IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Message Security using Armstrong Number and authentication Using colors with steganography

[1]Mr. Suraj Sayyad Jamadar, [2]Mr. Sagar Vilasrao Chavan
[1]Lecturer, [2]HOD
[1]Computer Science & Engineering,
[1]Sanjay Ghodawat Institute, Atigre, India

Abstract: ***We are living in an information age. Hence data security plays an important role when we exchange data over the network. Nowadays hackers are becoming more active so we need to protect our data from the hacker. There are some techniques used to make data transmission protection. The cryptography technique is one of them. This paper uses the Armstrong number for encryption and uses RGB color for authentication its acts as a password. By using steganography hide this encrypted data with the image. In this message is encrypted the actual embedding process starts and this hidden message is encrypted using the secret key and the DCT technique is used for embedding and extraction of the file.***
Keywords: Armstrong number, RGB color, Steganography, Encryption, Decryption, Sender, Receiver

INTRODUCTION

In the real world, data security is very important where importance is given to confidentiality, authentication, and integrity. Secure data exchange is very difficult because of attackers or hackers. Cryptography is a worldwide used technique for providing security to confidential data. For encryption and decryption processes need a secret key. Sometimes the same key is used for Encryption and decryption or a different key is used for Encryption and decryption. In this RGB colors are used for authentication, Armstrong number for encryption, and steganography (Image) is used for hiding the encrypted data.

RGB representation of color:

Any mixture of three colors RGB in preset quantity. Here values of RGB represent each pixel. So by combining these colors generate one color and this color acts as a password for the authentication process. Some color combinations are as follows:

1. Blue:- (0,0,1)
2. Red:- (1,0,0)
3. Green:- (0,1,0)

Armstrong number:

An Armstrong is a number with a cube of each digit addition that generates the same number. For example, 371 is Armstrong's number because $3^3+7^3+1^3=27+343+1=371$. So this Armstrong number is used for the encryption and decryption process.

Cryptography:

It is a technique to convert plain text into cipher text. Cipher text is data that is in an unreadable format. With the help of a secret key converting the plain text into cipher text is called encryption and cipher text to plain text is called decryption.

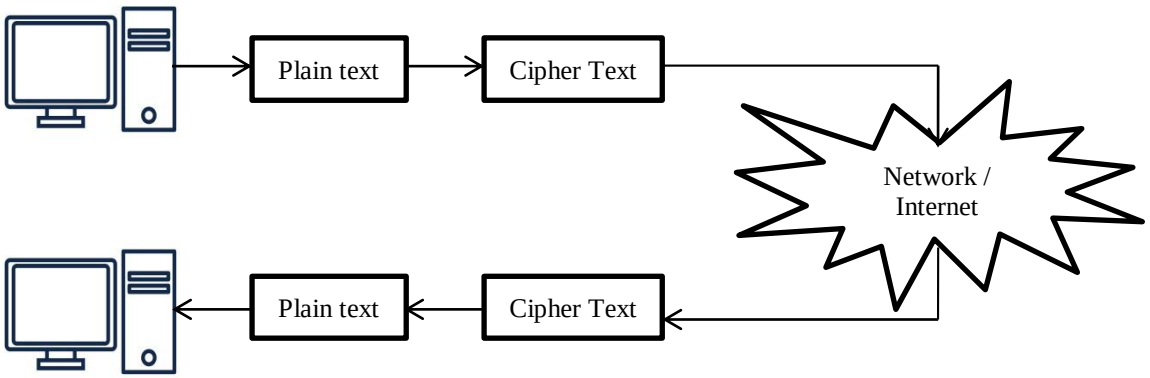

Figure. Cryptography process

Steganography: Steganography is the process of hiding data using images, audio, and video for more security of data. Because of steganography, the encrypted data is invisible to the attacker.

NEED OF THE STUDY

In nowadays hackers are more active and try to access private data like messages, images, videos, and important private information. If hackers are stealing or accessing this type of information then they misuse this information or demand money. So this topic is trying to protect messages when we communicate with each other. For protecting messages we encrypt the data using an Armstrong number and make authentication using a color that act as a password. After that, all encrypted data hide using images using the steganography technique.

RESEARCH METHODOLOGY

There are many algorithms for encryption and decryption process like AES, DES, and RSA which is done with the help of substitution technique and transposition technique plain text data is encrypted. It also uses the prime number for encryption.

a. Cryptography using a secret key (SKC):- It is an encryption technique of plain text which is value-independent. Only a single key is used for converting plain text into cipher text means encryption and also used the same key for converting cipher text to plain text means decryption. The same keys are used DES (Data Encryption Standard) and AES (Advanced Encryption Standard). It comes under the symmetric key algorithm technique.
b. Cryptography using the public key (PKC):- In this technique uses different keys. One key used for converting plain text into cipher text means encryption and the second key used for converting cipher text to plain text means decryption. In the RSA algorithm, different keys are used for encryption and decryption.
c. Hash Function: It is a function that is used to digest the original message in fixed length message which is not recoverable from the cipher text.

The user needs to run the application. The user has two tabs option one for encryption of data and another one for decryption of data.

If the user selects encrypt the data using the Armstrong number, the application gives the screen to convert to a given message in the format of the ASCII number of each alphabet and adds this ASCII number with the Armstrong number. After that hide these details using an image and send it to the receiver. Then the receiver authenticates the sender by its own RGB color key with the sender color if matches then click on decryption then this encrypted data is converted into the original message.

This system has four modules:

a. Sender Encryption module: This is the sender module in which this sender can send a message to the destination more securely. In this module written a message that he wants to send to the receiver. After that sender can send this message without encrypting it or with encrypting it. When the sender selects encryption the text will be converted into ASCII code then this ASCII code add to the Armstrong number then there will be one Armstrong matrix and a message matrix will be generated then select the receiver. After that encrypted message will be generated then select RGB color value for authentication. After that select image for hiding the encrypted message and send it to the receiver. The sending process is as follows:
   Step I: Write a Message
   For Example: hi
   Step II: ASCII value of this Message
   h=104, i= 105
   Step III: then ASCII value of this message add with Armstrong number.
   104+3= 107
   105+7=112
   Step IV: Calculate Armstrong and message matrix multiplication.
   Step V: Select the receiver
   Step VI: Encrypted Message matrix will be generated.
   Step VII: Select the Colour for authentication.
   Step VIII: Select the image for hiding the data.

b. Receiver Decryption Module: This is the receiver decryption module in which this receiver receives the message from the sender if the receiver is authenticated. When the receiver receives the message the sender authentication is done by

matching the RGB color. If the sender is valid then click on the decrypt button and convert it to the original message and sender is not authorized then discard this message. The receiver process is as follows:

Step I: Received Encrypted Message
Step II: Perform authentication by matching RGB color.
Step III: Decrypt the encrypted data to get the original message for this first obtains the inverse of the encrypted encoding matrix.
Step IV: Multiplication of the inverse of the encrypted encoding matrix with the encrypted data matrix.
Step V: then the result of the Multiplication of the inverse of the encrypted encoding matrix with the encrypted data matrix.
Step VI: Subtract from Armstrong number
Step VII: Then ASCII code is generated and ASCII code generated into character means the original message.
Step VIII: get the original message to the receiver.

IV. RESULTS AND DISCUSSION

We identified the problem of the security of secret messages. Hence a technique is used in it in which the Armstrong number is used instead of the prime number for enhancing the security of the message. Confidential areas like the military and government centers are mostly targeted by hackers so these areas need to provide more security that private data or communication take place between government agencies. By using the Armstrong number for encryption, color for authentication, and steganography technique make sure that there is secure transmission of the message. This technique provides two levels of security first is encryption and second is steganography.

REFERENCES

[1] S. PavithraDeepa, S. Kannimuthu, V. Keerthika., "Security using color and Armstrong number",Proceedings of the National Conference on Innovations in Emerging Techonolgy-2011. India.17 &18 February,2011 .pp. 157-160.
[2] Neil F. Johnson, Zoranuric, sushil.Jajodia, Information Hiding: steganography and watermarking- Attacks and countermeasures", Kluwer academic press, Norwrll, MA, new York ,2000
[3] Atul Kahate, "Cryptography and network security" Tata Mcgraw Hill Publications.
[4] Rafael C. Gonzalez, Richard E. Woods: Digital Image processing, Third edition, pearson Education.
[5]htttp://aixl.uottawa.ca/~jkhoury/cryptography.html
[6] http://mathworld.wolfram.com/UnimodularMatrix.html