Vol-01, Issue 03, Jun 2015.

Secure Information Transferring System Using Color Cryptography

[1]Nilam Yadav
[1]K J Somaiya Institute of Engineering & IT, Sion, Mumbai, Maharashtra, India.
[1]yadavnil12@gmail.com

***Abstract* — Cryptography is basically concerned with keeping communications privately and secretly. Indeed, the protection of important and highly sensitive communications has been the prime motto of cryptography throughout much of its history. Encryption is the conversion of data into some spidery form. Its motto is to ensure privacy by hiding information from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption.**

Data encryption technique converts data into a spidery format so as to protect it from external fraud entity. It is thus useful in ensuring the privacy and security of the information transferred or shared between the systems. Here, we propose a color coding RGB scheme that can be used for data encryption which represents text in the form of colored patches by grouping together binary bits and assigning them colors.

Keywords— encryption, decryption, information security.

I. INTRODUCTION

Cryptography is the practicing and studying techniques for secure and private communication in the presence of third parties (called adversaries). More generally, it is about building and analyzing protocols that is not affected by the influence of adversaries or fraud intruder and is related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography consists of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Data encryption technique converts data into an unreadable format so as to protect the information from external intrusion. It is thus useful in ensuring the private and secured information transfer or shared between the systems.

It is essential to describe the term ‘Steganography’. Steganography, the term means, "Covered Writing" which is derived from the Greek language. Steganography is the art and science of communicating in a way by hiding the existence of communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other messages which is harmless message in a way that does not let any enemy to even detect or know that there is a second message present”. In a digital world, Steganography and Cryptography both have a axiom to protect information from unwanted intruder or any fraud party. Both Steganography and Cryptography are excellent means by which to accomplish this motto but neither technology alone is perfect and both can be broken. It is for this reason that most experts have suggested using both to add multiple layers of security. Steganographic technologies are a very important part for future of Internet security and privacy on open systems such as the Internet. Steganographic research is primarily driven because of lack of strength in the cryptographic systems and on the other hand the desire to have complete secrecy in an open-systems environment.

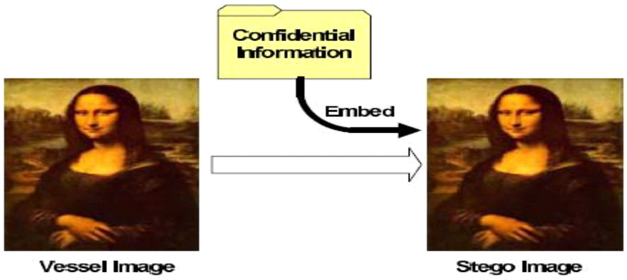

Figure 1. Information Hiding Using Steganography

© 2015, IJREAM All Rights Reserved.

II. EXISTING SYSTEM

Region Based Visual Cryptography Scheme for Color Images talked about chipping in image is done by splitting the image into different region. The concept of visual secret sharing method is encrypting a secret image into futile share images. It cannot leak any information about the original image unless all the shares are obtained. The original image is obtained by superimposing all the shares directly, so that the human visual system can recognize the shared secret image without using any complex computational devices. In this paper it is proposed a region based on sharing a visual secret scheme for color images without any pixel expansion and high security.[1]

Drawback : This scheme did not use a pattern book to generate a share images, paid more attention to evaluate the contrast of revealed images and the security result of the generated share images.

Securing Images Using Color Visual Cryptography and Wavelets states new Cryptography technique which is used to secure the images. In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the bi-level or binary images or monochrome images. Later it was advanced to suit for the Color Images means Gray Images and RGB/CMY Images. For the RGB/CMY Images different methods are developed based on the color decomposition techniques. In this paper it is proposed a new way of performing color visual cryptography using wavelet technique. Wavelet technique is used to convert the Color Image to Gray Image. The important feature of the Visual Cryptography is decryption doesn't require any computer and it requires less computational power. [2]

Drawback : The proposed model does not produce the image of optimal contrast which can be enhanced.

A Review On RGB Color Preserving Cryptography For Secure Data Transmission talks about To maintaining the secrecy and confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves hiding the data using data hiding algorithm to maintain the images secrecy.[3]

Drawback: This scheme did not have provision of choosing the key and more encode decode time consumption.

III. PROPOSED SYSTEM

The proposed system works on symmetrical key i.e. same key is shared among sender and receiver. The key is generated by the system itself by using different algorithms. In our proposed system we provide user with 3 algorithms such as 3DES, DES & Rijndael algorithm. It's upon user choice by using which algorithm the sender wants to encrypt the message. The image that is created on encryption is unique and each time the key generated is unique. Even the image created each time is different for the same text. The system works on both sender and receiver side.

On the sender side, the sender provides the text that is to be sent and select the algorithm of their choice and accordingly encrypt the message and the key is generated and the text message is converted into a color image using RGB color format. While on the receiver side it does the reverse, the receiver decrypts the message using the same key.

IV. PROCEDURE

4.1 Sender End:

Before forwarding the message to the receiver's end the secret key, color channel, initialization vector is distributed manually. The Encryption system is on the Sender side can be understood as:

Given a stored text file which is to be encrypted , the system first converts the file into its binary representation , which in turn is given to the vector is then next given as input to the encryption process, which then takes in the numeric vector data and transforms it into a color coded JPEG image. The encrypted image has a series of colored patches. The process of color assignment is pre-decided and is done by grouping 3 bits of the binary data steam together at a time corresponding to RGB format, thus giving a possibility of 8 colors in all.

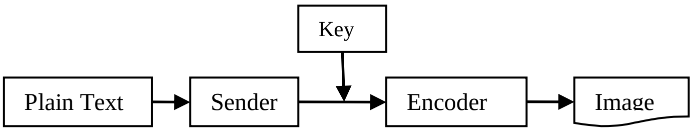

Figure 2. Encryption System on Sender End

4.2 Encryption of data:

Using Encryption technique, the proposed algorithm takes a text file as an input & then it picks each character in the text and finds the binary value of it. Now binary value is converted to ASCII value. After getting ASCII value of each character, RGB channel is selected and accordingly all the character converts it into color image.

After selecting the appropriate algorithm, a key is generated. The same key is used by receiver to decrypt the message.

4.3 Decryption of data:

The receiver uses the shared key to generate the original text message. The encrypted text at the receiver side goes through a reverse process to generate ASCII value; the ASCII value is then converted to equivalent binary value. And finally the binary data gets converted to original plain text.

4.4 Receiver End:

On the receiving side, the system takes in the encrypted image as input, which it accesses for restorating. The system will check the color of the various color patches iteratively and then takes a mean of the values for getting a practical perspective of the color of the particular patch in question. Using this process of decryption, it recreates the vector data. The vectored data converts the data back to the original binary representation as it was given in the input. The binary file is translated back to the original ASCII text file, thus restoring the text file on the receiver side.

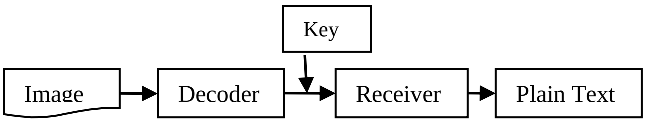

Figure 3. Decryption System on Receiver End

V. DATA FLOW OF THE SYSTEM

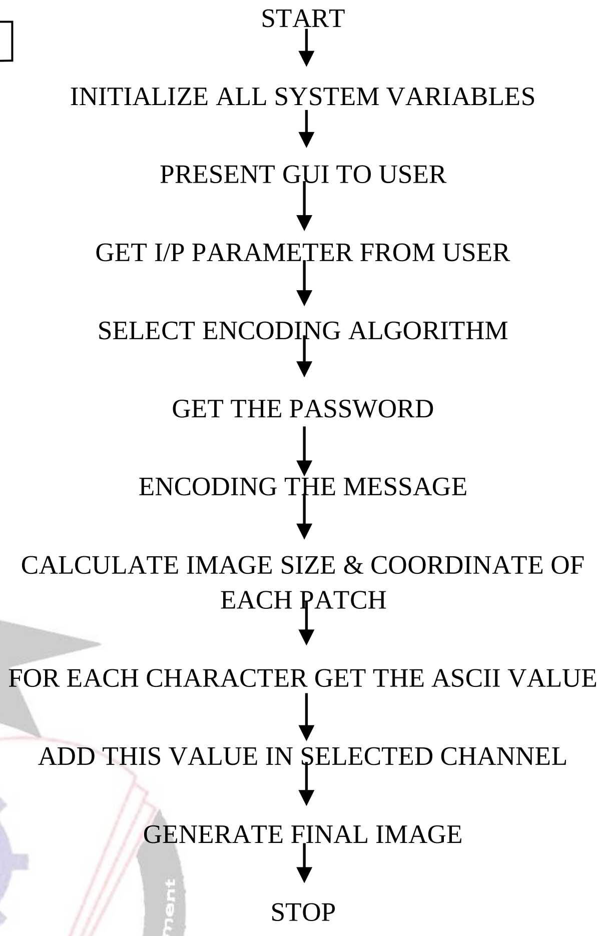
START
INITIALIZE ALL SYSTEM VARIABLES
PRESENT GUI TO USER
GET I/P PARAMETER FROM USER
SELECT ENCODING ALGORITHM
GET THE PASSWORD
ENCODING THE MESSAGE
CALCULATE IMAGE SIZE & COORDINATE OF EACH PATCH
FOR EACH CHARACTER GET THE ASCII VALUE
ADD THIS VALUE IN SELECTED CHANNEL
GENERATE FINAL IMAGE
STOP

Figure 4. Data Flow of Encoding side

The reverse is done at decoding side, firstly the receiver at the decoding side provides the same password and select the decoding algorithm, note both the algorithm used at the sender and receiver side should be the same and thus the original plain text is retrieved at the receiver side. Thus the receiver had to provide the system with the key as well as the algorithm. Thus this provides higher security.

VI. EXPECTED OUTPUT

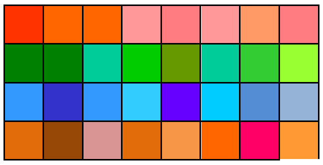

Figure 5. Encrypted Message in Image Format

IJREAM

Vol-01, Issue 03, Jun 2015.

The three characters of the text corresponds to one patch of the image .The size of the patch can be varied depending upon the users selection .The image generated varies every time. The color of the image can be decided by the user by selecting different RGB color values. The image created cannot be directly encrypted.

VII. CONCLUSION

The proposed system provides higher security, authentication and confidentiality of data. System provides flexibility of choosing 3 distinct algorithms i .e DES, triple DES, Rijndael algorithms. The system also provides with different RGB values to create different output image. Each time the image created and the key generated is unique. The proposed system is working on text file only. The user can select the file directly to be transferred .The data transferred is lossless.

REFERENCE

[1] D. R. Denslin Brabin1, Divya Venkatesan2, Divyalakshmi Singaravelan3, LekhaSri Rajendran4 “Region Based Visual Cryptography Scheme for Colors Images” IJARCCE Vol. 2, Issue 3, March 2013.

[2] Sagar Kumar Nerella, Kamalendra Varma, GadiRajaSekhar Chaganti ”Securing Image Using Color Visual Cryptography and Wavelets” IJARCSSE Vol. 2, Issue 3, March 2012.

[3] Anchal A. Solio, Dr. S. A. Ladhake “A Review On RGB Color Preserving Cryptography For Secure Data Transmission” IJARCET Vol. 3, Issue 1, January 2014.

[4] Morampudi Naresh kumar, Datrika Srinivas Rao, D.Sravanthi “A Novel Approach for Cheating Prevention through Visual Cryptographic Analysis” IJCSES Vol.2, No.4, November 2011

IJREAM International Journal of Research in Engineering Application & Management