

Color Coded Encryption Based on Chatting Application

Rubnar I. Lanjekar, Pournima S.Nevarekar

Department of Computer Engineering, RMCET Engineering College, Ambav, Maharashtra, India

ABSTRACT: Nowadays different encryption algorithms are used for data security. Some of them are RSA, Blowfish, AES etc. All of these traditional algorithms deal with substituting plaintext with cipher text. As cipher text consists of different characters, symbols and numbers, it is possible to decrypt the text using cryptanalysis. One of the strongest encryption algorithms is color coded encryption in which plain text is converted into a bitmap image of color pixels. As the time required for forming bitmap image may get increased as the text size increases, we are proposing a system in which this time will get reduced. In the proposed system, instead of forming bitmap image, arrays of color pixels will be transferred to the receiver side. They will be decrypted and plain text will be available for the user resulting in minimizing the encryption time with maximizing the security. We will apply this modified play color cipher algorithm on chatting application for providing maximum security to the user.

KEYWORDS: Cryptography, colorcoded, PlayColorCipher, Cryptanalysis.

I. INTRODUCTION

In these days of increasing socialization, privacy and security have become a big issue. Many social networking sites and applications claim to provide privacy using different encryption algorithms such as RSA, Blowfish, AES etc. One of them is color coded encryption in which plain text is converted into color pixels. By using these color pixels, the bitmap image is formed. This image is sent to the receiver. At the receiver side, bitmap image gets decrypted and the original message is displayed to the receiver. The major drawback of this current system is time required for forming a bitmap image. If the text size is larger then we have to wait till all the characters get converted to color pixels which will result in a delay in formation of the bitmap image. Thus, to overcome this drawback, we will modify the existing algorithm. Rather than waiting for bitmap image to be formed, we will transfer the arrays of pixels to the receiver, reducing the time required for forming a bitmap image. The array of pixels will get decrypted at the receiver side and original message will be available for the receiver. This proposed system will be more secure. It will be harder for any attacker to decrypt the encoded text messages as 18 decillion colors are available for formation of pixels.

II. RELATED WORK

In paper [1] and [3] different existing cryptographic systems have been explained such as traditional symmetric key cryptography, modern symmetric key cryptography, asymmetric key cryptography etc. As these all algorithms substitute alphabets with another alphabet, cryptanalysis becomes easy. To avoid this, play color cipher algorithm has been used which will replace each alphabet by color block. Here cryptanalysis becomes difficult as there are nearly 18 decillion colors are available.

Paper [1] uses symmetric key cryptography based play color cipher algorithm where key is formed by using block size and color channel entered by the user. Each character is encrypted into block of color where blocksize is as specified by the user. Bitmap image is formed by using all the color blocks and this image is sent at the receiver side. At receiver side image is divided into blocks of size as specified in key. For each block Centre pixel is extracted and it is converted into character. In this way all the characters are extracted and original message is retrieved.

Paper [2] gives the Multilanguage support where if the input text message is in Hindi language then it will be first translated into English and then encryption algorithm will be applied on it. The main difference is, they use PCC encryption algorithm for generating cipher image and key is encrypted using RSA algorithm. This helps in generating asymmetric key which provides more security. At receiver side, reverse process is applied to get the original message.

Paper [3] uses same method as that of [1]. For decryption at receiver side, from each block Centre pixel and it's four nearest neighbor pixels are extracted. This helps to improve robustness in case noise is present.

III. EXISTING SYSTEM

1] In paper [1], first convert the character into color block using generated the key. All the characters are converted to color blocks and single image (bitmap image) is generated. At the receiver side the block size and the color channel are extracted from the key. Then extract the pixel value from each block and then the original message is retrieved.

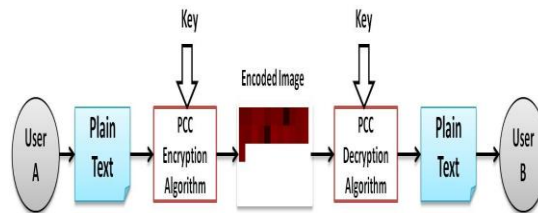


Figure 1: Block Diagram of Existing System

2] Another technique is used in [2] is, if sender sends the message in Hindi language then first this message translated in English using translator. Select R, G and B values. ASCII value of each character is added with its position and color block is formed. On this color block apply the play color cipher algorithm with RSA key. It produces the cipher image and sends to the receiver.

IV. PROPOSED SYSTEM

In proposed system at sender side, sender will send the text in human readable format (i.e. written in English language). After that in background the encryption algorithm will be used to encrypt that plaintext. Also, the value of key will be set at the encryption time. Using the ASCII value, position of character and the value of key each character will get encrypted in color pixel format. The encrypted data and the key value will be send to the receiver side as shown in below block diagram.

At receiver side, the decryption algorithm will be used for retrieving actual text send by sender. Using decryption algorithm, the encoded text will get converted to the plaintext (original text message) and receiver can read that message easily.

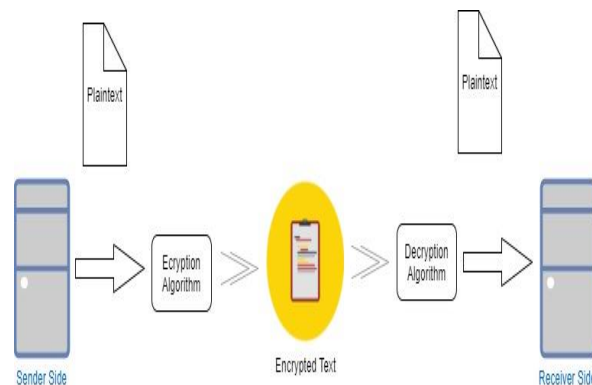


Figure 2: Block Diagram

Above block diagram describes the working of proposed system. The sender will send the message in plain text format which will be encrypted in hexadecimal format. This encrypted message will be send at the receiver side and will get decrypted to original text. This original message will be displayed to user.

V. PROPOSED ALGORITHM

A. ENCRYPTION

- Accept the input text file.
- Set the key for G and B channel for RGB model ranging between 0 to 255.
- Separate the text message into characters and store it in an array.
- For each character generate pixel value based on ASCII value and position in an array.
- Generate the array of pixels
- Transfer it to the receiver side.

B. DECRYPTION

- Accept the encrypted message in the form of array of pixels.
- Find the value of R channel (in RGB) based on key value.
- Decrypt the pixel value using R channel value and position from the array.
- Retrieve the actual character for each pixel.
- Get the original plaintext

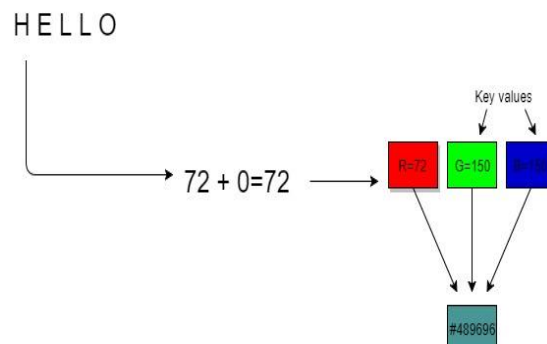


Figure 3 Example of Encryption

As shown in above figure, the message will get encrypted. The ascii value of H is 72 and position of H is 0th. Thus, the value of H will become 72. It will get converted into hexadecimal format. The hexadecimal value of H is 48 whereas the hexadecimal value of G and B channel is 96. Thus, the final hexadecimal value for letter H becomes #489696. In similar way, whole text will get encrypted.

VI. IMPLEMENTATION

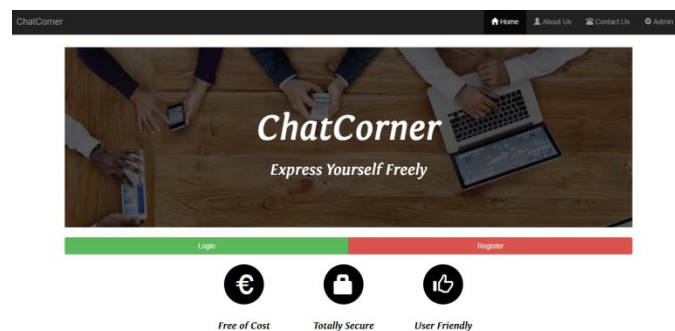


Figure 4 Homepage of Chatting Application

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 6, Issue 1, January 2019

The above figure describes the homepage of developed chatting application named as Chat Corner. As shown in above figure, the homepage of chatting application contains the link for login and register page. Also, the navigation menu contains home, about us, contact us and admin panel menus.

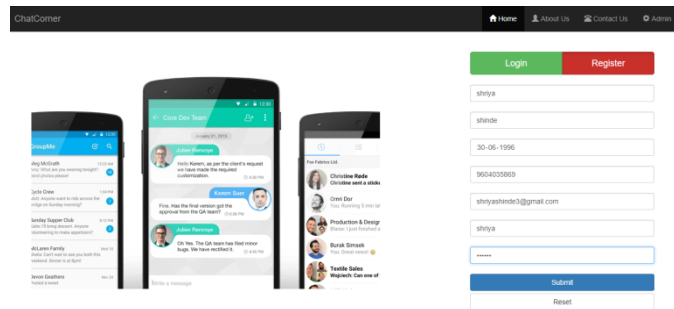


Figure 5 Register Page of Chatting Application

As shown in above figure, the register page contains different fields such as first name, last name, username, password etc. After successful registration, user will be directed to login page.

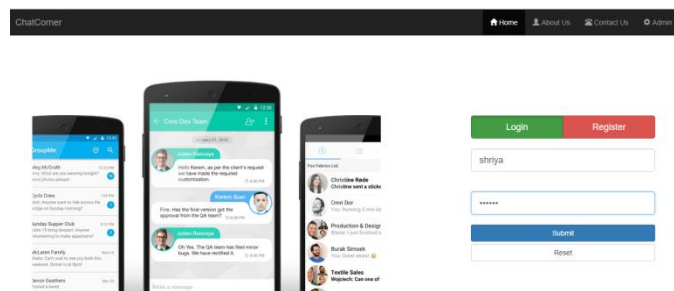


Figure 6 Login Page of Chatting Application

The above login page contains the different fields for login such as username and password. After successful login user will be directed to chat window. If wrong credentials are entered then user will be restricted from logging in to the system.

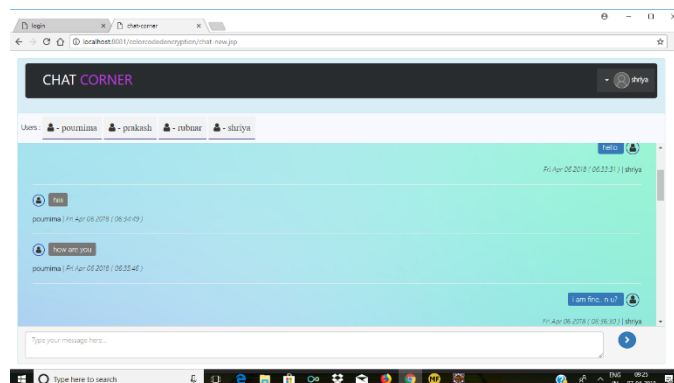


Figure 7 Chat Window

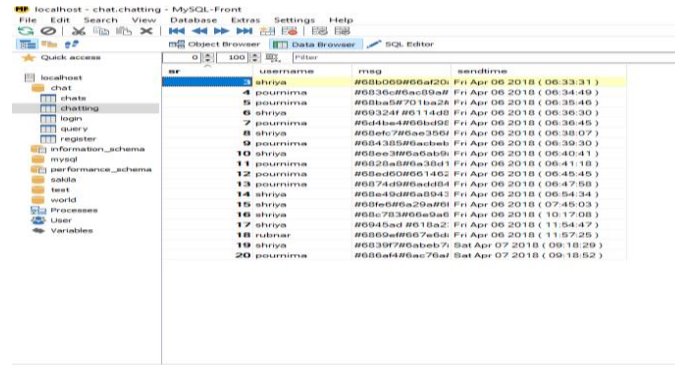
After successful login, user can chat with other members. Along with message, details such as send time, date and day will be displayed. Basically, it is online chat room where any registered member can chat with any other registered member.

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 6, Issue 1, January 2019



sr	username	msg	sendtime
1	shriya	#0000000000000000	Fri Apr 06 2018 (06:33:31)
2	pournima	#0000000000000000	Fri Apr 06 2018 (06:34:49)
3	pournima	#0000000000000000	Fri Apr 06 2018 (06:35:49)
4	shriya	#0000000000000000	Fri Apr 06 2018 (06:36:30)
5	pournima	#0000000000000000	Fri Apr 06 2018 (06:36:45)
6	shriya	#0000000000000000	Fri Apr 06 2018 (06:36:45)
7	pournima	#0000000000000000	Fri Apr 06 2018 (06:36:45)
8	shriya	#0000000000000000	Fri Apr 06 2018 (06:36:45)
9	pournima	#0000000000000000	Fri Apr 06 2018 (06:36:45)
10	shriya	#0000000000000000	Fri Apr 06 2018 (06:40:41)
11	pournima	#0000000000000000	Fri Apr 06 2018 (06:41:18)
12	pournima	#0000000000000000	Fri Apr 06 2018 (06:45:45)
13	pournima	#0000000000000000	Fri Apr 06 2018 (06:47:58)
14	shriya	#0000000000000000	Fri Apr 06 2018 (06:54:34)
15	shriya	#0000000000000000	Fri Apr 06 2018 (07:45:03)
16	shriya	#0000000000000000	Fri Apr 06 2018 (10:17:08)
17	shriya	#0000000000000000	Fri Apr 06 2018 (11:54:47)
18	rubnar	#0000000000000000	Fri Apr 06 2018 (11:57:25)
19	shriya	#0000000000000000	Sat Apr 07 2018 (09:18:28)
20	pournima	#0000000000000000	Sat Apr 07 2018 (09:18:52)

Figure 8 Encrypted Messages in Database

As shown in above figure, all the messages will be stored in encrypted format. As the messages are in hexadecimal format, it will be hard for any attacker to decrypt the messages. This will result in more secure system.

VII. CONCLUSION

Thus, here we conclude that our proposed system will provide maximum security as data will be encrypted in color pixels instead of cipher text. The system will be less vulnerable to attacks like Brute Force attack, Man in the middle attack, Birthday attack etc. Also, it will reduce the time required for generation of encrypted data.

REFERENCES

- [1] Devyani Patil, VishakhaNayar, AkshayaSanghavi, Aparna Bannore, "Cryptography based on color substitution", International Journal of Computer Application "(0975-8887) Volume 91No. 16, April,2014
- [2] Monica Kanchan, Avinash Shah, Jayesh Gupta, SunitaNaik, "Advance Cryptography using Color Code based Substitution with Multi-Language Support", International Journal of Computer Application (0975-8887) The National Conference on Role of Engineers in National Building
- [3] Manali Naik, PushpanjaliTungare, Pooja Kamble, ShirishSubnis, "Color Cryptography using Substitution methods", International Research Journal of Engineering and Technology(IRJET)Volume: 03 Issue: 03|Mar-2016
- [4] Prof. K. Ravindra Babu, 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.
- [5] Sastry V.U.K, S. Udaya Kumar and A. Vinaya babu, "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): 698703,2006.
- [6] Pritha Johar, Santosh Easo and K KJohar, "A Novel Approach to Substitution Play Color Cipher", International Journal of Next Generation Computer Application Volume 1- Issue 2,2012.
- [7] Aditya gaitonde, "Color Coded Cryptography", International Journal of Scientific & Engineering Research, Volume 3, Issue 7,2012.
- [8] Sastry V.U.K, S. Udaya Kumar and A. Vinaya babu, "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, 2006.
- [9] Rami El Sawda, Habib Hamam, "RGB Coloured Image Encryption Processes Using Several Colored Keys Images" – IEEE Research Paper
- [10] Rajesh N, Sushmashree S, Varshini V, Bhavani N B, Pradeep D, "Color Code Based Authentication And Encryption", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015
- [11] Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.
- [12] Renaud, "Evaluating authentication mechanisms," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, ch. 6, pp. 103–128,2005.