ISSN 2348 – 9928
IJAICT Volume 5, Issue 4, April 2018 Doi:01.0401/ijaict.2015.11.06 Published on 05 (04) 2018

A SURVEY ON HIGH LEVEL DATA SECURITY USING RGB COLOR AND ARMSTRONG NUMBER

Vedvati Kulkarni ***Ashwinee Dandawate*** ***Suraj Bajaj*** ***Priyanka Dumbre***

Marathwada Mitra Mandal's College of Engineering,
Pune, India

Abstract— Use of internet is one of the best modern ways of communication in Information Technology. But sharing of data through the network may cause some issues regarding the security concern. Confidential and crucial data sharing through the network has become so risky because of the hackers or intruders attack on the data through the hacking improved hacking technologies. It requires security. Cryptography is generally used for the security purpose in which encryption and decryption is used for converting the data into cipher text and extracting it into the original format. In this paper the combination of three color values are used to provide authentication for the password and the data is encrypted using the Armstrong number on which RGB values are applied for high level security. Merging of the two will provide two level securities and the crucial data to be send will be more secure. Unless and until the hacker knows both the values he\she will not be able to get the actual data in the decrypted format. Here password as well as data will be encrypted for the security purpose. The concept of Armstrong number is one of the best ways to achieve security. User can easily send the important data through the network as it provides high level security. The algorithm for Armstrong number and RGB values for the encryption and decryption is explained in the paper which can help to secure the confidential data in the fields like banking sector where data confidentiality plays an important role.

Keywords— RGB color value, Armstrong Number, Cryptography, Data security.

I. INTRODUCTION

Exchange of data through the network is very popular now a days but the security is one of the major aspect of this communication. The data may get hacked by the intruder, hacker or the people having access to such credential data. The basic technique used for the security purpose is cryptography; but the general techniques are known to the hackers as their experience and knowledge is increasing day by day. They are becoming powerful and more active [1][2][3].

The technique cryptography consist of two terms

1.1 Encryption

Encryption is nothing but converting the original form of data into the encoded format keys on it to keep the third party people away from the important and confidential data.

1.2 Decryption

The term decryption refers to converting the encoded format of data into the original one which is readable by the user by applying the same key or different key which was applied while encryption.

II. PROPOSED SYSTEM

2.1 Armstrong Number

An Armstrong number of three digits is an integer such that the sum of the cubes of its digits is equal to the number itself. For example, 371 is an Armstrong number since 3**3 + 7**3 + 1**3 = 371.

2.2 RGB Color Model

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and blue [4][5][6].

2.3 *Data Encryption Standard (DES)*

The Data Encryption Standard (DES) algorithm is a block of cipher that transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. The DES algorithm is widely used and is still considered reasonably secure.

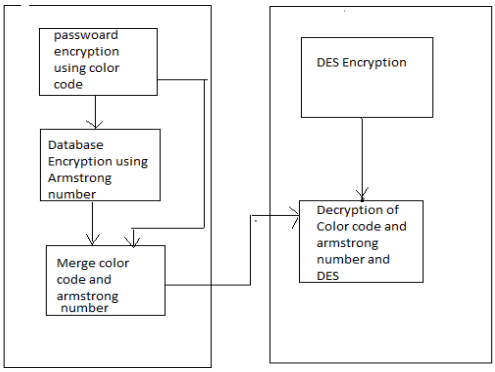

Fig 1: System Architecture

2.4 Algorithm Description

Actual working of algorithm is given below:

Lets consider A & B who want to transfer data. A is sender while B is receiver.

Sender side :

A has to transfer data to B. B has already allocated the RGB color values along with the key values.

Encryption of color which is Red(1,0,0).The key values are suppose (20,-10,10)

Step 1:

```
   1    0   0
  20  -10  10
-------------
  21  -10  10
```

This will give the encrypted format of the actual password.

Encryption of actual data:

Lets assume the data to be transmitted is CRYPTOGRAPHY.

Step 1: Convert the data into its ASCII values.

C	R	Y	P	T	O	G	R	A	P	H	Y
67	82	89	80	84	79	71	82	65	80	72	89

Let the Armstrong number be 153.

Step 2: The digits of Armstrong number will get added into the ASCII values if data.

```
     67  82  89  80  84  79  71   82  65  80  72  89
(+)  1   5   3   1   25  9   1   125  27  1   5   3
-------------------------------------------------------
 68  87  92  81  109 88  72  207  92  81  77  92
```

Step 3: Given values will be converted into matrix format.

$$X = \begin{bmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 82 & 92 & 92 \end{bmatrix}$$

Step 4**:** Encoded matrix will be formed using Armstrong number.

$$Y = \begin{pmatrix} 1 & 5 & 3 \\ 1 & 25 & 9 \\ 1 & 125 & 27 \end{pmatrix}$$

Step 5: Multiplication of matrix X & Y will be performed for encryption purpose.

$$Z = Y*X = \begin{pmatrix} 779 & 890 & 1383 & 742 \\ 3071 & 3598 & 6075 & 2834 \\ 13427 & 16082 & 28431 & 12190 \end{pmatrix}$$

Output will be encrypted data.

779, 3071, 13427, 890, 3598, 16082, 1383, 6075, 28431, 742, 2834, 12190

Step 6: To perform two level security the RGB color value will get added into the encrypted data.

779 3071 13427 890 3598 16082 1383 6075 28431 742 2834 12190

(+)1 0 0 1 0 0 1 0 0 1 0 0

780 3071 13427 891 3598 16082 1384 6075 28431 743 2834 12190

Receiver Side:

Decryption of password

As B already knows his/her RGB color value and the key value, he/she will subtract the given key values from the received color values.

Step 1:

```
      21  -10   10
(-)   20  -10   10
-----------------
       1    0    0
```

If the decrypted values are matching with A's database then B can proceed to decrypt the actual data.

Decryption of data

Step 1: B will subtract the key values from the encrypted data.

780 3071 13427 891 3598 16082 1384 6075 28431 743 2834 12190

(-) 1 0 0 1 0 0 1 0 0 1 0 0

779 3071 13427 890 3598 16082 1383 6075 28431 742 2834 12190

Step 2: Matrix will be formed for data.

$$Z = \begin{pmatrix} 779 & 890 & 1383 & 742 \\ 3071 & 3598 & 6075 & 2834 \\ 13427 & 16082 & 28431 & 12190 \end{pmatrix}$$

Step 3: Inverse of encoding matrix will be formed.

$$(-1/240) * \begin{pmatrix} -450 & 240 & -30 \\ -18 & 24 & -6 \\ 100 & -120 & 2 \end{pmatrix}$$

Step 4: Multiply the matrix by inverse matrix to get original message.

$$\begin{pmatrix} 68 & 81 & 72 & 81 \\ 87 & 109 & 207 & 77 \\ 92 & 82 & 92 & 92 \end{pmatrix}$$

Step 5: Values of Armstrong number will get subtracted from the data.

	68	87	92	81	109	88	72	207	92	81	77	92
(-)	1	5	3	1	25	9	1	125	27	1	5	3
	67	82	89	80	84	79	71	82	65	80	72	89

Step 6: Convert the data into original message from given ASCII values.

67	82	89	80	84	79	71	82	65	80	72	89
C	R	Y	P	T	O	G	R	A	P	H	Y

Table-1: Comparison between Armstrong and DES algorithm.

Parameter	Armstrong Number	DES
Number	Armstrong Number along with RGB values is used.	Prime Numbers are used.
Validation	Checks validation after login.	No validation after login.
Authentication	Password and color is used for authentication.	Password is used for authentication.
Security	Password itself is secured using color and data is secured by using Armstrong Number and RGB color.	Encryption and Decryption.

III. PROJECT SCOPE

In the proposed system we will be developing the high level security to database. UsingColor code and Armstrong Number. We provide the security in two levels. In the first level we use the RGB colors as a password in encrypted format to login into account and in the second level we encrypt the actual data by using Armstrong Number and RGB color value.

IV. CONCLUSION

The proposed technique uses the combination of RGB color value for the authentication purpose where password itself is in the encrypted format. Also the actual data to be transmitted is encrypted by the technique in which merging of Armstrong number and RGB color value is done hence the technique can be used in the fields like banking sectors as well as message passing purpose.

References

[1] "Security Using Colors and Armstrong Numbers" S. Pavithra Deepa UG Student, Department of IT, Sri Krishna College of Engineering and Technology;,Coimbatore,Tamilnadu,India ,S. Kannimuthu Assistant Professor, Department of IT, Sri Krishna College of Engineering and Technology, Coimbatore,Tamilnadu,India.

[2] A Survey on Security Mechanism using Colors and Armstrong Numbers International Journal of Science and Research (IJSR) Nutan Gurav, Savitribai Phule Pune University, Institute of Knowledge 2Professor, Savitribai Phule Pune University, Institute of Knowledge COE, Pimple Jagtap, Pune, Maharashtra, India.

[3] Edathala, Alwaye, "Security using Colors, Figures and Images" International Conference on Emerging Technology Trends on Advanced Engineering Research (ICETT'12) Proceedings published by International Journal of Computer Applications® (IJCA) , Ajmal K.A. Computer Science & Engineering K.M.E.A. Engineering College, India , Dalton Dhavarev Computer Science & Engineering K.M.E.A. Engineering College, Edathala, Alwaye, India, M. Selin ,Computer Science & Engineering K.M.E.A. Engineering College, Edathala, Alwaye, India,

[4] "Message Security Using Armstrong Numbers and Authentication Using Colors"Gayatri Kulkarni* , Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav Computer Department Pune University, India.

[5] "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques" Sombir Singh* Sunil K. Maakar Dr.Sudesh Kumar M.Tech. Scholar (CSE) Asstt. Prof. in CSE Dept Assoc. Prof. in CSE Dept. BRCM CET, Bahal, India

[6] COE, Pimple Jagtap, Pune, Maharashtra, India, Pratap Singh