HIDING DATA USING COLOR BASED CRYPTOGRAPHY

K.Bergin Shyni
Assistant Professor
Dr.Sivanthi Aditanar College of Engineering, Tiruchendur.

ABSTRACT

The threats to information security are increasing at very rapidly. The most effective and universal approach to counter such threats is encryption. In Traditional encryption techniques substitution and transposition is used. In Substitution techniques plaintext is mapped into cipher text. In all traditional substitution techniques plaintext characters, numbers and special symbols are substituted with another characters, numbers and special symbols. In this new method an innovative cryptographic substitution is proposed to generate a stronger cipher than the existing substitution algorithms. This method focus on the substitution of characters, numbers and special symbols with color blocks. This algorithm of substitution is based on Play Color Cipher. This is a symmetrical system which is implemented by encryption of text by converting it into colors. Each character of the plaintext is encrypted into a block of color. Every character will be substituted by a different color block. To produce the original text, inverse process is used using color block, to ensure more security the color blocks is hidden by a cover image.

1.1 INTRODUCTION:

Information security is the protection of information and minimizes the risk of exposing information to unauthorized 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.

Color Coded Encryption is a technique of implementing a symmetrical system for security purpose. The symmetrical system is implemented by encryption of text by converting it into image format. To reduce the size of the image file, compression algorithms are to be implemented at the encryption stage. The converse process is used to generate at the destination system to recover the data in the original format.

A cryptographic substitution strategy called Color coded cryptography which adjusts the "Play Color Cipher". This algorithm alters the plain text in various ways before it takes the shape of cipher text. This is a symmetrical framework which is executed by encryption of text by changing it into color blocks. Every character of the message is encoded into a block of color. Each character will be substituted by an alternate color block.

At the receivers side reverse procedure is utilized to get the original text. Here, in our system symmetric key cryptography has been utilized. Our system will have support for multiple languages. On a fundamental level, Translator perform straightforward substitution of words in one language for words in another, enhancing yield by restricting the extent of passable substitutions.

2.1 EXISTING SYSTEM

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 &amp; should keep the key hidden. These ciphers consist of Substitution and Transposition ciphers. A Substitution cipher replaces one symbol with another. A Transposition cipher reorders the symbols.

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.

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 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.

2.2 PROPOSED SYSTEM

A cryptographic substitution method is proposed which modifies the "Play Color Cipher" that is called as Color coded cryptography. 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.

2.2.1 SYSTEM ARCHITECTURE

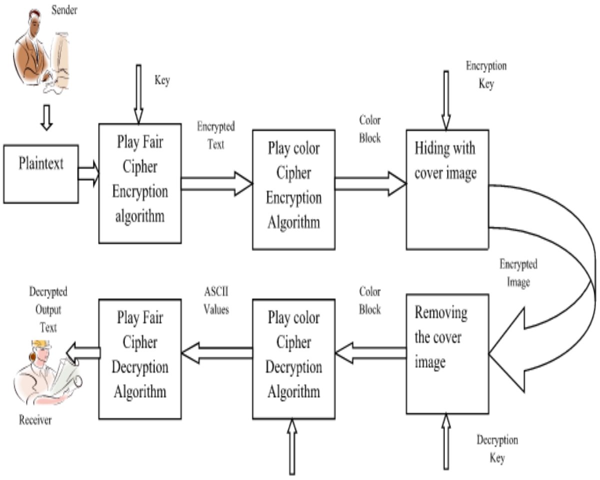


Fig.2.2.1 Architecture diagram

3.1 ENCRYPTION

First accept the input text and the key. Encrypt the text using play fair cipher. Separate the encrypted text into individual characters .Find the ASCII value of each character (say x).Then find the position of every character (say y). Add position value and ASCII of every characters (i.e. x + y=z).Then in the color channels R, G, B the value of z is assigned to any one of the channel, remaining two will be inbuilt.

Then add the values of R, G, B to produce a color, which will be assigned to the respective character .Now the text will be converted into color blocks. The color blocks are hidden using cover image.

3.2 DECRYPTION

The received cover image is separated into image and color blocks .The separated color block is splitted into individual color block .Get the value of individual color block and subtract the key from that value. Find the ASCII value of each character (say x).

Then find the position of every character (say y).Subtract position value and ASCII of every character to get an encrypted text. Using play fair cipher algorithm, the encrypted text is decrypted .The original text is obtained.

4.1 SCREENSHOTS

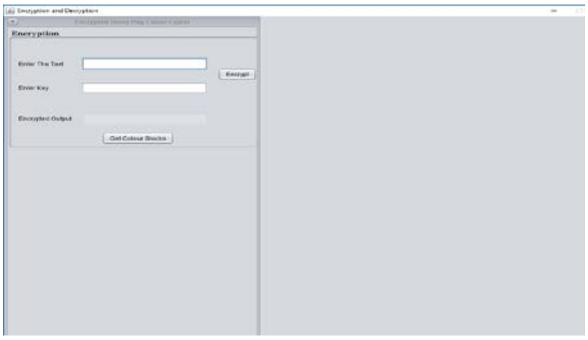
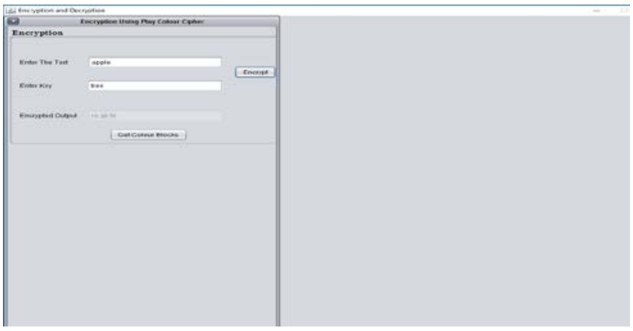
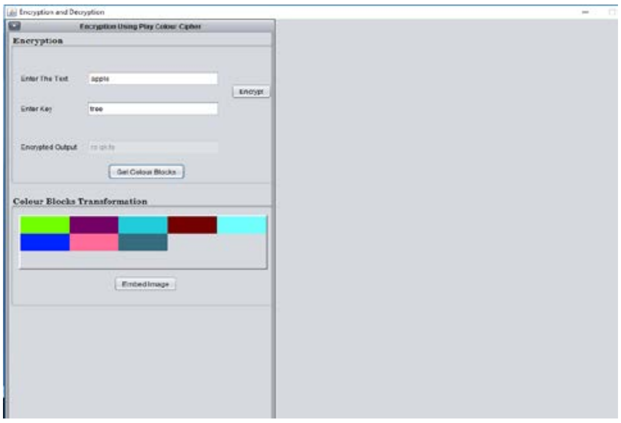


Fig.4.1.1 Screenshot indicating the user to input the plain text and key


Encryption and Decryption
Encryption Using Play Colour Cipher
Encryption
Encrypt
Get Colour Blocks

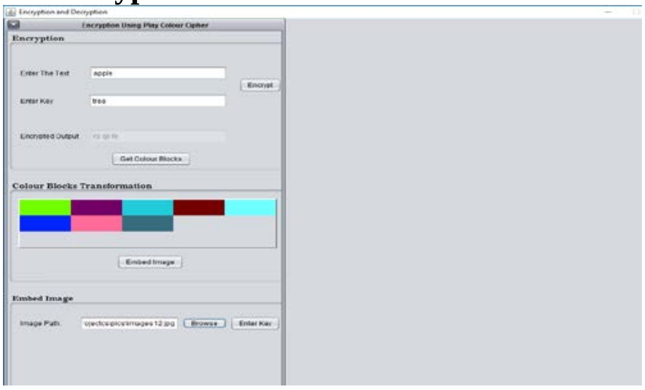
Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe

Fig.4.1.2 Screen showing the encrypted text.


Encryption and Decryption
Encryption Using Play Colour Cipher
Encryption
Encrypt
Get Colour Blocks
Colour Blocks Transformation
Embed Image

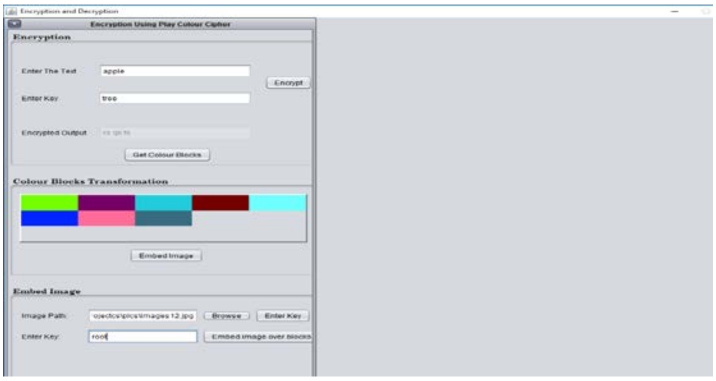
Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe

Fig.4.1.3 Color blocks transformation from the encrypted text


Encryption and Decryption
Encryption Using Play Colour Cipher
Encryption
Encrypt
Get Colour Blocks
Colour Blocks Transformation
Embed Image
Embed Image
Browse
Enter Key

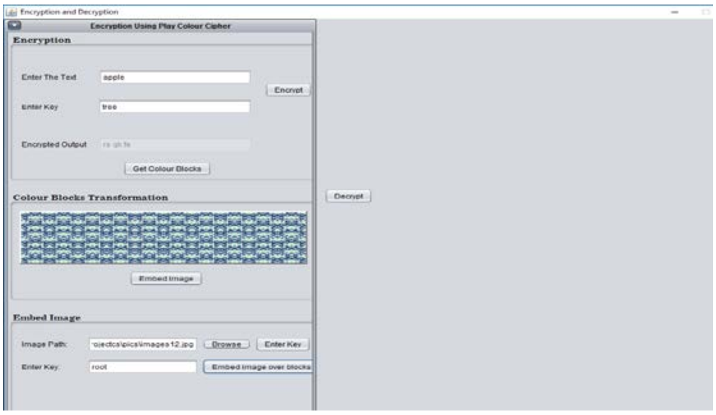
Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe
Image Path: ojects\pics\images12.jpg

Fig.4.1.4 Selecting the path of the image to hide the colour blocks.



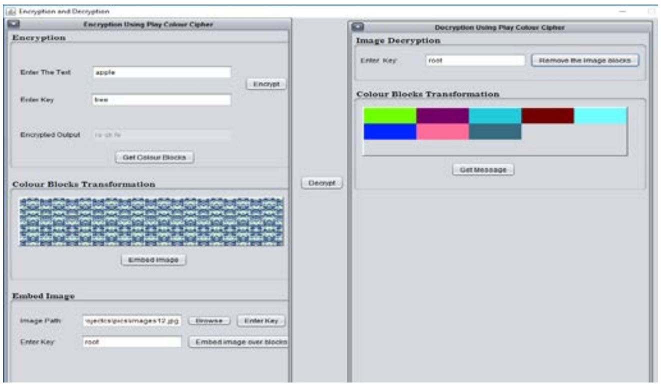
Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe
Image Path: ojects\pics\images12.jpg
Enter Key: root

Fig.4.1.5 Output screen indicating the user for a key to hide color block in image



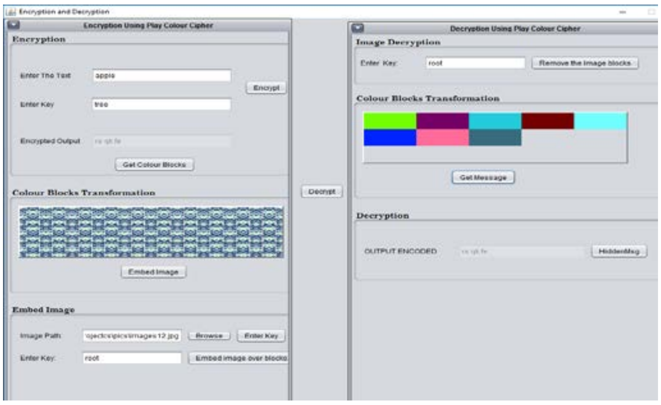
Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe
Image Path: ojects\pics\images12.jpg
Enter Key: root

Fig.4.1.6 The output screen after encryption.


Encryption and Decryption
Encryption Using Play Colour Cipher
Encryption
Encrypt
Get Colour Blocks
Colour Blocks Transformation
Embed Image
Embed Image
Browse
Enter Key
Embed image over blocks
Decrypt
Decryption Using Play Colour Cipher
Image Decryption
Remove the image blocks
Colour Blocks Transformation
Get Message

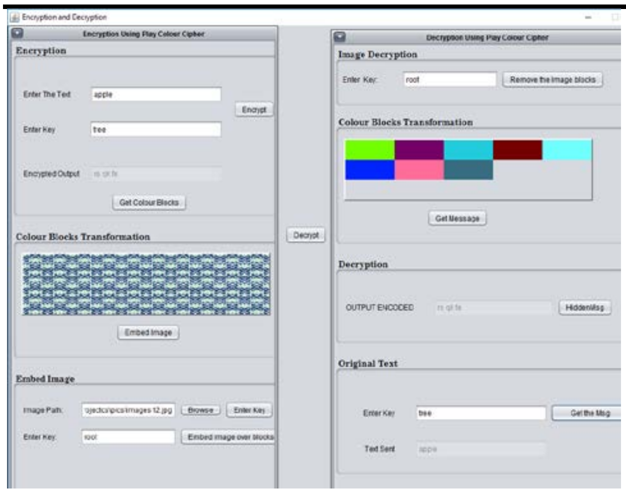
Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe
Image Path: ojects\pics\images12.jpg
Enter Key: root
Enter Key: root

Fig.4.1.7 Entering key to decrypt the color block from image.



Enter The Text: apple
Enter Key: tree
Encrypted Output: rs qh fe
Image Path: ojects\pics\images12.jpg
Enter Key: root
Enter Key: root
OUTPUT ENCODED: rs qh fe

Fig.4.1.8 The output screen showing the decrypted cipher text from color block.



Enter The Text: apple
Enter Key: tree
Encrypted Output: rs ql fe
Image Path: ojects\pics\images 12.jpg
Enter Key: root

Enter Key: root
OUTPUT ENCODED: rs ql fe
Enter Key: tree
Text Sent: apple

Fig.4.1.9 Finally the user entered text is decrypted.

4.2 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.

4.3 FUTURE ENHANCEMENT

In future, 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.

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.

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 CryptologyCRYPTO "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.