Vol 5 Issue 3 April 2015

ISSN No : 2230-7850

International Multidisciplinary Research Journal

Indian Streams Research Journal

Executive Editor
Ashok Yakkaldevi

Editor-in-Chief
H.N.Jagtap

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.org

Indian Streams Research Journal ISSN 2230-7850 Impact Factor : 3.1560(UIF)
Volume-5 | Issue-3 | April-2015 Available online at www.isrj.org

HYBRID SCHEME FOR SECRET SHARING USING SYMMETRIC KEY AND MULTI SECRET SHARING

Deepak Dhull
Department of Computer Science, Govt. PG College, Narnaul, Mahendergarh, Haryana, India.

Co - Author Details :

Rakhi Soni
Department of Computer Science, Govt. PG College, Narnaul, Mahendergarh, Haryana, India.

ABSTRACT:

Visual cryptography technique encodes the information in such a way that decoding can be performed by human visual system without any intricate decoding process. It is a special encryption technique in which any text/secret which has to be encrypted is taken in the form of images. It slice image into randomly looking noise called shares, which when stacked together in any manner with proper alignment reveals out the secret. As visual cryptography, is a secure method for transmitting secret, but it has its cons also. If someone gets access to all shares, he/she can divulge secret easily. The proposed technique first encrypts the secret using a symmetric key and then divides the secret into shares. After overlapping of shares, secret is not appears, until the symmetric key is not known. This paper discusses multi secret sharing schemes in which m secrets can be implanted into m shares, hence reducing memory wastage and enhancing security.

KEYWORDS

Multi Secret Sharing Scheme, Hybrid of Symmetric key and Visual Cryptography, Image Steganography, Visual Cryptography.

I.INTRODUCTION:

To prevent information forged by unauthorized person is most critical demand in present days. As the internet user is growing exponentially due to advance in information technology and instant access, this demand become more significant. Most widely used technique to prevent unauthorized access & misuse of information is cryptography. Cryptography is the study and implementation of techniques to hide information, or simply to protect a message or text from being read. The process of making the information unreadable is encryption, reversing this process and retrieving the original readable information is called decryption. Yet encryption and decryption process in cryptology needs complex computations. Generally, efficiency and cost of Hardware/Software performing decoding is proportional to security of encryption algorithm.

In order to secure data and reduce 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 decode the original secret. A (p,n)-threshold visual cryptography scheme[6] in which a secret is chopped into n pieces (called shares) such that for 2=p ≤n and delivers them to n participants. If someone has only p-1 shares then no information about secret leaks. At least p no. of participants can reveals the actual image if their shares are stacked properly in proper orientation. But fewer than p shares gets no information about the secret. This is referred as 'p out of n' VCS [2] and symbolically written as (p,n) VCS. One drawback of this scheme is the share size which is 4 times the size of main secret, hence consumes more bandwidth at time of transmission as well as more storage.

The main problem of mostly visual cryptography scheme for binary image is that the decrypted image size is larger than original and also some security issues are present. The proposed VCS have tried to overcome both issue. In the proposed scheme m secrets can be implanted into m shares, and the size of shares is same as original while security is provided using the concept of symmetric key encryption, hence reducing memory wastage and enhancing security.

II.RELATED WORK

Visual cryptography developed by M. Naor and A. Shamir described general (p,n) VCS. When shares are combined using OR/XOR operation, grayed secret image recovered. They designed (2,2) VCS using 4 sub pixels, it means one pixel of original image generates 4 subpixels in each share. Hence share size is 4 times as original. Here are some generated share for their (2,2) scheme[3][6].

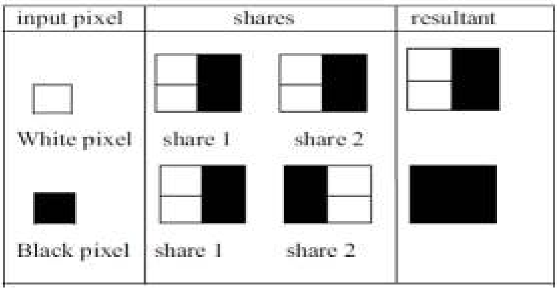


Figure 1: Shares used by Naor and Shamir in(2,2) VCS

Tai-wen Yue and Chiang[8] introduces a modified scheme in which the share dimension is twice of original in horizontal direction while remains same in vertical direction. Its contrast is same as Naor and Shamir 2 out of 2 scheme.

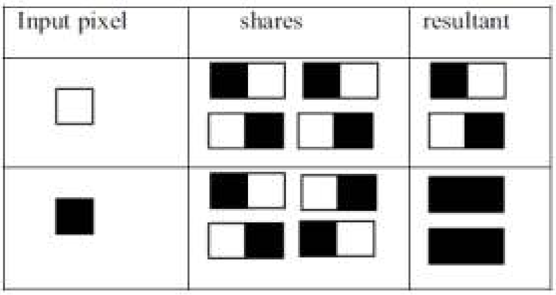


Figure 2: Shares used by Tai-wen and Suchen Chiang

In 1998, Chen and Wu proposed a novel (2,2) threshold visual cryptography scheme. The first secret image is decrypted by stacking two transparencies. And the second one is decrypted in same manner but one share is rotated. The process for creating shares for both secrets is shown below. Sender distributes share A and B between two participants and for decryption with present two participants, by stacking share A and B, secret image 1 appears and stacking share A on share B with 90 degrees rotation in clockwise then secret image 2 appears.

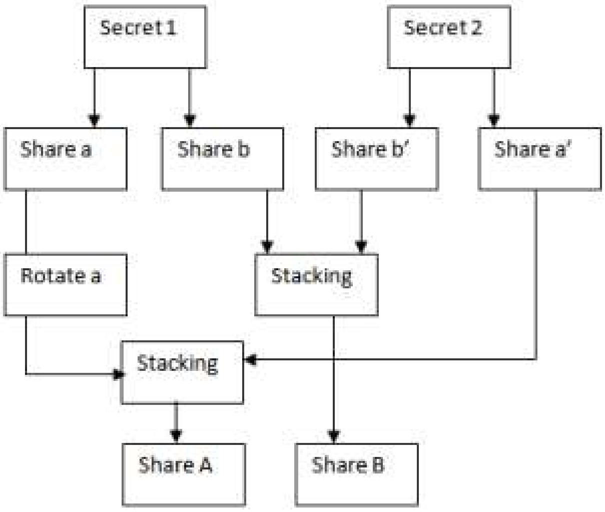


Figure 3: Flowchart of (2,2) VCS

All the above mentioned schemes increase the size of shares and loss visual fidelity.

III.THE SCHEME

VCS is used to make data secure by dividing secret image into a number of shares. These shares are distributed among authorized participants via different transmission mediums. So that intruder has less chance to forged or intercepts data. But it is not more secure, if someone gets access to all shares, he/she can easily decrypt the secret. This can be made more secure by introducing a symmetric key for encryption and decryption both.

The proposed scheme consider security of secrets in terms of encrypting it with the help of symmetric key, hence if someone access all the shares in unauthorized way, he/she cannot decrypt it completely without symmetric key. This scheme manages security as well as decrypted secrets are of same size as original. The scheme is divided into three parts:

- Encryption of original secrets using symmetric key.
- Generation of Shares
- Decryption of Secrets.

A.Encryption Process

Two secret image and key to be transmitted are inputs for encryption process. It should be noted that key size is much less than image size.

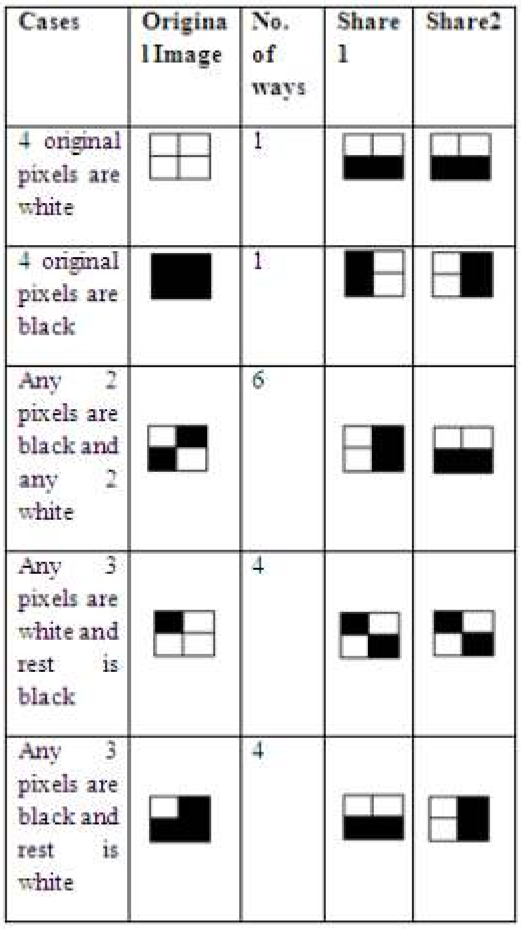
•Divide images into blocks such that block size equals to key size.
•Each block is XORed with key and then placed again in its original position.

Now, encrypted image is divided into shares using visual cryptography.

B.Share Generation

To overcome the increasing size problem, following approach is used for share generation. By considering 4 pixel of input image at a time and then generating 4 output pixels for each share [5]. There are 16 cases which are in following 5 Categories.

TABLE I
CASES FOR SHARE GENERATION



Cases	Origina lImage	No. of ways	Share 1	Share2
4 original pixels are white	⊞	1	▄	▄
4 original pixels are black	█	1	▌	▐
Any 2 pixels are black and any 2 white	▞	6	▐	▄
Any 3 pixels are white and rest is black	▘	4	▚	▚
Any 3 pixels are black and rest is white	▟	4	▄	▐

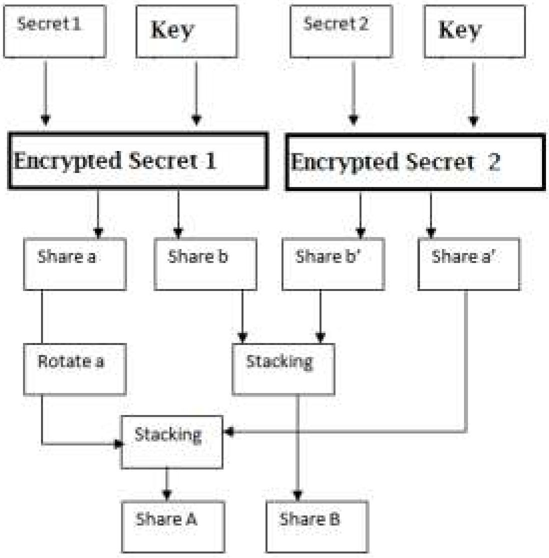
Shares and symmetric key is transmitted to the receiver. We can also divide the symmetric key into shares for more security.

C.Decryption Process

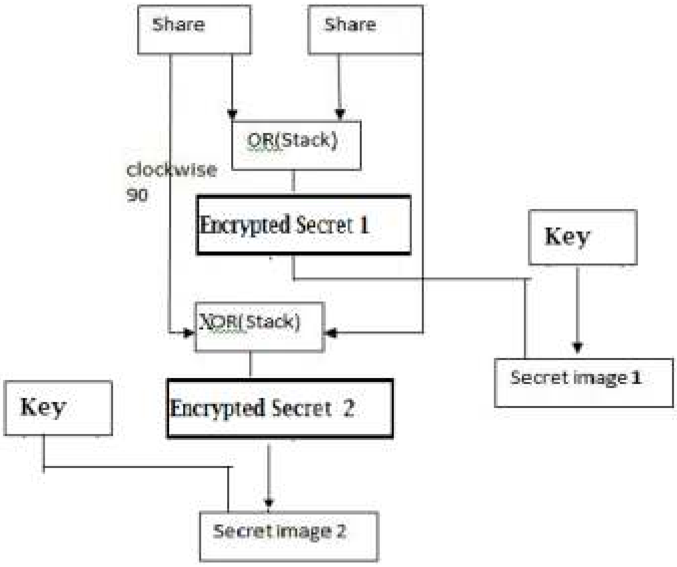
At Receiver site, first encrypted secret is recovered by stacking two shares and the second one is recovered in the same manner but rotating first share. Decrypt the images as below

- Divided into blocks such that block size equals to key size.
- Each block is XORed with key and then placed again in its original position.

Now original secret images are recovered.



Encryption Process



Decryption Process

IV.CONCLUSION AND FUTURE SCOPE

Visual cryptography provides a secure way to transfer images. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. The Multi Secret sharing schemes increases size of decrypted image and security gets ruined if someone has access to all shares. The proposed scheme improves with respect to size and security with a limitation of aspect ratio of original image cannot be maintained.

As conclusion it can be said that; the proposed visual cryptography scheme is undoubtedly fine and fantastic to use where size and security of original secret is of more concern. 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 technique can be applied to many applications in real and cyber world.

This scheme can be extended for colored images. Instead of symmetric key stream cipher can be applied for encrypting images.

V.REFERENCES

[1]Abhisek Parakh and Subhas Kak, " A Recursive Threshold Visual Cryptography Scheme", Dept. of Computer Science, Oklahoma State University.

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

[3]Debasish Jena and Sanjay Kumar Jena, "A Novel Visual Cryptographic Scheme", IEEE,2008, pp. 207–211.

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

[5]Jonathan Weir, WeiQi Yan, " Sharing Multiple Secrets Using Visual Cryptography" , IEEE Transactions on Information Theory, 2009

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

[7]Sandeep Katta," Recursive Information Hiding in Visual Cryptography,"2010

[8]Tai- Wen Yue and Suchen Chiang, "A Neural Network Approach for Visual Cryptography". Proceedings of the IEE-INNS-ENNS International Joint Conference on Neural Networks(IJCNN'00) .pp. 1-2.

[9]Ujjwal Chakraborty, Jayanta Kumar Paul and Priya Ranjan Sinha Mahapatra, "Design and Implementation of a (2,2) and a (2,3) Visual cryptographic scheme". IJCCT Vol.1 Issue 2,3,4; 2010 .