© 2018 IJSRSET | Volume 4 | Issue 9 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Visual Cryptography using KN Sharing Algorithm for Colour Images

Choksi Vandana M.
Department of E&C, FoT, Dharmsinh Desai University, Nadiad, Gujarat, India

ABSTRACT

Visual cryptography technique encipher the visual information in such a way, that decipher can be performed by human visual system without any complex process. Visual cryptography is a secure process for transmitting visual information but, if anyone gets access to all shares, he/she can reveal out the secret easily. In this paper a visual cryptography scheme is proposed. This technique first encrypts the secret using a symmetric key given by the user. Further, the encrypted image is divided into N different shares. These N shares can be distributed but, the end user needs only K of these shares to regenerate the original image. After piling of K shares, the original image is generated but it is still in encrypted form. The key which is used to encrypt the image originally is now required again to decrypt the image, thus providing an additional level of security. This technique is proposed for binary image, Grey scale image & colour images. Here the symmetric key used for encryption and decryption is any string (like password). Such a technique thus would be lucrative for defence and security.

Keywords: Visual Cryptography, Shares, Encryption, Decryption

I. INTRODUCTION

This In order to guard data and debase computation, Naor and Shamir introduces the concept of Visual cryptography. Main feature of visual cryptography scheme (VCS) is that it does not need mathematical computation to get the original secret. In visual cryptography scheme, visual information is chopped into N shares and distributed to N participants. At least K no. of shareholders can reveal the actual image if their shares are piled properly in proper orientation. But fewer than K shares gets no information about the secret. This is referred as K out of N visual cryptography scheme and symbolically written as (K, N) visual cryptography scheme. The main problem of most visual cryptography scheme for image is that the decrypted image size is larger than original and also some security issues are present. The proposed visual cryptography scheme has tried to overcome both issue. The size of shares is same as original while security is provided using the concept of symmetric key encryption. After the original image is generated it is still in encrypted form. The key which is used to encrypt the image originally is now required again to decrypt it, thus providing an additional level of security.We have also successfully implemented this scheme in Matlab R2017a. Here the proposed scheme is described in section-3. Result of implementation is shown in section-4. Comparison of new scheme with others is shown in section-5. Conclusion and Future work is described in section-6.

II. METHODOLOGY

Visual cryptography enrooted by M. Naor and A. Shamir, and they described general (K, N) Visual Cryptography Scheme. When shares are merged using OR/XOR operation, grayed secret image recovered.

Each original pixel is made up of m subpixels as shown in figure 1. Each pixel appears in N modified versions called shares.

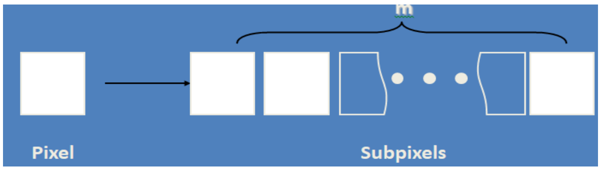

Figure 1. Pixel Division (per share)

Each share is a collection of m black and n white sub-pixels. The resulting structure can be described by an n x m Boolean matrix S = s_{ij} as shown in figure 2 and figure 3.

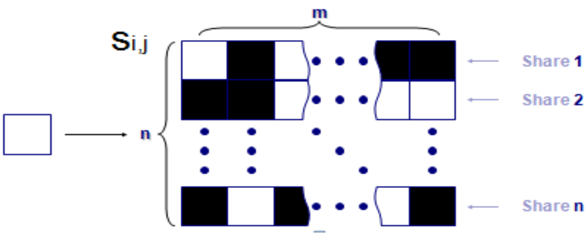

Figure 2. Pixel (in the group n)

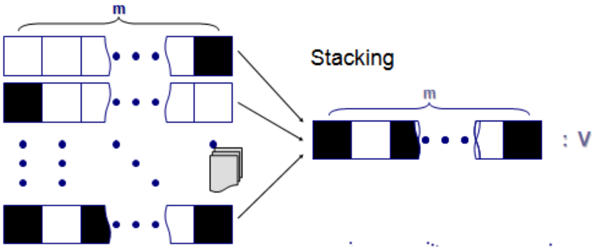

Figure 3. After piling all the shares we get original one.

2.1. 2 out of 2 Scheme (2 subpixels):

Divide the original pixel into 2 subpixels as shown in figure 4. After the piling of share 1 and 2 we get original image.

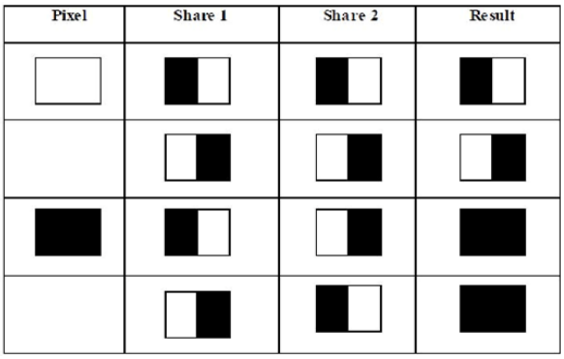

Figure 4. 2 out of 2 scheme using 2 subpixels

2.2. 2 out of 2 Scheme (4 subpixels):

Divide the original pixel into 4 subpixels as shown in figure 5. After the piling of share 1 and 2 we get original image.

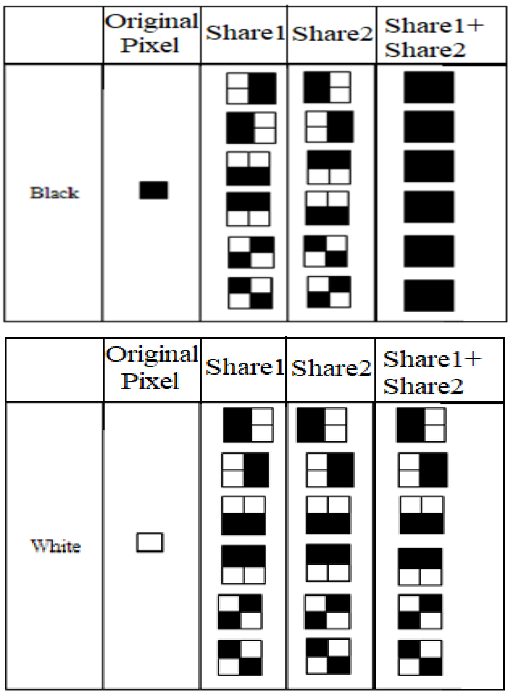

Figure 5. 2 out of 2 scheme using 4 subpixels

Assuming an input 24-bit bitmap colour image which each 3-bytr sequence in the bitmap array represents the relative intensities of red, green, blue. Firstly, decompose the colour image into three planes under additive model. By this way we can generate the N shares of the colour image.

III. PRIOR ARTWORK

The proposed scheme consider security of image in terms of encrypting it with the help of symmetric key, hence if someone access all the shares in unauthorized way, he/she can't decrypt it completely without symmetric key.

This scheme manages security as well as decrypted images are of same size as original. The scheme is divided into three parts as shown in figure 6.

3.1. Encryption of original image using AES Encryption key
3.2. Generation of Shares
3.3. Decryption of Overlapped shares

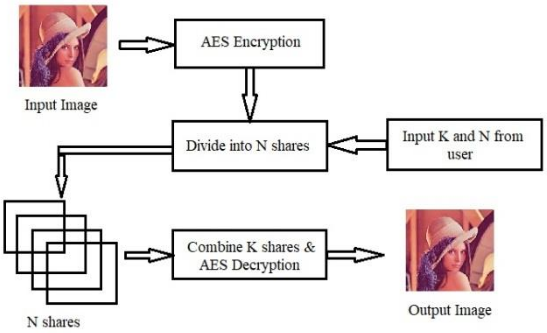

Figure 6. Block Diagram

3.1. Encryption Process:

User will have to provide the key for encryption using AES (Advanced Encryption Standard). Key also goes along with the shares to the end user. Encrypted image shown in figure 7. Now, encrypted image is divided into shares using visual cryptography. Before Share generation of any image User have to provide the value of K and N. Where N=maximum number of shares of an image & K= minimum number of shares require to regenerate the original image.

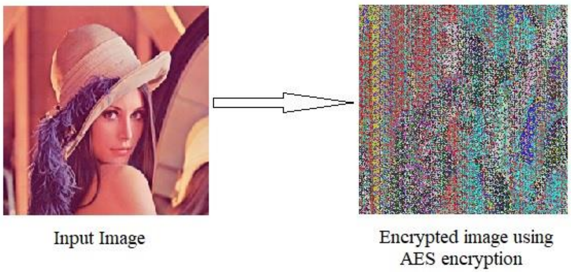

Figure 7. Original and Encrypted Image

3.2. Share Generation:

To overcome the increasing size problem, following approach is used for share generation. Assuming an input 24-bit bitmap colour image which each 3-byte sequence in the bitmap array represents the relative intensities of red, green, blue. Firstly, decompose the colour image into three planes under additive model as shown in figure 8. By this way we can generate the N shares of the colour image.By considering 4 pixel of input image at a time and then generating 4 output pixels for each share. There are 16 cases which are in 5 Categories as shown in Table 1. Shares and symmetric key is transmitted to the receiver. We can also send the symmetric key into shares for more security.

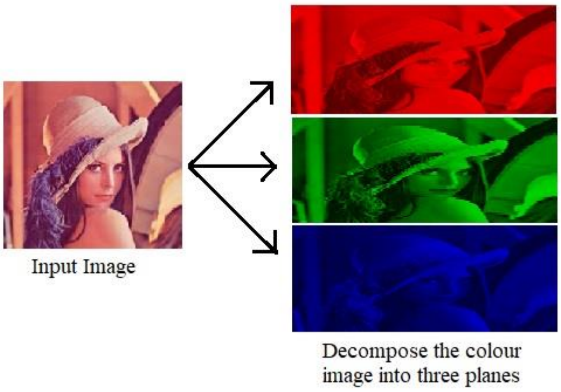

Figure 8. Decomposing of original image into R-G-B planes

Table 1. No. of ways to generate the Share to get minimum size

Cases	original image	No. of ways	share1	share2
4 original pixels are white	⊞	1	▄	▄
4 original pixels are black	█	1	▌	▐
Any 2 pixels are black & 2 are white	▚	6	▐	▄
Any 3 pixels are white & rest is black	▘	4	▚	▚
Any 3 pixels are black & rest is white	▛	4	▄	▐

Shares Generation from Original Input Image without encryption of the image shown in figure 9.

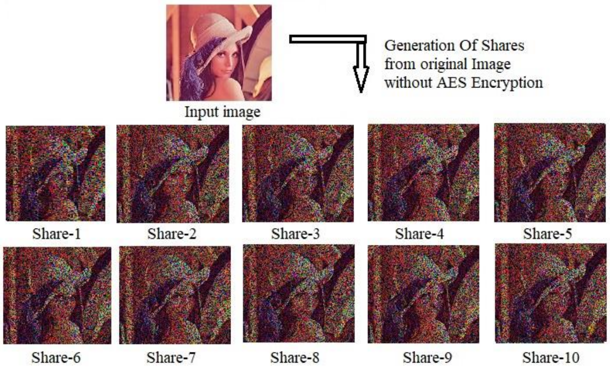

Figure 9 . Generated shares of original image

From the figure 9 we clearly observed that anyone can read our secret image from shares. So it is important to encrypt our original image then generate the N number of shares as shown in figure 10.

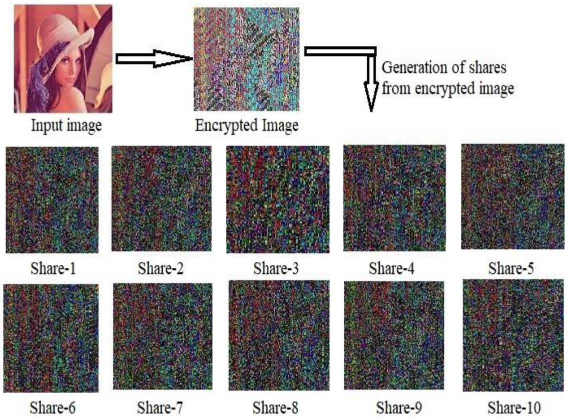

Figure 10. Generated shares of Encrypted image

3.3. Decryption Process:

At Receiver site, the end user needs only K out of total N shares to generate the original image. After the original image is generated it is still in encrypted form as shown in figure 11. The key which is used to encrypt the image is now required again to decrypt it, thus providing an additional level of security. Now original secret image is recovered as shown in figure 11.

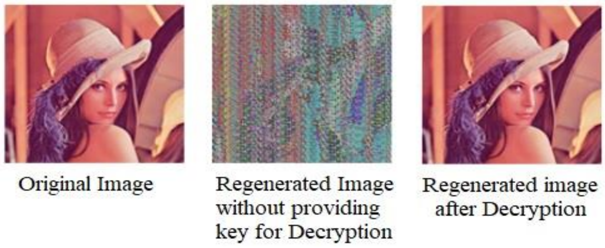
Original Image
Regenerated Image without providing key for Decryption
Regenerated image after Decryption

Figure 11. Effect of Decryption on the regenerated image

IV. RESULT

The above mentioned scheme is implemented into "MATLAB R2017a". The results are as our expectation shown in figure 12.

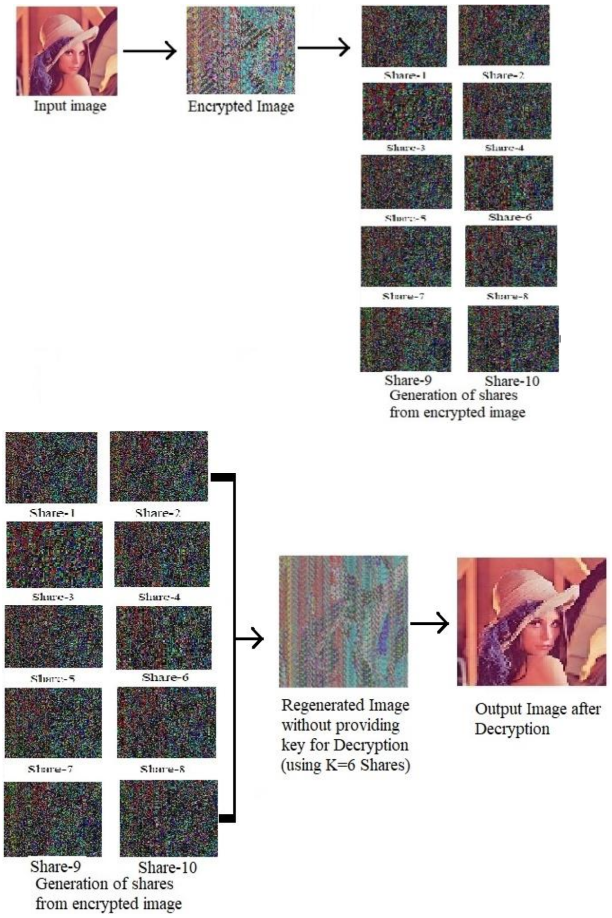
Input image
Encrypted Image
Share-1
Share-2
Share-3
Share-4
Share-5
Share-6
Share-7
Share-8
Share-9
Share-10
Generation of shares from encrypted image
Share-1
Share-2
Share-3
Share-4
Share-5
Share-6
Share-7
Share-8
Share-9
Share-10
Generation of shares from encrypted image
Regenerated Image without providing key for Decryption (using K=6 Shares)
Output Image after Decryption

Figure 12. Outcome of our proposed scheme.

Encrypted image and Shares are also an image, but it is a one kind of noisy image. We try to analyse the PSNR v/s K ratio. Result is shown in figure 13.

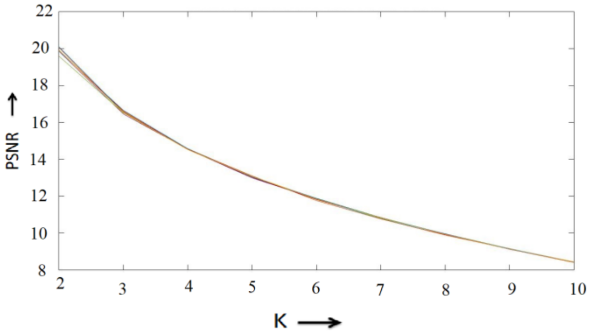

Figure 13 . PSNR v/s K Graph

We can state that if we use less number of Shares to regenerate the image, PSNR of regenerated image is high. It means that if we want to regenerate the image same as our original image we have to use high number of Shares. Our value of K is near to N shares to get appropriate outcome.

V. APPLICATIONS

5.1. Distributed Systems:

Suppose we have N distributed servers. Traditionally if we store a file in only one server, there is a high risk that if it breaks or get hacked, all of our data will be lost. So we would like to store our information in a distributed manner, with each server storing a part of the information. We can encrypt and break our data into N different parts with each part going into a server. Even if N – K servers are broken, we can still generate our original data using the K alive servers.

5.2. Data Transfer Security:

It is obvious that transferring our data through N channels is more secure than transferring all of it through one channel. We can use the above algorithm to encrypt and break data into N different parts and transfer the data simultaneously through N channels. End user can get K shares and ignore the other N – K shares.

VI. CONCLUSION & FUTURE ASPECTS

As conclusion it can be said that, visual information where size and security is more concerned, the proposed visual cryptography scheme is undoubtedly fine and fantastic to use. But, this scheme increases some kind of computation at time of encryption and decryption. This scheme is best suitable for pictures having secret in the form of text. This scheme can be extended for hiding multiple secrets. Instead of symmetric key, any other image can be applied for encrypting original image.

VII. REFERENCES

[1]. Prof. Wu C., Chen L., A study on visual cryptography," Master‟s thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[2]. Sirisha B. L., Lakshmi G. S., A novel cryptographic technique under visual secret sharing scheme for binary image, International Journal of Engineering Science and Technology, Vol. 2(5),2010, pp: 1473-1484.

[3]. Yu B., Xu X., Fang L., Multi-secret Sharing Threshold Visual Cryptography Scheme, International Conference on Computational Intelligence and Security, 2007

[4]. Parakh A., Kak S., A Recursive Threshold Visual Cryptography Scheme, Dept. of Computer Science, Oklahoma State University.

[5]. Jena D., Jena S. K., A Novel Visual Cryptographic Scheme," IEEE,2008, pp. 207-211.

[6]. Kessler G. C., An Overview of Cryptography"- http://www.garykessler.net/library/crypto.html. 28 April 2013.

[7]. Pal J. K., Mamdal J. K., Gupta K. D., A (2, N) Visual Cryptographic Technique For Banking Applications, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[8]. Weir J., Yan W. Q., Sharing Multiple Secrets Using Visual Cryptography, IEEE, 2009

[9]. Naor M., Shamir A., Visual cryptography, Advances in Cryptology EUROCRYPT ‟94. Lecture Notes in Computer Science,1995,(950):pp. 1-12.

[10]. Mandal, J.K.; Ghatak, S. A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography (SCOSVC), Electronic System Design (ISED), 2011 International Symposium on, On page(s): 329 - 334

[11]. Mandal, J.K.; Ghatak, S. Secret image / message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC), Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, On page(s): 263 - 268

[12]. Katta S., Recursive Information Hiding in Visual Cryptography, 2010

[13]. Yue T. W., Chiang S., A Neural Network Approach for Visual Cryptography. Proceedings of the IEE-INNS-ENNS International Joint Conference on Neural Networks(IJCNN‟00) .pp. 1-2.

[14]. Chakraborty U., Paul J. K., Mahapatra P. R. S., "Desigan and Implementaion of a (2,2) and a (2,3) Visual cryptographic scheme". IJCCT Vol.1 Issue 2,3,4; 2010 .