International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 1, December 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Color Cryptography using Substitution Method

Yashvanth. L[1], Dr. N. Shanmugapriya[2]

[1]MCA Student, [2]Assistant Professor,
[1,2]Department of Computer Application (PG),
[1,2]Dr. SNS Rajalakshimi College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT

In world of computer network, fears come in many different forms. Some of the most common fears today are software attacks. If we want to secure any type of data then we can use encryption method. All traditional encryption methods use substitution and switch. Substitution methods map plain text into ciphertext in which characters, numbers and special symbols are substituted with other characters, numbers and special symbols. In this paper, we are using a creative cryptographic replacement method is to generate a stronger cipher than the existing replacement algorithms. This method focuses on the replacement 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*

How to cite this paper: Yashvanth. L | Dr. N. Shanmugapriya "Color Cryptography using Substitution Method" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-1, December 2019, pp.98-100, URL: https://www.ijtsrd.com/papers/ijtsrd29360.pdf

IJTSRD29360

1. INTRODUCTION

Information security is the safety of information and minimises the risk of exposing information to unauthorised gatherings from expose, modification, and destruction of data. Cryptography is a method of storing and conducting data in a particular form so that only those for whom it is future can read and process it. The security of cipher text is totally dependent two things: the power of the cryptographic algorithm and the privacy of the key. Many researchers have adapted the existing algorithms to fulfil the need in the current market, yet the ciphers are weak to attacks.

2. LITERATURE SURVEY

2.1. Existing Cryptographic System

A. Traditional Symmetric-Key Ciphers

In symmetric key ciphers, plaintext is new into cipher-text using a shared secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is better from the cipher-text. The Secret Key is shared by both, the sender and the receiver which they must have create in a secure fashion & should keep the key unseen. These ciphers consist of Switch and Transposition ciphers. A Substitution cipher replaces one figure with another. A Transposition cipher rearranges the symbols .

B. 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 usages a k-bit key. A modern block cipher can be intended to act as a substitution cipher or a transposition cipher DES and AES are examples of this type of cryptography algorithm.

C. Asymmetric-Key Cryptography

Unequal cryptography or public-key cryptography is cryptography in which a couple of keys is used to encrypt and decrypt a message so that it spreads securely. In such type of cryptography worker who needs to send an encrypted message can grow the future recipient's public key from a public directory. They use this key to encrypt the message, and they refer it to the recipient. When the receiver gets the message, they decrypt it with their secluded key, which no one else should yield access to. RSA and Merkle–Hellman knapsack cryptosystem is the most commonly used irregular key algorithm. The security of RSA relies on the difficulty of factoring huge numbers.

2.2. Threats and vulnerabilities in existing systems

RSA is occupied on the improper growth of two prime facts. Hence, number factorization is a grave intimidating in error of RSA and currently different kinds of spells have identified against RSA by cryptanalysis. Most spells seem to be the effect of waste of the scheme or evil choice of parameters. Substitution methods like Caesar Cipher, Mono alphabetic Cipher, play just Cipher and Poly alphabetic Ciphers are not strong enough since they are weedy to brute-force spells.

3. PROPOSED CRYPTOGRAPHIC SYSTEM

Green and blue (RGB). The user must specify the standards for the R, G and B channels among the ranges 0-255. Too a block size of color block requests to be detailed. We propose a cryptographic substitution method which alters the "Play Color Cipher" that is called as color coded cryptography.
This system is constructed on symmetric encryption which is applied by encrypting text into color image. Each troposphere of the message is encrypted into a section of color. Every character will be swapped by a different colour block. The inverse process is used to produce the original text from color block at the earpiece side. The user enters a message which is the plaintext spring side. A channel needs to be special from the three color channels i.e. red

All the characters of the text are then converted to color blocks formed by joining 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 certain 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 removed and then converted to a plaintext character. This is done for all blocks and the matching characters are removed.

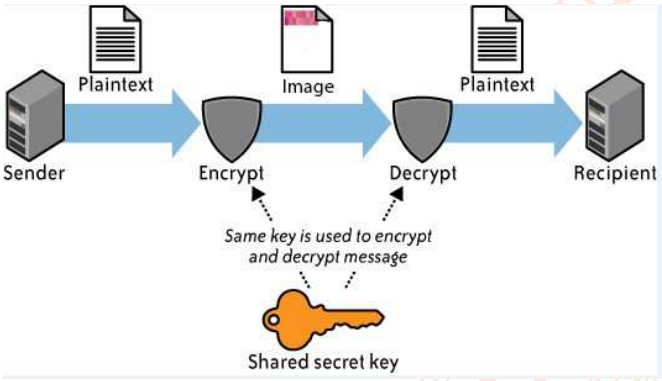

Fig 1: Block Diagram

3.1. Advantages of proposed system

Each character current in the plaintext is replaced with a color block from the available 18 Decillions of colors in the creation and at the getting end the encryption text block (in color) is decrypted in to plain text block. It stops against problems like Meet in the mid attack, Birthday outbreak and Brute force outbreaks.

4. ALGORITHM

4.1. Encryption.

- Receive the input text file and the key.
- Isolated the input text into isolated fonts. Input the color-channel (R/G/B) and a color (RGB value).
- Undefined on the predefined block-size (say n), divide the copy box into a web of blocks, each of extent.
- Rise the ASCII charge of every paradise with key and put the charge in the colour-channel chosen.
- For the remaining 2 channels, put the value of the Color inside by the user.
- Pull the bitmap image.
- Create the Key.
- Send the image to the telephone.

4.2. Decryption

- Receiver obtains the image and the key.
- Divide the colour copy into color slabs giving to block size definite into the key.
- Get the charge of separate colour block and withdraw the key from that value.
- Convert the resulting value into attractiveness and become the writing.
- Decrypt the text using the decryption process of the normal encryption process used.
- Get the unique writing posterior.

5. IMPLEMENTATION

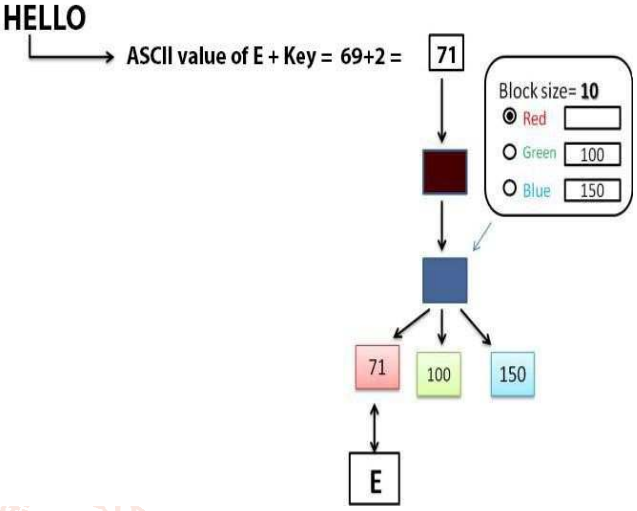

Fig 2: describes a working of this concept.

5.1. Encryption

1. The user chooses a one color network (R, G or B) and springs the ideals for outstanding two networks among the arrays 0-255. The atmosphere is changed to its ASCII charge and allocated to the designated color channel. Also, a block scope larger than 0, is stated by the user. Colour is given to the color slab of the sure slab extent is then shaped by joining the values of all three networks.

2. Key Generation
The color channel selected and the color block size systems the key.

3. Image Generation
All the characters are changed to color blocks and then a only image is produced by merging all the color slabs of.

5.2. Decryption

1. Getting copy and common hide key
The section size and the colour network are removed from the common hide key.

2. Extracting of pixel value from the image
The established image is separated into blocks of the size stated in the key. A pixel and its 4-nearest neighbour pixels from each wedge are removed and the most shared pixel value is particular. This is to recover the strength of the procedure in the situation of company of noise.

3. Retrieval of the plaintext
From the designated pixel value, the section charge of the particular network is occupied (R, G or B component) and careful as an ASCII value. This ASCII value is before renewed to its agreeing heaven likewise for all additional color blocks. After removing all such characters, the unique communication is saved.

6. Technology used

A. C#.net

C# is a jazzy and nature-safe article situated language that enables makers to manufacture an unrest of sheltered and lively applications that course on the .NET Framework. You can use C# to make Windows customer applications, XML Web administrations, spread apparatuses, customer server applications, database applications, and bountiful, plentiful extra. C# grammar is exceptionally expressive, yet it is likewise basic and simple to learn. The wavy-brace syntax of C# will be instantly recognizable to anyone familiar with C, C++ or Java [8] [9].

7. APPLICATION

This arrangement of shading cryptography can be utilized for validation of login frameworks. During the enlistment procedure, the new client will enter his own subtleties and the secret word. The secret key is then scrambled into a shading coded picture utilizing the proposed shading substitution calculation. The picture is then put away at the server. At the hour of login, the client enters the username and secret key. In view of the username, relating picture of the secret key is recovered from server, decoded and changed over to content. This content is then coordinated with the secret phrase entered by the client. In the event that it coordinates, the client effectively signs in. The key for encryption and unscrambling can be founded on the parameters of the individual subtleties entered by the client. Numerical capacities performed on the timestamp of enrollment and user‟s date of birth can produce a key. In this manner, the requirement for capacity of key is disposed of

8. CONCLUSION

The present standard cryptographic strategies are dependent upon an assortment of assaults. A creative methodology exhibited and executed in this paper makes data secure by shading substitution. In future, the figures, tables, pictures, and so forth can be incorporated into the plaintext for transformation and subsequently the extent of the calculation can be expanded.

9. REFERENCES

[1] Aditya gaitonde 2016. Color Coded Cryptography, International Journal of Scientific & Engineering Research, Volume 3, Issue 7.

[2] Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger, 2015, Biclique Cryptanalysis of the Full AES, Crypto 2015 cryptology conference, Santa Barbara, California.

[3] Prof. K. Ravindra Babu, Dr. S. Udaya Kumar, Dr. A. Vinaya Babu and Dr. Thirupathi Reddy, 2017. 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, 2016. 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, 2017. “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, 2017.