Private Data Distribution using Visual Secret Sharing Scheme

Pradeep S
Department of computer science and Engineering
Shridevi Institute Of Engineering And Technology,
Tumakuru. Karnataka, India

Somashekhar B. M.
Assistant Professor,
Department of computer science and Engineering
Shridevi Institute Of Engineering And Technology,
Tumakuru, Karnataka, India

Abstract— Data securing is one of the major issue in the computer world. Visual secret sharing is the technique which divides the image into n number of multiple shares. Each share constitutes some data and when k shares out of n mass with one top of another together the secret will give knowledge of that data. However, less than k shares will not work. Decryption process is the resplendency of the visual secret sharing scheme i.e. decryption process of secret takes place using Human Visual System (HVS) without using any computation and calculation. The obtained secret recuperate through this design is twice in size of the pristine secret. Steganography is the art of transferring the information using original files in unknown pattern. In our approach we have recommended the incipient algorithms for the (2, 2) visual cryptography, visual secret sharing and steganography process which includes LSB (Least Significant Bit) is essential for data hiding. Our proposed approach is for gray scale image and by putting one on top another shares; the outcome is achieved in same size with pristine secret image and its shades and shared over the network, hidden data will be obtained in original format. Randomization and pixel reversal approach is being used in all methods.

Keywords: Data securing, Steganography, Visual Cryptography, Data hiding, secret sharing.

INTRODUCTION

The concept of secret sharing was developed by knowing "To split data D into n shares so that D is easily reestablishable from any k pieces, but even consummate congizance of k – 1 pieces reveals precisely no information about D"[1].The transmission of secret data to be taken place in between the authorized users. The idea of dividing image into number of shares is considered as core to the visual cryptography and also visual secret sharing scheme and every work which was presented in this area with having this idea as resource. In the abstract of this paper we said "We enhance it into a visual variant of the k out of n secret sharing quandary in which a dealer provides a pellucidity to every one of the n users any k of users can optically discern the image by stacking their pellucidities, but any k-1 of them gain no information about it". Further this core concept many researcher ascertain different schemes for the visual cryptography. This amendment zested to colored images from gray scaled image and distinct ways and techniques were evolved with astonishing conceptions.

Secret data hiding in the image incorporates the steganography process which is essentially needed. Steganography process i.e accomplished by hiding the information in another information. "The word Steganography is obtained from the Greek words "STEGO" meaning "cover" and "GRAFIA" meaning "writing" defining it as "covered writing". In image steganography the data hidden in images exclusively. After embedding the secret data into the image it is said as Stegno-Image. While visual cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. Steganography and Visual cryptography are both the ways to protect information from unwanted unauthorized parties but neither technique alone is perfect and can be executed together. Now a days the steganography is frequently utilized on computers with digital data being the transporters and networks being the high speed distribution channels [2]. Since both the fields are still burgeoning and needs to be amplifying in future based on the ordinant dictation". Now a day for the security of data is very famous and potent algorithm is used.

.

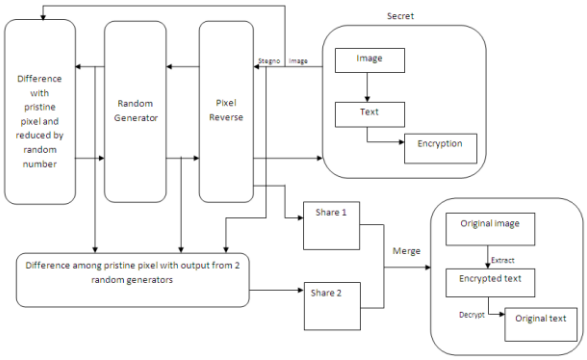
I. RELATED WORK

Adi Shamir has executed and shown the idea of "Visual cryptography", in this a new type of cryptographic scheme which can untangle concealed images without any cryptographic calculations has been proposed. Dmitri V proposed "Digital Security and Privacy for Human Ruman Rights Defenders" which shows superimpose multiple invisible texts on each other. Ravindra Gupta, Akanksha Jain and Gajendra Singh presented the paper "Combine use of Steganography and Visual Cryptography for Secured

Data hiding in Computer Forensics" provides a profitable RS- resistance secure algorithm which comprises the use of two steganography and visual cryptography. Obaida Mohammad Awad Al-Hazaimeh proposed "Hiding Data in Images Using New Random Technique" enhanced security goals were implemented via proposed cryptosystems to maintain cover image security

II. PROPOSED SYSTEM

Our proposed approach is for gray scale image and by putting one on top another shares; the outcome is achieved in same size with pristine secret image and its shades and also hidden data will be obtained in original format. It is of a framework which takes input as an image. Secret data is made to hide in the image in the plain text format.



By LSB (Least Significant Bit) technique the secret data is stored into image. Advanced Encryption Standard (AES) is applied for the encryption/decryption of secret data in the image. Using visual secret sharing scheme the image is being divided into number of shares, then the shares that are arrived others via network are merged to obtain the original image in the original format and also secret data is decrypted and obtained as original format.

System architecture is the notional design that defines the structure and deportment of a system. In our design, at secret block the image is considered for hiding the text and then the secret text is taken and it is encrypted and further it is hidden into the image. Then the resultant Stegno image is transferred to pixel reverse process. Pixel reversing is sent in the name for the secret image which containing the secret text in it. Random number generator reduces the pixel randomly. Difference with pristine pixel and diminished by the random number has taken and use random number generator to diminish the inverted value of pixel randomly. Pixel reversal is applied, stored in matrix as image called shares. The shares that are obtained by dividing the image using visual secret sharing scheme. Further the shares are merged and pristine image obtained, decryption process is applied and the pristine secret text is obtained.

IV. IMPLEMENTATION AND RESULT

The described project work is executed in JAVA with core i3 processor,4GB RAM,1.80GHz and 64bit Windows OS. The original image is in JPG format of 14.6 KB and secret text is taken in plain text format then further it is encrypted.

Fig 2:Original image and secret text encrypted

Using LSB method the secret text is embedded into the image. LSB has low computational complexity and high embedding capacity in which, a secret binary sequence is utilized to supersede the least significant bits of the host medium. It is the Supersession method of Steganography where the right most bit in a binary notation is replaced with a bit from the message to be embedded. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24-bit image, the colors of each component like RGB (red, green and blue) are changed. The text embedded image can be called as stegno image, the image after embedding the secret text into pristine image, so that it is difficult detect the secret text by intermediate attack only receiver can detect. (Fig:3)

Step1: Data is converted from decimal to binary.
Step2: Read original Image.
Step3: Image is converted from decimal to binary
Step4: Break the byte to be hidden into bits.
Step5: First 8 byte of original data is taken from the Image.
Step6: Reinstate the least significant bit (LSB) by one bit of the data to be hidden.

Fig 3: Original image and stegno image

Visual secret sharing scheme is used to divide the image into shares. The shares of the stegno image, it is shown in fig 4.

Step1 - Pixel with position i and j is the input called original pixel.
Step2 - Apply pixel reversal.
Step3 - Use random number generator to reduce Pixel randomly.
Step4 - Take the difference with original pixel
Step5 - Utilize random number generator to diminish inverted value of Pixel randomly.
Step6 - Apply pixel reversal.
Step7- Store it in matrix as image call it as share 1.
Step8- Take the difference of two random numbers generators with pristine pixel
Step9- Apply pixel reversal
Step10- Store pixel in matrix as image call it as share 2.
Step11- Repeat from point 1 to 10 for every pixel from pristine image

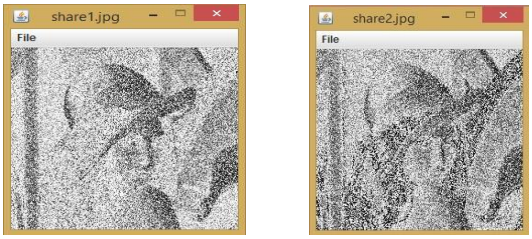


Fig 4:Stegno image shares

The shares which arrive at destination system will be merged by using AES method, AES is a block cipher which encrypts a 256-bit block (plaintext) to a 256-bit block (cipher text), or decrypts a 256-bit block (cipher text) to a 256-bit block (plaintext), to obtain the secret image and the secret text in the original format.

For the encryption:

```
Key key = generateKey();
Cipher c = Cipher.getInstance(ALGO);
c.init(Cipher.ENCRYPT_MODE, key);
byte[] encVal = c.doFinal(plainText.getBytes());
String encryptedValue = new
BASE64Encoder().encode(encVal);
return encryptedValue;
```

For the decryption:

```
Key key = generateKey();
Cipher c = Cipher.getInstance(ALGO);
c.init(Cipher.DECRYPT_MODE, key);
byte[] decordedValue = new
BASE64Decoder().decodeBuffer(encryptedData);
byte[] decValue = c.doFinal(decordedValue);
String decryptedValue = new String(decValue);
return decryptedValue;
```

Step1: Substitution of Byte
Step2: Shifting rows of the State Array
Step3: Mixing data within a column of the State Array.
Step4: Round key addition to the State Array.

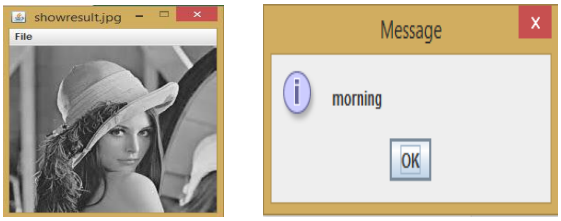


Fig 5:Original image and text

It is highly difficult for any intermediate attack to decrypt and retrieve the secret text which is stored in the image. So we can say it is highly secured.

V. CONCLUSION

In this approach using visual cryptography and steganography process we have discussed the implementation of hiding secret text in an image." This can be consummated that when regular image security utilizing steganographic and visual cryptographic technique is imposed, it makes the job of the investigators unattainable to decrypt the ciphered secret message". This approach shows the less pixel expansion which is better and desirable for the retrieval of original image. The secret text is efficiently protected in communication and confidently retrieved in the original format. Because of randomness this approach shows high level of security. This approach can be further enhanced with 3D color images for making shares and retrieve the secret by stacking each other.

REFERENCES

[1] Naor, M. and Shamir, A., "Visual cryptography", Eurocrypt 94, Perugia, Italy, in May 912, LNCS 950, pp. 112. Springer Verlag.,2010.
[2] Dmitri V., "Digital Security and Privacy for Human Ruman Rights Defenders", The International Foundation for Human Right Defenders, Manual, Feb. 2007
[3] Ravindra Gupta, Akanksha Jain and Gajendra Singh "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics", IJCSIT, Vol. 3 ((3)) , 2012.
[4] Obaida Mohammad Awad Al-Hazaimeh," Hiding Data in Images Using New Random Techniques", IJCSI, Vol. 9, Iss 4, # 2, Jul 2012.
[5] Ajit Singh, Swati Malik," Securing Data by Using Cryptography with Steganography" ,IJRCS&SE Vol 3, Iss 5, May 13.
[6] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo "Halftone Visual Cryptography via Direct Binary search" , Department of Electrical and Computer Engineering University of Delaware, Newark, DE, USA, 2010.
[7] Zhi Zhou, Gonzalo R. Arce, "Half Visual Cryptography", IEEE Transactions on image processing, volume 15, no. 8, 2006.

[8] Dr.M.Umamaheswari Prof. S.Sivasubramanian S.Pandiarajan,Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS ,Volume.10 #8, Aug 2010.
[9] A. E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi and Ahmed.BD," A Proposed Algorithm For Steganography In Digital Image based on LSB", Research Journal Specific Education, Iss No. 21, April. 2011.
[10] Nakajima, M. and Yamaguchi, Y., Extended Visual Cryptography for Natural Images, WSCG02,2002, 303.
[11] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav / International Journal of Engineering Research and Applications (IJERA) ,Vol. 2, Issue 3, May-Jun 2012, pp. 338-341.