International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

ENHANCED SECURITY SYSTEM FOR REAL TIME APPLICATIONS USING VISUAL CRYPTOGRAPHY

AbhishekShinde, Neha R. Prabhudesai,SnehalB.Sable,Lakshmi Madhuri[4]

1. shinde.abhishek93@gmail.com2.nehaprabhudesai1992@gmail.com3.snehalsable92@gmail.com
4.lakshmimadhuri1983@gmail.com

***Abstract*--With the rapid development of internet, transfer of data reliably and securely has become one of the challenges. This paper basically deals with the visual cryptography technique. This method is applicable for both Bitmap colour and Grayscale images. This method uses some algorithms for share creation and share stacking of a given image. First, Secret image is hidden in cover image to get stego-image, and then a cipher pixel is obtained. After encryption, the cipher pixel is divided into 'n' shares. These 'n' shares are stored and sent to the destination. The proposed approach like any other visual cryptography technique is very secure, efficient, reliable, fast and easy to implement. Lastly, performance analysis of this visual cryptography technique can be done with the help of histograms.**

***Keywords* –Visual Cryptography, Steganography, Symmetric Encryption, Sharing, Stacking.**

I. INTRODUCTION

1. STEGANOGRAPHY

Steganography is a branch of data hiding that allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of steganography on our lives will continue to grow. In general, steganography is the art of hiding a message signal in a host signal without any perceptual distortion of the host signal. The composite signal is usually referred to as the stego signal. By using steganography, information can be hidden in carriers such as images, audio files, text files and videos. The main terminologies used in the steganography systems are: the cover message, secret message, secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

embedding algorithm is the way or the idea that usually use to embed the secret information in the cover message. The most frequently used carriers are digital images. The use of digital images for steganography makes use of the weaknesses in the human visual system (HVS), which has a low sensitivity in random pattern changes and luminance. The human eye is incapable of discerning small changes in color or patterns. Because of this weakness the secret Message can be inserted into the cover image without being detected. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden in images. The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information.

2. VISUAL CRYPTOGRAPHY

Visual cryptography (VC) is a secret-sharing scheme that uses the human visual system to perform the computations. Naor and Shamir introduced Visual Cryptography (VC) in 1994 .Examination of one share should reveal no information about the image. Naor and Shamir devised the scheme that specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared. This scheme is illustrated in the figure given below. A pixel P is split into two sub pixels in each of the two shares. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure above. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure above. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the figure. Every pixel is encrypted using a new coin toss. Suppose we look at a pixel P in the first share. One of the two sub pixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white. Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). It involves breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. In this technique n-1 shares reveals no information about the original image. Wecan achieve this by using one of following access structure schemes:

i:(2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

ii :(2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed.

iii :(n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined the secret image will be revealed.

iv :(k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

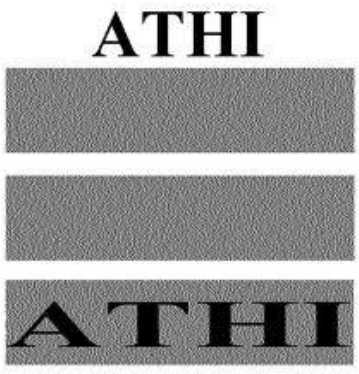


Figure 1: Basic VCS Scheme

2.1 VCS Algorithms

VCS Scheme normally involves two algorithms. Algorithm for creating shares. Algorithm for combining shares VCS algorithm's efficiency is very critical factor and reliability and level of security are some more metric which we need to consider while designing a VCS algorithm. The VCS system should be reliable enough such a way that intruders are not able to read the original image. One important functional requirement of any VCS system is size of shares which should be same as that of original image to prevent doubt for unauthorized user.

2.1.1 Algorithm for creating shares:

This algorithm divides secret image into n number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted separately through communication network, security is achieved.

2.1.2 Algorithm for combining shares:

This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input.

II RELATED WORK

Visual Cryptography is a secret sharing scheme that uses the human visual system to perform computations. This Secret sharing scheme was invented independently by MoniNaor and Adi Shamir in 1994[1]. Recursive information hiding is a technique where certain additional secret information can be hidden in one of the shares of the original secret imageRecursive information hiding in visual cryptography can be applied to many applications in real and cyber world. The advantage is that the final decryption process is done by human visual system instead of complex computations [2]. VC also deals with the work that is carried out in steganography and it also discusses the encryption process of the visual cryptography. It gives a clear idea about, how a stego-image is created and how encryption process can be carried out on it [3]. VC method is used as a tool for providing security in

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

Real time applications. This work explores the possibility of using visual cryptography for biometric authentication. It explains us how can visual cryptography be used for authentication using finger prints, tongue scanning etc. It further tells us that it can also be extended for face-scanning. It is one of the most secured ways authentication[1]. This works tells us about the color decomposition technique that is used in visual cryptography in case of colored images. It gives us complete information about the visual cryptography in case of colored images.

III PROPOSED SYSTEM

The overall proposed system is given as follows:

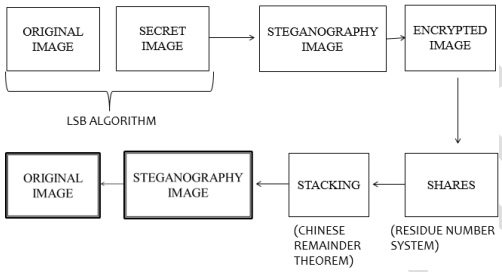


Figure 2: Proposed System

The proposed system is divided into four modules for systematic implementation. The four modules are as follows:

i)Implementation of Steganography

ii)Symmetric encryption of the Stego-Image

iii) Share creation

iv)Stacking and Decryption

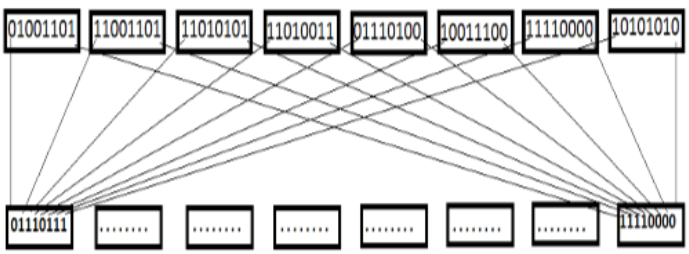
1) IMPLEMENTATION OF STEGANOGRAPHY

Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication.

The basic structure of Steganography is made up of two components: the "carrier"and the message. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will 'carry' the hidden message.

2) SYMMETRIC ENCRYPTION OF STEGO-IMAGE

First, for encryption additive modulo 255 algorithms is used. Keys are generated using a unique technique called Mixed Key Generation (MKG). In this method block of size of 8 byte keys are generated using PRN generation algorithm and individual bits from every byte is selected, since we have 8 byte word we can perform parallel operation with 8 byte of source data. Structure of Key generation technique is given in figure 2.By taking the keys generated by MKG method each pixel is encrypted to form Cipher pixel. Since, we can generate 8 keys at a time this improves the efficiency of cipher pixel generation.



International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

Figure 3: Key Generation

3)SHARE CREATION

Share Creation Process

The encrypted stego-image is then selected and mapped into 3 shares using Share creation algorithm which is discussed in previous section. The resultant shares are as in figure 4; by observing the shares generated we can conclude that there is no pixel expansion problem which is solved compared to other visual cryptography techniques without using random grids and these individual shares are sent to destination via different communication channels. If intruder can access all of these communication channels than he may get all shares or subset of shares; since stego-image itself is encrypted even if he/she stack those shares they will get only random noise as reconstructed image. In traditional visual cryptographic technique if intruder can access individual communication channels by which shares are sent than he/she can construct original image very easily simply by stacking those individual shares; this problem is solved in proposed system. By these observations we can conclude that the proposed system has enhanced security, reliability, aspect ratio not distorted (i.e. no pixel expansion) and efficient.

Figure 4: Output of share Creation Algorithm

4)STACKING AND DECRYPTION

Stacking deals with the combining of shares.The shares that are created during the share creation process are combined together in the stacking process and then the decryption process takes place after which we get the desired output. In the decryption phase we need to provide the key that was given in the encryption phase.

IV IMPLEMENTATION

1) IMPLEMENTATION OF STEGANOGRAPHY

The proposed system first uses LSB technique for embedding information in the cover image. The simplest form of spatial domain image steganography is implemented by inserting the secret data into the least significant bits. Different algorithms would insert the binary form of the secret data in 1, 2, 3 or 4 – LSBs of the cover image. So, it is simple to implement for RGB, Gray Scale or Binary Images and less susceptible to detection by Human Vision System (HVS).In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit bitmap image where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following grayscale values:

(11010010 01001010 10010111 10001100 00010101 01010111 00100110 01000011)

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

(11010011 01001010 10010110 10001100 00010100 01010110 00100111 01000011)

a b

Figure 5: a) Secret Image b) Cover Image

2)SHARING

Share Creation Algorithm

The algorithm for share creation is as given below:

Step 1 : select 3 prime numbers m1,m2,m3 such that their product is greater than 255 and gcd of selected 3 numbers is 1(i.e. relatively prime)

Step 2: calculate ri1=X mod m1, ri2=X mod m2,ri3=X mod m3 Where, ri1, ri2, ri3 are residues of i'th pixel; X is an individual pixel; m1, m2 and m3 are selected prime numbers.

Step 3: Represent the residues ri1, ri2, ri3 as i'th pixel of share 1 2 and 3 respectively.

Step 4: Repeat step 2 and 3 until all pixels are processed

3)STACKING AND DECRYPTION

Share Stacking Algorithm

Chinese Remainder Theorem concept is used for share stacking process. The entire process is shown in figure 6

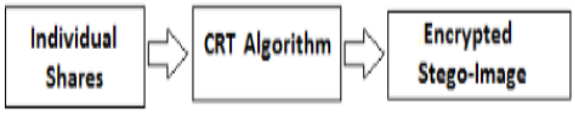


Figure 6: Share stacking process

Share stacking algorithm is given below:

Step 1: Calculate the dynamic range M=m1.m2.m3

Step 2: Calculate Ai = M/mi

Step 3: Find the solution of congruence's Ai.Ti mod mi (Where Ti is multiplicative inverse of Ai)

Step 4: We can get back original pixel by CRT using below equation

$$x = \sum_{i=1}^{N} A_i . T_i . r_i \bmod M$$

Step 5:Repeat step 4 until all pixels of shares are processed.

Share Stacking Process

At destination side, share stacking algorithm is run. Input to this algorithm is shares which are generated as in figure 4 and we got Figure 7.a as output. This algorithm is exact reconstruction algorithm which does not have any data loss. This algorithm is very efficient which has less execution time.

a

b

Figure 7 a) Output of Stacking Algorithm b) Reconstructed Stego-Image

Decryption Process

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

When Figure 7.a is given as input to Symmetric decryption algorithm and we get Figure 7.b as output. Since the algorithm initially used is based on feedback shift register same sequence of numbers are generated in destination also satisfying the requirement of symmetric key encryption.

Extraction Process:

Finally, Secret image is extracted from the stego-image which is as shown in figure 7.By Comparing Figure 5.a and Figure 8 this paper concludes that extracted image is exact copy of original image and there is no loss of information.

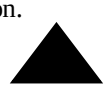


Figure 8 Extracted Image

V ADVANTAGES

- No pixel expansion
- Use of symmetric encryption
- Symmetric encryption, steganography and visual cryptography is used in combination

VI CONCLUSION

A new visual cryptographic technique has been introduced. The traditional VCS suffer from pixel expansion problem. The proposed technique rectifies this problem. Another drawback of existing VC schemes is if intruder can access all communication channels than reconstruction of secret can be done easily; since symmetric encryption is introduced before sharing secret; our approach which overcomes this problem. The concept of symmetric encryption, steganography and Visual cryptography is combined in this paper to give a secured image sharing system.

VII FUTURE SCOPE

If lossless Image compression methodology is applied before encryption we can strengthen cryptographic security. Because compressed image has less redundancy than the original image, cryptanalysis will be difficult .The proposed system can be extended such that it can be applied to all types of image formats like Jpeg, png etc. The LSB technique although it is simple and straight sometimes it is breakable so, in future any other steganographic which is not very easily breakable by intruder may be applied.

REFERENCES

[1]. M.Sukumar Reddy and S.Murali Mohan. VisualCryptography scheme for secret image retrieval. International journal of innovative research ,June2013

[2]. Abdelmgeid Amin Ali, Al – HussienSeddikSaad. Image Steganography Technique By Using Braille Method of Blind People (LSBraille). International Journal of Image Processing (IJIP),Volume(7):Issue(1):2013

[3]. Mrs.Kavitha, KavitaKadam, AshwiniKoshti, PriyaDunghav. Steganography Using Least Signicant Bit Algorithm. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[4]. SonaliPatil, KapilTajane, JanhaviSirdeshpande. Secret sharing schemes for secure biometric authentication. International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 ISSN 2229-5518

[5]. JagdeepVerma, Dr.VineetaKhemchandani.A visual cryptographic technique to secure image shares,International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-10 , July, 2014

[6]. AnushreeSuklabaidya and G.sahoo.Visual cryptographic applications. International journal on computer science and engineering June 2013

[7]. L.N.Pandey and Dr.MuktaBhatele. Visual cryptography schemes : A comparative survey . ISSN 2320-9984,volume 1,Issue 2,July2013

[8]. Juby Justin and GissGeorge . An extended color visual cryptography algorithm for general access structures. International journal for advance research in engineering & technology June 2013

[9]. Young-ChangHou, Visual cryptography for color images, Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC Received 6 June 2012; accepted 26 August 2012

[10]. Ranjan Kumar H S1, Prasanna Kumar H R1, Sudeepa K B2 and Ganesh Aithal. Enhanced security system using symmetric encryption and visual cryptography. ISSN: 22311963, Vol. 6, Issue 3, pp. 1211-1219,July 2013