International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Security Mechanism using Colors and Armstrong Numbers

Nutan Gurav[1], Pratap Singh[2]

[1]Savitribai Phule Pune University, Institute of Knowledge COE, Pimple Jagtap, Pune, Maharashtra, India

[2]Professor, Savitribai Phule Pune University, Institute of Knowledge COE, Pimple Jagtap, Pune, Maharashtra, India

Abstract: ***In today's tech-savvy world, electronic media is a basic necessity. Modern ways of communication have replaced the simplest of tasks. As the growing computer use implies a need for automated tools for protecting files and other information. The use of networks and communications facilities for carrying data between users and computers is also growing. Network security measures are needed to protect data during transmission; hence data security is very important. In this paper we analyze different techniques of cryptography to secure the data at the time of transmission and along with newly discovered cryptography algorithm that provides more security in data transmission.***

Keywords: Encryption, Decryption, Armstrong Number, Authentication, color, matrices.

1. Introduction

The world we live in today is a very fascinating and mysterious place. The widespread impact and use of the Internet did not hypnotize the world before the early 1990s. As the growing computer and internet use implies a need for some techniques for protecting files and other information from the user who is not intended for the same. Network security measures are needed to protect data during transmission and to ensure the security there are various techniques being used. More generally, it is about constructing and analyzing protocols that overcome the influence of the third party and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Encryption is the technique that transforms the information from readable state to unreadable state. Decryption is the totally opposite to the encryption that converts the information from unreadable or nonsense state to readable state. There are many cryptography techniques, but we are designed a new technique for encryption and decryption purpose. In this technique we are going to use the concept of secret key as the Armstrong number and colors instead of prime numbers. As we know that each pixel of the image has color and it's a combination of RGB (Red, Green, and Blue) component. The main purpose of the RGB color model is for the sensing, representation, and display of images in digital systems. In this technique initially allocates an identical color with triplet of key for each user. The data owner is conscious of intended user to receive data. The data owner uses identical color of the user (receiver) as password. The triplet is added to the receiver's actual color RGB values and it encrypted at the data owner's side. The receiver is conscious of his own color and triplet of the key while registering and decrypt the color by subtracting the triplet from the color RGB values of received image. Finally it compare with the color values which are stored at data owner's side. Data become encrypted using Armstrong number if and only if decrypted color matched at data owner's side.

a. *Encryption:* Suppose Bob has to be sent data to Alice and Alice who is allocated color is gold (206,172, 65) and the triplet of key is (-30, -20, +10) and 153 is Armstrong number for encryption.

Step I: Encrypt the color (password)
First, Bob adds the triplet to the color values of the Alice become,

```
  206   172  65
  -30   -20  10
 ---------------
  176   152  75
```

This encrypted color used as password.

Step II: Create ASCII values for message is to be sent.

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

Step III: Now adds this digits with Armstrong number.

```
    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 IV: Convert message into matrix form
A=

$$\begin{bmatrix} 68 & 81 & 72 & 8 \\ 87 & 109 & 207 & 7 \\ 92 & 88 & 92 & 9 \end{bmatrix}$$

Step V: Encoding Matrix

B=

$$\begin{bmatrix} 1 & 5 & \vdots \\ 1 & 25 & 9 \\ 1 & 125 & 2 \end{bmatrix}$$

Step VI: Encrypt the data (B X A)
C=

$$\begin{bmatrix} 779 & 890 & 1383 & 742 \\ 3071 & 3598 & 6075 & 2834 \\ 13427 & 16082 & 28431 & 1219 \end{bmatrix}$$

The encrypted message is
779, 3071, 13427, 890, 3598, 16082, 1383, 6075, 28431, 742, 2834, 12190.

b. *Decryption*
Step I: Now Alice decrypt the color, subtract the triplet from received color values.

```
 176   152   75
 -30   -20   10
-------------------
 206   172   65
```

And compare with Bob's color database.

Step II: Now inverse the encoding matrix
D=

$$(-1/240)* \begin{bmatrix} -450 & 240 & -3 \\ -18 & 24 & -6 \\ 100 & -120 & 20 \end{bmatrix}$$

Step III:
Decrypt the message to get original message by multiplying decoding matrix.

$$\begin{bmatrix} 68 & 81 & 72 & 8 \\ 87 & 109 & 207 & 7 \\ 92 & 88 & 92 & 9 \end{bmatrix}$$

Step IV: Now subtract the Armstrong number from message

```
    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 V: Obtain the original message from the above ASCII equivalent.

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

Now Alice can use this message as an original message, since Bob uses the security using Armstrong number and color as password.

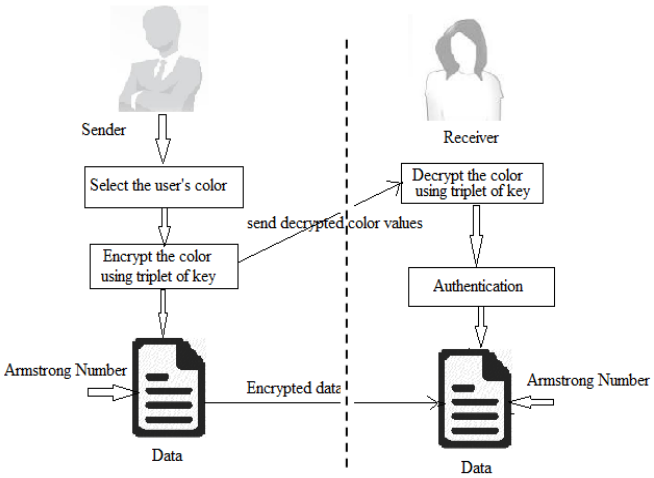

Figure 1: Encryption and Decryption using Armstrong number.

2. Armstrong Numbers

In recreational number theory, Armstrong number (also known as a pluperfect digital invariant (PPDI), a narcissistic number (after Michael F. Armstrong) or a plus perfect number) is a number that is the sum of its own digits each raised to the power of the number of digits.

For example, 371 is an Armstrong number since 3**3 + 7**3 + 1**3 = 371.

3. Security using Colors, Figures and Images

To overcome the problems associated with using the existing common and popular methods such as symmetric key cryptography, the proposed methods use the concepts of RGB color model to hide the encrypted contents. In this method the encrypted contents are converted to a bitmap image. It has many advantages over the simple symmetric key encryption and popular LSB steganography method.

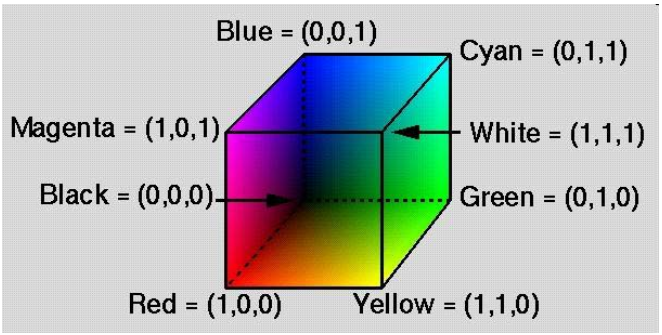

Figure 2: RGB Color Cube

3.1 Drawbacks and existing difficulties

a. Size of bitmap file to represent simple message may be larger.
b. In some cases, direct ASCII representation may prevent user from generating geometric figures with that values as parameters.(Example: rectangle(0,0,0,0)appear as line and chance.

4. Advance Cryptography Algorithm for Improving Data Security

In this paper developed a new cryptography algorithm which is based on block cipher concept. In this algorithm I have used logical operation like XOR and shifting operation. Experimental results show that proposed algorithm is very efficient and secured. The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups.

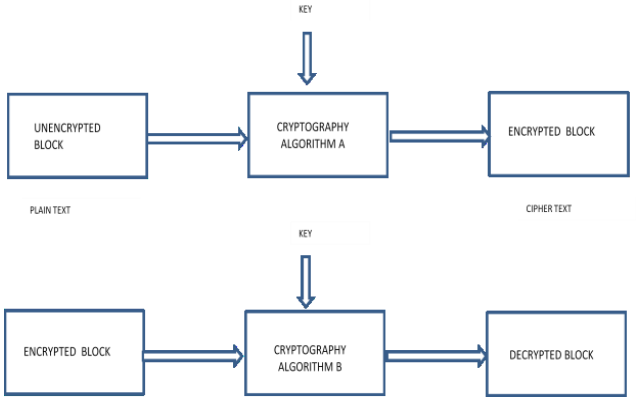

Figure 3: Basic Concept for Symmetric Cryptography.

The proposed key blocks contains all possible words comprising of number (n) of characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key blocks will depend on text key entered by the user. This system using 512 bit key size to encrypt a text message. It wills us very difficult to find out two same massages using this parameter. To decrypt any file one has to know exactly what the key blocks is and to find the random blocks theoretically one has to apply 2256 trial run and which is intractable. Initially that technique is only possible for some files such as Microsoft word file, excel file, text file.

5. A Secure Data Communication System Using Cryptography And Steganography

The main objective of this paper is to introduce a secure communication system that employs both cryptography and steganography to encrypt and embed the secret message to be transmitted over a non-secure channel. In this system, the encryption process is achieved using the filter bank cipher, which presents a high speed and level of security. The embedding process is achieved using the discrete wavelet transform based steganography. The proposed system consists from four stages as shown in Figure 4. Note that the main stages are encryption, embedding, extraction and decryption. Filter bank cipher is used for encryption the data. Filter bank cipher is a symmetric block cipher; it provides high level of security, scalability and speed. The encrypted data is embedded in a cover image using discrete wavelet transform.

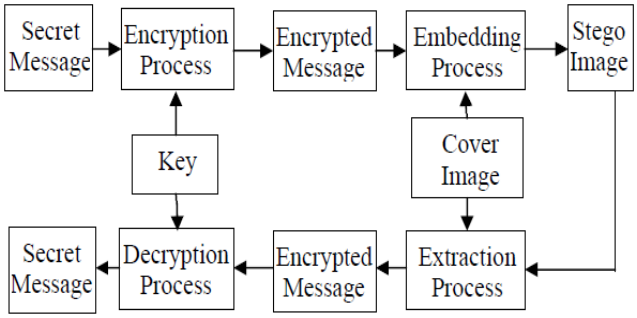

Figure 4: Block Diagram of the system.

5.1 Encryption and Decryption Process

The cryptographic algorithm used in this paper is filter bank cipher over Galois field (GF (2^8)). In this cipher the encryption process consists from two layers. Firstly, the diffusion layer is represented by the analysis filter bank to introduce a high diffusion rate. Secondly, the substitution layer which is represented by the lifting scheme over GF (2^8) to add the required nonlinearity to increase the resistivity of the cipher against the differential and linear cryptanalysis attacks.

5.2 Embedding and Extraction Process

DWT based steganography is used to hide the message using Haar wavelet. Wavelet transform converts a spatial domain into frequency domain. In this case the cover image is decomposed into four sub-images, namely, approximation coefficients, horizontal detail coefficients, vertical detail coefficients and diagonal detail coefficients.

Basically, the processing time depends on the specifications of the computer that used to run the program, and the speed of the compiler of the used programming language which is the Matlab in this paper. Usually the Matlab compiler is very slow when it compares with the compilers of other programming languages. Even though, the processing times for embedding and extraction are acceptable.

6. Analysis of all the reviewed Techniques

All these analyzed methods are good for giving security to the data if we considering only security. But any algorithm is said to be good quality algorithm if its processing time is less and efficiency is high. The Security using Colors, Figures and Images [2] algorithm has two drawbacks 1.size of bitmap file to represent simple message may be larger, 2. In some cases, direct ASCII representation may prevent user from generating geometric figures with that values as parameters.(Example: rectangle(0,0,0,0)appear as line and chance. Advance cryptography algorithm for improving data security [3] is again a complex part and time consuming process as the data block is XORing with block of keys and shifting of the blocks. 5. A secure data communication system using cryptography and steganography [4] embeds data into the image and then encryption is applied. It is also too lengthy process if I just want to apply simple but more encryption algorithm then these algorithms also fails. All the algorithms process and produce the efficient output, but the algorithmic parameters are neglected which we need to work on.

References

[1] Gordon L. Miller and Mary T. Whalen, “Armstrong Numbers”, University of Wisconsin, Stevens Point, WI 54481 (Submitted October 1990).
[2] Ajmal K.A., Dalton Dhavarev, V.P. Abeera, and G M. Selin, “Security using Colors, Figures and Images,” International Conference on Emerging Technology Trends on Advanced Engineering Research (ICETT’12), 2012.
[3] Vishwa gupta, Gajendra Singh, Ravindra Gupta, “Advance Cryptography Algorithm For Improving Data Security,” International Journal of Advanced Research in Computer Science and Software Engineering., vol. 2, no. 1, January 2012.

[4] Saleh Saraireh, "A Secure Data Communication System Using Cryptography And Steganography", International Journal of Computer Networks & Communications (IJCNCVol.5, No.3, May 2013.

Author Profile

Nutan Gurav received the B.E. (Information Technology) from university of Mumbai in 2013 and pursuing M.E. degree in Computer Engineering from Institute of Knowledge College of Engineering, Savitribai Phule Pune University, Pimple Jagtap, Pune, Maharashtra, India in 2014. During 2012-2013, she worked on 'ERP-CRM For College Management' project for fulfillment of her Bachelors' Degree.

Mr. Pratap Singh is working as a Assistant Professor in Institute Of Knowledge COE, Savitribai Phule Pune University, Pimple Jagtap, Pune, Maharashtra, India.