Colour Based Cryptography

Dinesh Sharma
Student of ACE
Mumbai,India

Rohit Prasad
Student of ACE
Mumbai,India

Gunraj Bedi
Student of ACE
Mumbai,India

Archita Dad
Assistant Prof. of ACE
Mumbai,India.

***Abstract*:- In the increasing concern of the data security ,most commonly method is encryption of messege to cipher text message ,which are based on various strategies to encode.traditional method is to convert the message to cipher text by substitution , swapping ,transposition etc. Transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. Whereas ,we are using an innovative cryptographic substitution method. where we 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.As there are n decillion of color with wide range of shades are available so the complexity for the attacker increase and that gives the assurance of strong cipher.**

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

1. INTRODUCTION

Information Security which refers to securing information in potentially hostile environments is a crucial factor in the growth of information-based processes in industry, business, and companies[1]. Cryptography is a key technology for achieving information security in the various aspects such as communications, computer systems, electronic commerce, and in the emerging information society[3]. Basically Cryptography requires some kind of mathematical processing in order to successfully encrypt or decrypt data.[2].Many Cryptographic terms has been developed throughout the year which have a great impact in the world of Cyber Security. Two types of Cryptographic algorithm are used throughout the world i.e:Public key Cryptography and Private Key Cryptography[4].DES is a Private key cipher algorithm, in which cryptographic key and algorithm are applied to the block simultaneously instead of one bit at a time. AES is also a private key cipher algorithm which is used to protect useful information and is implemented in software andhardware throughout the world to secure sensitive data.RSA is a Public key Cryptographic algorithm which is used for securing sensitive data with the help of two keys, when being sent over an insecure network such as the Internet[1]. There is also a Visual cryptography technique which allows pictures to be encrypted in such a way that decryption should be done via sight reading.

1.1. NEED

Existing Cryptographic algorithms are nowadays not enough to fully secure the information/files that should not be in the hands of the unauthorized people .There are many ways the data can be hacked or leaked by finding the loopholes or flaw in the data or the system even though they are encrypted. Brute force is a trial and error technique which helps to obtain user password or personal identification number of the system[4].The Meet-in-the-Middle attack is a type of attack where attacker targets the block cipher cryptographic function and applies the brute force technique to both the plaintext and the ciphertext block and then attempt to encrypt the plaintext according to the various key to achieve an intermediate ciphertext[7].Meet in the middle attack mainly gather the information but cannot change the information. A birthday attack is a type of cryptographic attack that can be used to abuse communication between two or more parties[2].The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations. DES uses a 64-bit key, but eight bits are used for parity checking, effectively limiting the key to 56-bits. Hence, it would take a maximum of 2^56 attempts to find the correct key which can be now done easily with the help of DES key generator software[5].Similarly AES keys depends on the rounds used in the process of encryption which can be very useful to the to attack if he/she knows the process. All of the above problems can be overcomed or can be reduced by using our technique. For this only 3 parameters (RGB) have been used where, each channel has a color range of 0-255[1]. Maximum number of color combinations is 1,67,77,216 in decimal. It will be very exhausting to try out all possible combinations. Hence that the brute force attack is not possible[3].

Also, there are 18 Decillions of colors in the world of computer. Thus, if man in the middle, known plain text, known cipher text attacks is considered, it will be impossible to guess or decrypt the plain text just by obtaining the color image[9].Also this technique will ensure the plaintext size reduced by 4 times in a lossless manner.

2. LITERATURE SURVEY

Sr no	Paper	Year	Description
1	Cryptography based on Color Substitution	April 2014	In this paper, an innovative cryptographic method is proposed to generate a stronger cipher the existing substitution algorithms. This method on the substitution of characters, numbers and symbols with color blocks.
2	Securing Informative Text using Color Visual cryptography.	February 2016	The aim of this project is to provide secure communication between two parties. So, that secret message/data cannot be compromise.
3	Extended Visual Cryptography for Color shares using Random Number Generators	August 2012	The concept of visual information pixel (VIP) synchronization and error diffusion is used to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality.

3.TECHNOLOGY USED

an object-oriented programming language known as **C#** having strong typing, essential, declarative, efficient, class-based is used to implement this research

4. WORKING

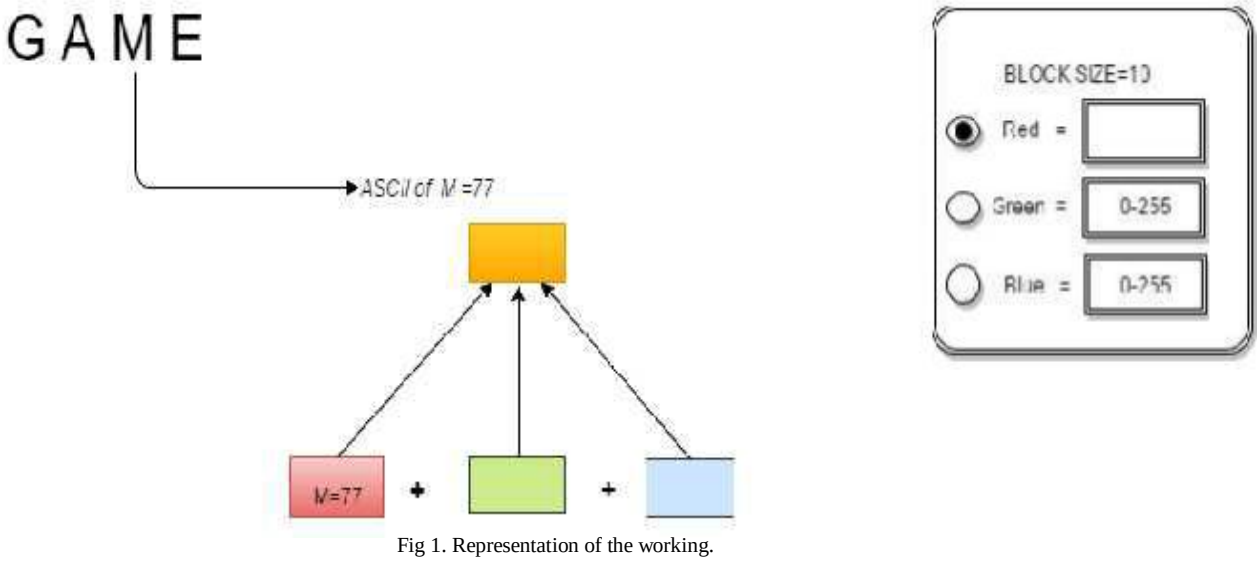

Fig 1. Representation of the working.

Fig 1. Shows the working pattern of our technique.In this we will create a Windows platform software that will convert the plain-text into the color block image which will be represented as a bitmap-Image

4.1 ALGORITHM

A] ENCRYPTION PART

1. Accept the text file and the key.
2. Separate the text into individual characters.
3. Specify the size of the block, color-channel (R/G/B) and a color (RGB value).
4. Depending on the block-size (say x), divide the picture box into a grid of blocks, each of size x
5. Add the ASCII value of every character and put the value in the color-channel that is selected.
6. For the remaining 2 channels, put the value of the Color from 0-255,This should be user input.
7. Originate the bitmap image
8. Generate the Key.
9. Send the image to the intended reciever

OUTPUT AFTER ENCRYPTION

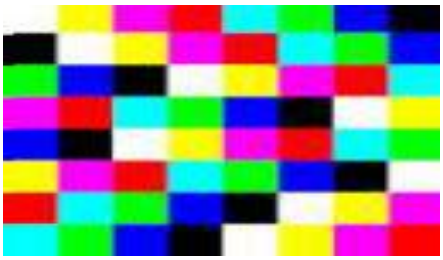

Fig2.Representation of output

Fig 2. Shows the output that is obtained after the encryption process.

B] DECRYPTION PART

1. Add the ASCII value of every character and put the value in the color-channel selected.
2. For the remaining channels, put the value of the Color that was given by the user.
3. Originate the bitmap image.
4. Generate the Key.
5. Send the image to the intended receiver.
6. Subtract the blocks position from that value.
7. Convert the resulting value into character and obtain the text.
8. Decrypt the text using the decryption process of the encryption algorithm used.
9. Get the original text back.

5. CONCLUSION

An innovative approach presented in this paper makes information secure by color substitution. The cryptanalysis carried out on this experiment shows that this technique 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 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 can be increased for generation of the color to get 18 Decillions of color combinations. This can be used for languages other than English by making some minor changes.

6. ACKNOWLEDGEMENT.

We Would like to express our gratitude to miss Archita Dad for her constant guidance and support also we would like to thank library and computer center department of our college who helped us to carry out our research.

.

7. 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,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 Vol- 1.
[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.
[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.
[6] Jay Hilyard and Stephen Teilbet, C# 3.0 Cookbook, 3rd edition, 2007.
[7] Nguyen, H. Number Theory and the RSA Public Key Cryptosystem.
[8] B.A.Forouzan, Cryptography and Network Security, 4th edition, 2008.
[9] Christian Gross, Beginning C# 2008 From Novice to Professional Second Edition 2008.