E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

SECURING WHITE AND BLACK IMAGE USING VISUAL CRYPTOGRAPHIC SHARES

Ms. Kirti Mhamunkar [1]
Dr. Deven Shah [2]
Mrs. Smita Deshmukh [3]
kirtimhamunkar@gmail.com [1]
Department of Information technology

ABSTARCT:
Visual Cryptography (VC) is a technique used for securing image-based secrets. The Visual Cryptography Scheme is a secure method that encrypts a secret image by breaking it into shares. By taking the advantage of this property, third person can easily retrieve the secret image if shares are passing in sequence over the network. The encryption technique requires a cryptographic computation to divide the image into a number of parts or we can call it shares. The encrypted data is decrypted using Human Visual System (HVS). This is the benefit of the visual secret sharing scheme. A distinctive property of Visual Cryptography Scheme is that one can visually decode the secret image by superimposing shares without computation. Intent of this paper is on study of visual cryptography for black and white image.

***Keywords*:** *cryptography, encryption, decryption, VSS, HVS.*

I INTRODUCTION

Visual cryptography is introduced by first in 1994 Noar and Shamir [4]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. Generally XOR operation is use for decryption. Because this property visual cryptography is useful for the low computation load requirement. In encryption procedure, visual cryptography is a technique for hiding a two-tone secret image into a set of binary transparencies which seem like random noise. In the decryption step, the secret image can be observable by human visual system by stacking some transparencies. Generally, visual cryptography use a visual secret sharing (VSS) scheme based on a {*k*, *n*} threshold framework, where *n* means a secret image will be hidden in *n* transparencies, and k is that we can stack *k* or more than *k* transparencies to reconstruct the secret image in visual.

Visual Cryptography (VC) is a special encryption technique used to encrypt images in such a way that it can be decrypted by the human visual system if the correct key images are used. The technique was proposed by Moni Naor and Adi Shamir [4] in 1994. According to them Visual Cryptography is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies.

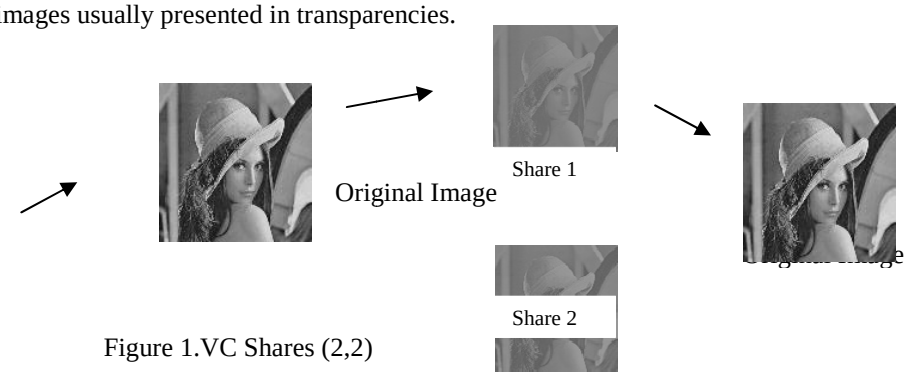

Figure 1.VC Shares (2,2)

Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret image. The act of decryption is to simply stack shares and view the secret image that appears on the

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

stacked shares. Visual Cryptographic technique is being used for secretly transfer of images in military , hand written documents, financial documents, text images etc.VC shares exist in their actual form during the transmission over network. However, directly third person cannot guess the secret information with any single share [2].

II BLACK AND WHITE VISUAL CRYPTOGRAPHY SCHEMES

Sharing Single Secret: Naor and Shamir's [4] proposed encoding scheme to share a binary image into two shares Share1 and Share2.

Table1. Naor and Shamir's scheme for encoding a binary pixel into two shares

Pixel	Probability	Share1	Share2	Share1 □ Share2
	50%			
	50%			
	50%			
	50%			

If pixel is white one of the above two rows of Table 1ist chosen to generate Share1 and Share2.Similarly If pixel is black one of the below two rows of Table1 is chosen to generate Share1and Share2. Here each share pixel code white and two black pixels each of share alone gives no is clue about the pixel whether it is white or black. Secret image is shown only when both of the images became shares are superimposed.

To hide a binary image into two meaningful shares Chin-Chen Chang et al [1.] suggested Spatial-domain image hiding schemes. These two secret shares are embedded into two gray level cover images. To decode the hidden messages, embedding images can be super imposed. Balancing the performance between pixel expansion and contrast Liguo Fang[3.] recommend a (2, n) scheme based on combination. Threshold visual secret sharing schemes mixed XOR and OR operation with reversing and based on binary linear error correcting code was suggested by Xiao-qing and Tan [7].

Sharing Multiple Secrets: S J Shyu et al [5] were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circle shares. A master key is generated for all the secrets; correspondingly, secrets are shared using the master key and multiple shares are obtained [7].

III METHODOLOGY OF THE PROPOSED SCHEME

Visual Cryptography Encryption is implemented. It consists of generation of shares from secret image using VC (2, 2) scheme. The secret image is first converted into a binary image then each pixel in the secret image is broken into 8 sub pixels, 4 pixels in each share by selecting the random pixel encoding scheme [5].

The algorithms for conversion of image into binary and share generation are given below:

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

Image-conversion
Input: .jpg image/.bmp image
Output: BIN_IMG, R_size, C_size
IMG=read ()
BIN_IMG=Convert_to_binary (IMG)
[R_size C_size]=Cal_size (BIN_IMG)

Algorithm 1. Image Conversion

Input: BIN_IMG, R_size, C_size
Output: SHARE1
SHARE2
For i=1 TO R_size
Do
For j=1 TO C_size
Do
Pix_enc_scheme=Rand_select()
SHARE1=Pix_enc_scheme(BIN_IMG(i,j))
SHARE 2=Pix_enc_scheme(BIN_IMG(I,j))
Done
Done

Algorithm 2. Share Generation

For decrypted the original secret image by applying the binary XOR operation on both decrypted shares.

The characteristics of visual cryptography

For visual cryptography, it has some advantages [6].

1. Complete security.
2. Robust method against the loss of compression and distortion because of the property of binary.
3. Do not need computer device for decryption.

The drawback of visual cryptography:

1. The resolution of the restored secret image is lower than the original secret image.

IV CONCLUSION AND FUTURE SCOPE

Providing security to the confidential data shared in day to day life is an important issue in real life. Visual cryptographic scheme, which can decrypt secrete images without any cryptographic computations. The scheme is perfectly secure and very easy to implement with low computation cost. It has been observed that there are many possible extensions exist as the visual quality & size of revealed image. We can implement this type of system in various fields like in Military, Defense, and other places where the confidentially of data should be must. The major areas of future scope are:

1. We can use color image in place of black and white image and then generate the shares using Visual Cryptography.
2. Using Compression techniques we can reduce bandwidth requirement of encrypted shares to reduce bandwidth requirement..

V ACKNOWLEDGMENTS

I sincerely thank to my project guide for guidance and encouragement me.

REFERENCES

[1] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, “Sharing a Secret Two-Tone Image In Two Gray-Level Images”, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05),2005
[2] Kulvinder Kaur2013 3rd IEEE International Advance Computing Conference (IACC) “Securing Visual Cryptographic Shares using Public Key Encryption”.
[3] Liguo Fang, BinYu, “Research On Pixel Expansion Of (2,n) Visual Threshold Scheme”, 1st International Symposium on Pervasive Computing and Applications, pp. 856-860, IEEE.
[4] Naor and Adi Shamir, “Visual Cryptography”, advances incryptology–Eurocrypt, pp1-12, and 1995.
[5] S.J.Shyu, S.Y.Huanga, Y.K.Lee, R.Z.Wang, and K.Chen, “Sharing multiple secrets in visual cryptography”, Pattern Recognition, Vol.40, Issue 12, pp.3633-3651, 2007
[6] W. Q. Yan, D. Jin, M. S. Kankanhalli, “Visual cryptography for print and scan applications”, ISCAS, vol. 5, pp. 572-575, 2004
[7] Xiao-qing Tan, “Two Kinds Of Ideal Contrast Visual Cryptography Schemes”, International Conference on Signal Processing Systems, pp. 450-453, 2009.