Application Volume 91 – No.16, April 2014.