RESEARCH PAPER | Engineering | Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

A Proposed Model of Visual Cryptography Technique

KEYWORDS: Halftone Visual Cryptography (HVC), Error diffusion, Visual Cryptography (VC), watermarking, Visual threshold, half toning Watermarking, Visual threshold, half toning

Ms.Hiral Rathod	Ms.Hiral Parmar
Asst. Professor, CSE Department, S. P. B. Patel Engineering College, Mehsana, Gujarat, India	Asst. Professor, CSE Department, S. P. B. Patel Engineering College, Mehsana, Gujarat, India

ABSTRACT In digital era security is the most important issue and cryptography is one of the mathematical solution related aspects of Information Security like integrity, confidentiality, data security, entity data origin authentication and authentication. Visual cryptography is another new solution or technique which provides information security with the help of simple algorithm. Use of the visual cryptography is easier than complex algorithms used in different techniques like normal cryptography (Symmetric and asymmetric). Through this technique we allow visual information (pictures, text, etc) that will be encrypted in such a way that their decrypted information can be seen by the human visual system, without using any type of complex algorithms. In this technique we encrypt a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. In this paper we provide a brief introduction of the Visual Cryptography (VC) and related security research work done in this area. And finally we are proposing a new visual cryptography model to overcome the existing security issues improving overall efficiency of visual cryptography algorithm

I. INTRODUCTION

Visual Cryptography is the special encryption technique proposed by Naor and Shamir in 1994 to hide information in images, such a way that it can be decrypted by the human vision if the correct key image is used [8]. They demonstrated a visual secret sharing scheme, where an image is broken up into n shares so that only someone with all n shares could decrypt the image, while any n – 1 shares revealed no information about the original image. It uses two transparent images. One image that contains random pixels and the other image contain the secret information. It is almost impossible to get the secret information from one of the images. Both transparent images and layers are needed to reveal the information. The simplest way to implement Visual Cryptography is it should be print onto a transparent sheet into the two layers. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

II. WORKING PRINCIPAL OF VISUAL CRYPTOGRAPHY:

Each pixel of the images is separated into smaller blocks. There are two blocks which contains white and black color blocks.. If the pixel is divided into two parts, there is one white and one black block. Same way, If it is separated in four equal parts, two are white and two are black blocks.. Below is the figure 1 that uses the pixels that are separated into 4 parts.

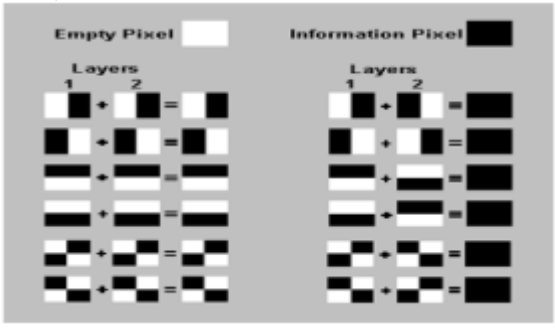

Figure 1: Visual Cryptography's Sub-Pixel Principle

In the figure 1[6] on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

In the figure 1, we can see that if a pixel is separated into 2 parts then 6 distinct states can be possible. Now, the pixel of layer 1 and pixel of layer 2 are inverted or opposite, the overlaid version will be totally black. This is the information pixel.

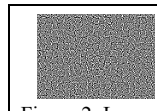

Figure 2: Layer 1

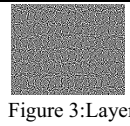

Figure 3:Layer 2

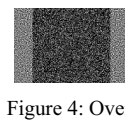

Figure 4: Overlay

Two layers can be created. One transparent image, layer 1 shown in figure 2, contains one of the six possible states. Layer 2 which is shown in figure 3 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid which is shown in figure 4. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlapped, the areas with identical states will look gray, and the areas with opposite states will be black.

If the pixel states of layer 1 are genuinely (crypto secure) random, both empty and information pixels of layer 2 will also have fully random states. One cannot determine if a pixel in layer 2 is used to create a black or grey pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

Visual Cryptography is used to protect the sensitive data sent over the internet, here first of all sender can sent the

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

random one or more image to receiver and if sender has the message he can select the layer 2 image with message itself. If the receiver gets the two layer image, he can retrieve the image without using complex computations.

III.RELATED WORKS

Now a day, Security is the main aspect in data transmission via internet. Different kinds of data are available for example video, audio, text, images etc. There are so many techniques and algorithms to ensure confidentiality, availability and integrity. For example RSA, DES, BLOWFISH, IDEA etc. All these techniques are widely used for text and they are very complex plus it requires mathematical complex computations. To overcome these issues visual cryptography has been introduced. In visual cryptography technique, visual information is encrypted such a way that their decryption can performed by only human visual system. It is simple and easy to understand.

In [1] the researcher proposed a novel combine method of visual cryptography and staganography. Using both the method the computational complexity was high but security was more. It is difficult to understand the complexity of algorithm. They proposed the method for increase the impression of output carrier image by preserving the edge structure in [2]. In this [3] proposed architecture researcher approached hybrid technique of visual cryptography and digital watermarking in which secret image is broken into parts and using digital watermarking parts are covered.
In the proposed scheme [4], initially the secret data is encrypted using visual cryptography and then cipher image is embedded into different carrier images using steganography. Secret image is decomposed into its CMY components and the Random grids of the individual components are generated.
Advantage of this scheme is that, key encryption before Secret sharing of image provides added security and using Steganography in secret sharing provides extra security. The main advantage of Steganography techniques is that it will give no clue to the unauthenticated user by hides the secret share inside a cover image.

IV. PROPOSED CONCEPT

Proposed Work: Proposed Concept will propose three steps in proposed scheme:

1) Hybrid halftoning:

- FM halftoning using Error diffusion
- AM halftoning using Cluster dot screenin
- Separating homogeneous and non-homogeneous areas

2) Encoding and Generation of Shares

- Producing Key Value
- Cover Images Encoding
- Original or Secret Image Encoding
- Producing Share's

3)Decryption

In proposed work process include three processes. There are two main types of halftoning, AM (Amplitude Modulated) and FM (Frequency Modulated) used in above proposed work [9] In the AM technique Size of the dots is not constant while spacing is not variable. The one dot in halftone cell increase larger as the value of tone becomes dark and smaller as value tone becomes lighter. In the FM technique, contrary to the AM technique, there is size of the dots is kept constant while their spacing varies. The number of microdots within the halftone cell increases as the tone value becomes darker and decreases as the tone value becomes lighter. In proposed work process include three processes. Last process is decryption and it is reverse process of encryption .Figure 5 is showing the simple architecture of the proposed scheme. In this scheme I will pass original image, cover image and key image as an input then process colors component of' original or secrete image, cover image and key image. After completing this process, apply hybrid halftoning, then apply encoding process on original and cover images. Finally shares will produce.

Figure 5: Architecture of Proposed Scheme

V. OUTCOME AND CONCLUSION

To evaluate proposed and existing algorithm we will selected cover images and secret image. All images will be of size NxN pixels. Number of Share's will generate MxM pixels. Key Image will also of size MxM pixels. By stacking all shares and Key Image together, the original or secret image will be revealed. In the experimental results

In this paper the proposed scheme successfully encrypts the original or secret image inside the meaningful shares, and later the original or secret image will recover simply by stacking the shares and the Key Image with each other. The efficiency of proposed scheme will more than 70% i.e. only 30% of the pixels of the secret image will be black and the other 70% will be the same color as the original or secret image. There are two main features which will improve the security of proposed scheme First is the Key image that will ensures that the pixels of the original or secret image will encoded in different ways. Second, during the generation of shares, and encoded cover images will randomly chosen, which will ensures that any share by itself, or a single share along with the Key Image will not reveal the secret image.
The following objective metrics [13] will be use for comparison between the original secret image and the reconstructed secret image:
i) Mean Square Error (MSE): It measures the average of the square of the error. The error is the amount by which the pixel value of original image differs from the pixel value of decrypted image.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))^2}{MN}$$

Where x(i,j) represents the original image, y(i,j) is the decrypted image and (i,j) represent the pixel positions of the MxN image. Here, M and N are the height and width of image respectively.
ii) Peak signal to noise ratio (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel. PSNR is given by

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

$$PSNR = 10\log_{10}\frac{(2^n-1)^2}{MSE}$$

iii) Normalized Correlation (NC). It measures the similarity representation between the original image and decrypted image.

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) * y(i,j))}{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j))^2}$$

IV. COLCULTION & FUTURE ENHANCEMENT

In this research we have presented about VC scheme for color images using meaningful shares. Like the existing schemes, the size of the shares produced and final image after stacking are twice the size of original image. However, the visual quality achieved by proposed algorithm will be higher. Proposed VC Scheme the Key value and Image Encoding procedure will use considerably
improves the security by increasing the randomness. Therefore, the probability of the secret image being guessed is very low. In future, I will implement and secure visual secret sharing scheme. The proposed scheme will produces good decryption results and it will also less computationally expensive compared to a previous scheme. Further, original image will be recovered more accurately by stacking and making some improvements in the decryption process.
In the future work, total processing time to encrypt and decrypt the image can be reduced and for more security triple novel method of visual cryptography, steganography and digital watermarking can be implemented.
Another future enhancement is that video files can be encrypted by dividing it into frames and the proposed algorithm can be applied to each frame to encrypt it.

REFERENCE

[1] Analysis of Visual Cryptography, Steganography Schemes and its Hybrid Approach for Security of ImagesMoumita Pramanik1, Kalpana Sharma21,2Sikkim Manipal Institute of Technology, Majitar, Sikkim, India | [2] Bin Liu,Ralph R Martine,Ji Hu Huang,Shi Mi Hu. "Structure Aware Visual Cryptography" 2014 | [3] Jagdeep Verma, Dr.Vineeta Khemchandani "A Visual CryptographicTechnique to Secure Image Shares" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1, pp.1121-1125, Jan-Feb 2012. | [4] Pratarshi Saha, Sandeep Gurung and Kunal Krishanu Ghose Hybridization of DCT based Steganography and Random Grids International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.4, July 2013. | [5] Poonam Bidgar, Neha Shahare,"Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 8, Issue 2 (Nov. - Dec. 2013), PP 11-18. | [6] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm |[7]https://decryptedmatrix.com/live/what-is-visual-cryptography/ | 8]http://www.learnwithnirab.com/2011/04/beginner-guide-what-is-visual.html | [9]Savan Gooran,Bjoran Kruse ,"Hybrid Halftoning,two levelhybrid halftoning tequniques" | [10] allavi Vijay Chavan1, Dr. Mohammad Atique2 and Dr. Latesh Malik3," Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares" (IJNSA), Vol.6, No.1, January2014