Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 4, April-2016

A NOVEL APPROACH FOR VISUAL CRYPTOGRAPHY BY FUSION OF MULTIPLE SECRET IMAGES

Arundhuti Das[1], Runita Acharekar[2], Akhila Panicker[3], Arushi Khurana[4]

[1]Department of Electronics and Telecommunication Engineering, MES's Pillai's Institute Of Information Technology, Media Studies and Research, University of Mumbai

[2]Department of Electronics and Telecommunication Engineering, MES's Pillai's Institute Of Information Technology, Media Studies and Research, University of Mumbai

[3]Department of Electronics and Telecommunication Engineering, MES's Pillai's Institute Of Information Technology, Media Studies and Research, University of Mumbai

[4]Department of Electronics and Telecommunication Engineering, MES's Pillai's Institute Of Information Technology, Media Studies and Research, University of Mumbai

Abstract- Internet is one of the most popular but insecure communication mediums. Since it is an open and insecure medium, malicious users can intercept data when people transmit personal information. In order to achieve data security, users need secure communication methods for transmitting secret messages over the Internet. Visual Cryptography (VC) is a technique for achieving data security. It is simply a mechanical process in which the original image can be decoded directly by the human visual system. In VC, one secret image is encoded into n shares that are distributed to participants. Each participant cannot retrieve any information from his own transparency, but when at least k of them superimpose their transparencies pixel by pixel, they retrieve the secret from the superimposed result by using their visual system. In this paper, we propose a method that takes two secret images. These are fused together and shares are generated out of this fused image. At the decoding side, shares are overlapped to get the fused image back and then the original secret images are separated.

Keywords- Visual cryptography, Lagrange's interpolation, shares, composite image, fusion, threshold

I. INTRODUCTION

Internet is one of the most popular but insecure communication mediums. People use the internet for all kinds of communication needs including VOIP, peer-to-peer file sharing, up-to-date news reading, e-commerce, and online transactions. Since it is an open and insecure medium, malicious users can intercept data when people transmit personal information. The fast growth of online applications results in the data security problem, which is an important issue for all users. In order to achieve data security, users need secure communication methods for transmitting secret messages over the Internet.

Encryption is a well-known method for achieving data security. It transforms secret information into an encrypted form, which looks like a random message. Transformation procedure is called encryption process and the result is called cipher text. Encryption makes the message unreadable, making message suspicious enough to attract eavesdroppers' attention. A computational device is required to perform decryption of the cipher text. Therefore, the cost or efficiency of the hardware is mostly proportional to the security level of the encryption algorithm. Thus, stronger encryption algorithms need hardware with more processing power. Visual Cryptography (VC) is another technique for achieving data security. It is a cryptographic method in which cipher text can be decoded directly by the human visual system. Decryption process does not require any special calculation or computational device. Thus, it eliminates the drawback of hardware and software requirement, which is essential for the decryption process in traditional cryptography. In VC, one secret image is encoded into *n* shares that contain seemingly random pictures and are distributed to participants. Each participant cannot retrieve any information from his own transparency, but when at least *k* of them superimpose their transparencies pixel by pixel, they retrieve the secret from the superimposed result by using their visual system. Such a scheme is called "(*k*, *n*) visual secret sharing (VSS)" by Naor and Shamir. Any transparencies can be stacked to retrieve secret. Stacking of *k-1* or less does not reveal the secret. Retrieved secret's contrast, when *k* or more transparencies are superimposed, is proportional to the number of superimposed transparencies. Such an interesting scheme's decryption process requires only human visual system instead of any computational device. It is much useful in situations where computing devices are not available or not possible to use.

In this paper, a novel method of visual cryptography for multiple secrets has been proposed. Here, multiple secret images are added together and shares of this fused image are generated. The size of the fused image is same as that of each image hence, less bandwidth is required as compared to sending each secret one at a time.

II. RELATED WORKS

The VSS scheme is based on Lagrange's interpolation. Given a set of points (x_i, y_i), i=0, 1, 2, 3,...., *k-1*, the Lagrange interpolation polynomial can be constructed using:

$$P(x) = \sum_{i=0}^{k-1} y \prod_{i\neq j} \frac{x-x_i}{x_j-x_i}$$

Given a secret, it can be easily shared using this interpolation scheme. If *GF* (*q*) denotes a Galois field (*q*>*n*), the following polynomial is constructed by choosing proper coefficients α_0, α_1, α_2,…, α_{k-1} from GF (*q*), which satisfy:

$$f\,(\mathrm{x}) = \mathrm{s}* + \sum_{i=0}^{k-1} \alpha \mathrm{i} x^{i}$$

where s* is the secret key. The coefficients are randomly chosen over the integers [0, *q*). Suppose $s_i = f(\alpha_i)$, *i* = 0, 1, 2,…, *n*, each s_i is known as a share and they can all be delivered to different persons.

Now, the original secret is to be reconstructed. Suppose *k* people have provide their shares $s_{i,}$ *i* = 1, 2,…., *k*. The following Lagrange polynomial is utilized to construct the original secret:

$$P(x) = \sum_{i=1}^{k} s_i \prod_{i\neq j} \frac{\alpha-\alpha_i}{\alpha_j-\alpha_i}$$

where addition, subtraction, multiplication and division are defined over *GF* (*q*):

$$P\,(\alpha_i) = s_{i,}\ i = 1, 2,.., k,\ s* = P(0)$$

Thus we obtain the original secret s*.

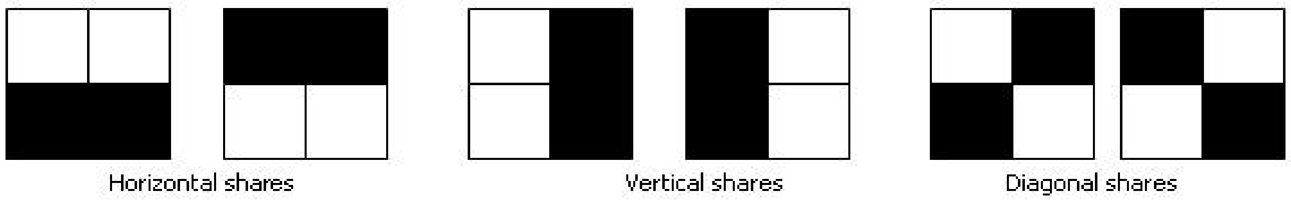
Each pixel appears within n mod versions (known as shares) per transparency. The shares are a collection of m black and white sub-pixels arranged closely together. The structure can be described as an *n* x *m* Boolean matrix *S*. The structure of S can be described thus: $S = (s_{ij})_{mxn}$ where s_{ij} = 1 or 0 i.f.f. the j^{th} sub-pixel of the i^{th} share is black or white.

The important parameters of the scheme are:

m: the number of pixels in a shares represents the loss in resolution from the original image to the recovered one. α: the relative difference in the weight between the combined shares that come from a white and black pixel in the original image, i.e., the loss in contrast. γ: the size of the collection of C_0 *and* C_1. C_0 refers to the sub-pixel patterns in the shares for a white pixel and C_1 refers to the sub-pixel patterns in the shares for a black pixel.

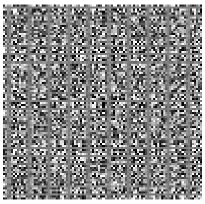
The Hamming weight *H (V)* of the ORed *m*-vector *V* is interpreted by the visual system as follows:

A black pixel is interpreted if $H(V) \leq d$ and white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and a relative difference α > 0.

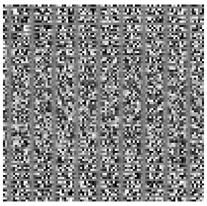


For a (2, 2)-VCS, the following is the implementation and result:

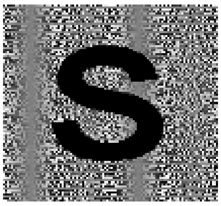
a) Secret Image (108×121)



b) Share 1 (216× 242)



c)Secret Image (216×242)



d) Restored image (216x242)

III. PROPOSED SCHEME

The proposed method uses more than one image. The secret images are added to form a composite image. Any number of secrets can be added together. Shares of the composite image are generated using the traditional visual cryptography. We have implemented (2, 2)- secret sharing scheme i.e. two shares are generated and for recovery both the shares are required. At the decoding end, the shares are superimposed on each other which is a mechanical process. Superimposing the shares retrieves the composite image. Now, each secret image is separated from the recovered composite image.

The main advantage of this scheme is that it encodes more than one secret without extra bandwidth requirement. Each secret is of the same size as that of the composite image.

The flow graph of the paper is shown.

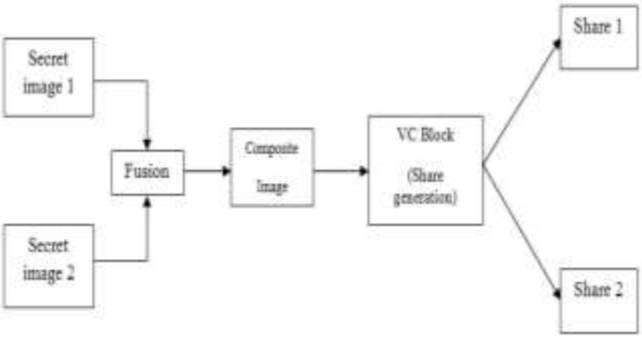


Fig (a)

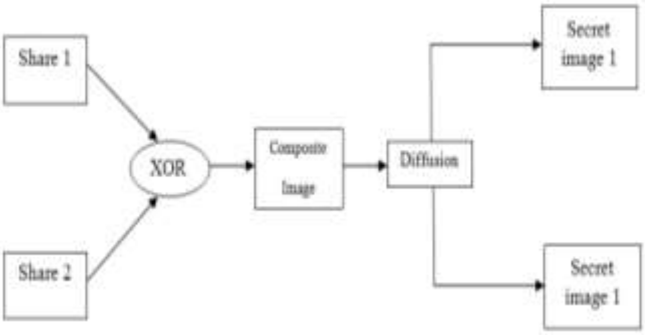


Fig (b)

The first fig. shows two secret images that needs to be sent given as input to the VC block. Prior to share generation, both the images are fused to get a composite image whose shares are generated.

The second fig. shows the overlapping of the two shares. This XOR operation retrieves the composite image and then the secret images are separated from it.

This scheme is easy to implement since the basic of visual cryptography is being used but with the advantage of multiple secret sharing. This results in lesser bandwidth requirement and storage space.

IV. EXPERIMENTAL RESULTS

The implementation of the proposed scheme has been done in MATLAB. MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

The flow of the scheme has been shown below. Fig A shows the two secret images that have to be encrypted. The next fig. shows the composite image which has is formed by the fusion of the secrets.

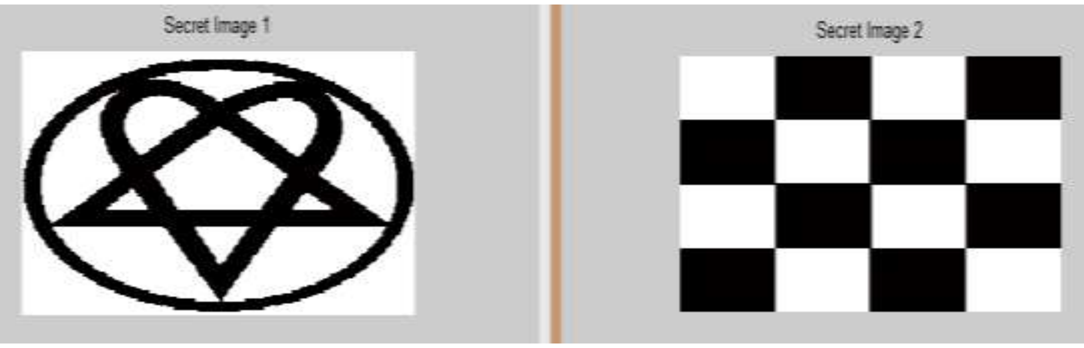


Fig A

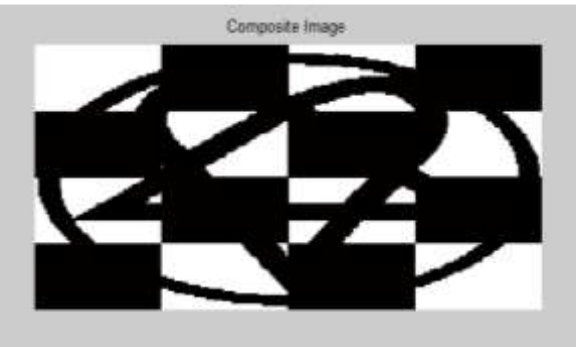
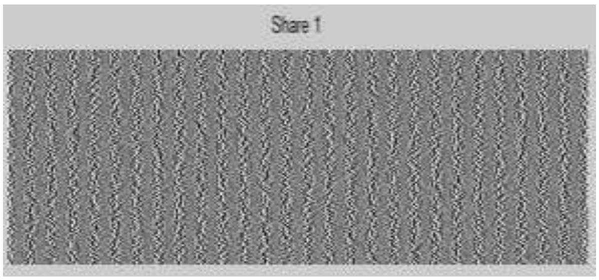
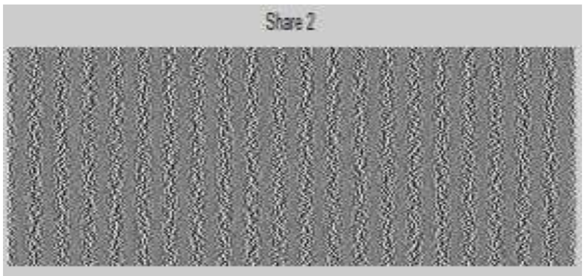


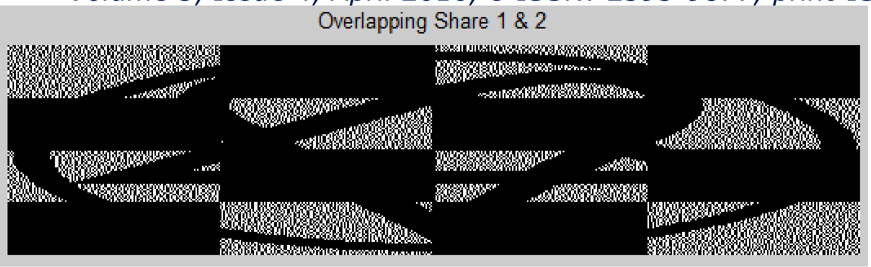
Fig B

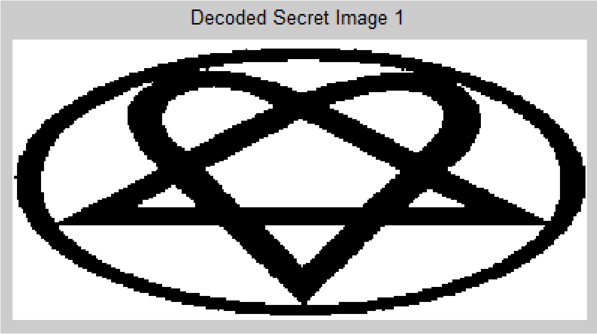
Figs. below are the generated shares out of the composite image.

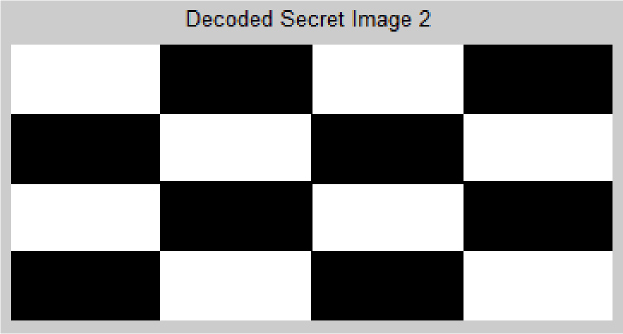




The final outputs are shown as follows: the overlapped recovered image and the decoded original secrets.







V. CONCLUSION

Visual Cryptography is a very secure technique to provide security to data. This paper explains the (2, 2) - VSS which takes two secret images for generation of two shares. It is different from traditional VC since it takes into account multiple secrets instead of a single secret image. It employs fusion of images at the sender and overlapping of the shares followed by separation of them at the receiver. Hence there is no constraint on the bandwidth requirement as well as storage space.

VI. REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography”, Advances in cryptology, Eurocrypt’94, pp.1-12, Springer Berlin Heidelberg, 1995.

[2] B.Padhmavathi, and Dr.P.Nirmal Kumar, “A Novel Mathematical Model for (t, n)-Threshold Visual Cryptography Scheme”, International Journal of Computer Trends and Technology (IJCTT) – volume 12 number 3 – Jun 2014.

[3] S.J Lin and W.H Chung, “A Probabilistic model of (t, n) Visual Cryptography Scheme with Dynamic group”, IEEE transactions on information forensics and security, vol.7, no.1, February 2012.

[4] A Shamir, “How to share a secret”, Communications of the ACM, vol.22, no.11, pp.612-613, 1979.

[5] Lekhika Chettri, “Visual Cryptography Scheme Based On Pixel Expansion for Black & White Image”, Computer Science and Information Technologies, Vol. 5 (3), 4190-4193, 2014.