INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

Multi Secret Sharing Techniques using Visual Cryptography

Rakhi Soni[1], Poonam Soni[2], Shivani Raina[3]

[1, 2, 3] M.Tech (CSE), Department of Computer Science and Applications (DCSA)
KU, Kurukshetra, Haryana, India
rakhisoni91@gmail.com[1] , soni.poonam1989@gmail.com[2] , shivani.raina251@gmail.com[3]

Abstract: *Visual cryptography is a special encryption technique in which any text/secret which has to be encrypted is taken as an image. It chops image into randomly looking noise called shares, which when stacked together in any manner with proper alignment reveals out the secret. This decoding process is done via human visual system without any complex computations. In most of current visual cryptography schemes only one secret is lodged into 2 or more shares, which are larger in size than the original secret, thus results in more bandwidth and memory wastage. This paper discusses multi secret sharing schemes in which m secrets can be implanted into m or m+1 shares using rotation or master key concept, hence reducing memory wastage and improving security.*

Keywords: *Multi Secret Sharing Schemes, Visual Cryptography, (2, m+1) Secret sharing scheme, Image Steganography.*

1. 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 in which plain text is converted into cipher text (unreadable form) using some mathematical computations. 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.

Visual cryptography is a new kind of security technique in which plain text (in terms of images) can be decrypted directly by human visual system. The binary image is encoded into two shares which are looking random pictures. Dealer distributes the two shares to two participants. Independently, the participant cannot tell anything about secret, but when the two transparencies stacked together, they recognized the secret. Neither computational device nor cryptographic knowledge is required for decryption process. However, in this scheme the size of shadow images is usually larger than or equal to secret image.

A (p,n)-threshold visual cryptography scheme 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. For reconstruction of secret at least p shares are needed. In such a model, the recovered secret image can be darker or lighter than the background. 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.

2. VISUAL SECRET SHARING SCHEME

Visual cryptography was proposed by Naor and Shamir [1] in 1994. The primary property of VC is using a method called stacking shares to recover secret message. Stacking means inserting shares on top of one another. The owner or dealer creates 2 or more shares for secret message. Receiving all secret, printing them on transparencies, and stacking all together, the secret message becomes visible.

In this way, VC has proven to provide perfect security. Furthermore, in group secret system, which is using (k,n) threshold visual secret sharing scheme, n shares of secret is distributed among n participants. When recovering the secret message , only k or more transparency stacks are required without any computation.

The main points of Naor and Shamir’s schemes

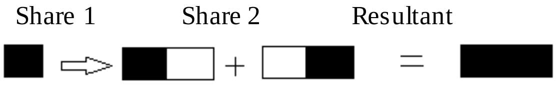
- The secret is chopped into n pieces

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

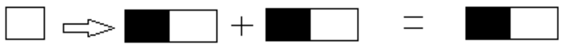
- Any k or more than k pieces need to recover secret
- Any k-1 or fewer than k pieces cannot compute the secret message.

Each pixel in secret is expanded upto four sub pixels that consist of black and white pixels value according to the patterns.

1. Each pixel is broken into two sub pixels as follows.

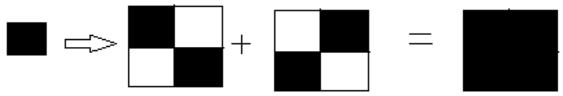


For Black

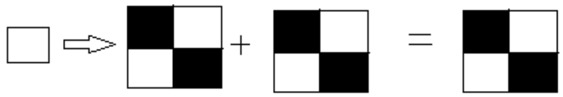


For White

2. Each pixel is broken into four sub pixels as follows.

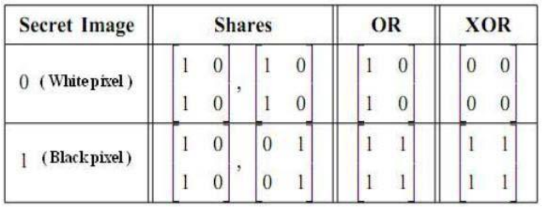


For black



For white

Two share of a white secret pixel are of the same while those of a black secret pixel are complementary. Using this basic VCS Scheme we can-not completely recover the white Secrete pixel which causes loss in contrast. In XOR based VCS scheme where the share images are superimposed using XOR operation which results in perfect reconstruction of both Black and white pixels.



Secret Image	Shares	OR	XOR
0 (Whitepixel)	$\begin{bmatrix}1&0\\1&0\end{bmatrix}, \begin{bmatrix}1&0\\1&0\end{bmatrix}$	$\begin{bmatrix}1&0\\1&0\end{bmatrix}$	$\begin{bmatrix}0&0\\0&0\end{bmatrix}$
1 (Blackpixel)	$\begin{bmatrix}1&0\\1&0\end{bmatrix}, \begin{bmatrix}0&1\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$	$\begin{bmatrix}1&1\\1&1\end{bmatrix}$

Example:

Figure 3(a): original binary image

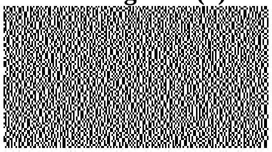


Figure 3 (b): share1

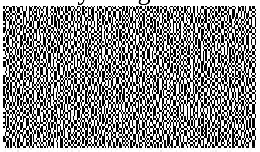


Figure 3 (c): share2

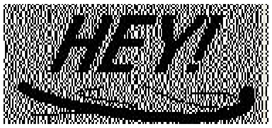


Figure 3 (d): Decrypted image using OR operation

Figure 3 (d): Decrypted image using XOR operation

A recursive visual cryptographic method proposed by Monoth et al. [7] is computationally complex as the encoded shares are further encoded into number of sub shares recursively.

3. MULTI SECRET SHARING SCHEMES

A. For encrypting 2 secret image into 2 shares: 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.

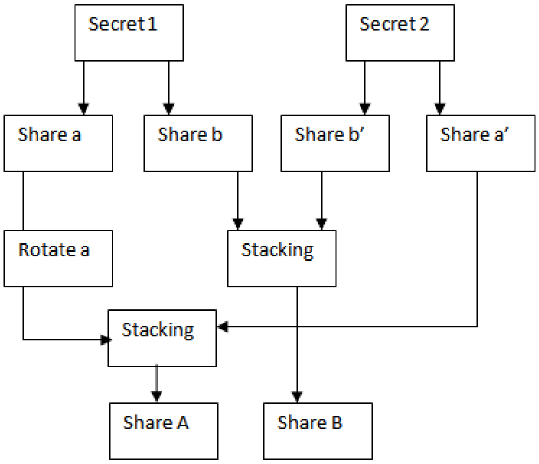


Figure 1: Flowchart of (2, 2) VCS

B. An (3, 3) - VSS Scheme for hiding three secrets: Tsai and Wang [] proposes a new visual secret sharing scheme to embed more information and have more secure than traditional visual cryptography. The three secret messages are passed through the first coding process to generate the share A and share Temp. The second coding process is used to generate share B and share C from the share Temp. Share A, share B, and share C are transmitted.

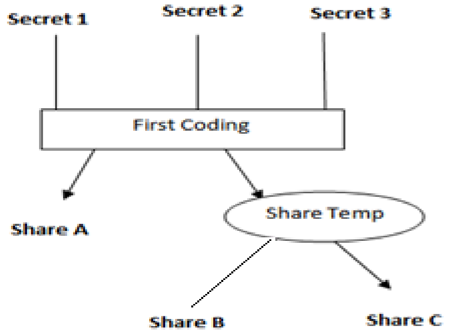


Figure 2: Process for generating share A, B, C

For decoding process, after getting the three shares, share B and share C are logic XOR to create a temporal image-share Temp. The first secret image can be obtained by stacking the share A and the share Temp. Then the second secret information can be obtained by stacking the clockwise 90^0 rotation of the share A and share Temp. The third secret information is obtained by stacking the counter clockwise 90^0 rotation of the share A and the share Temp.

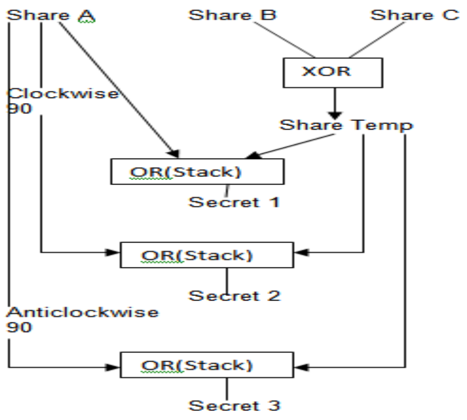


Figure 3: Regenerating secret 1, 2, and 3

C. *Multiple secret sharing using Master Key*

In this scheme, Shares are generated for each secret using master key. After merging all the shares in a combined share, master key is adjusted and a new key is generated. The secrets are revealed when the key is superimposed on the combined share in different locations

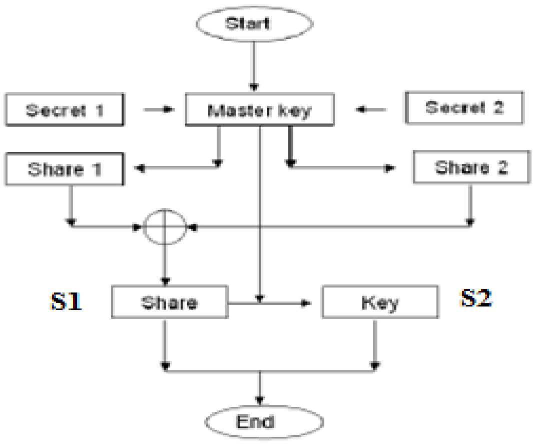


Figure 4: Flowchart for combined shares visual secret sharing scheme

The new share S1 and the key share S2 are employed to recover the secrets by shifting the key share S2 to various positions on S1.

The master key is a randomly generated image using the patterns of visual cryptography. It is generated using a random one-time pad, which makes it to be unconditionally secure. This means that even if an adversary knows how to generate the master key or the shares they will have no clues as to how they can reconstruct the hidden secrets. After the master key is generated using the random one-time pad, the pad is discarded, leaving no evidence as to how the shares or master key generated.

1. ***Disjoint Sharing:*** The basis of disjoint sharing scheme is to share independent images with the same master key and then arrange the shares into one image horizontally, vertically or diagonally. When the key is superimposed on the combined image, the secret will become appears. If the shares are arranged vertically, shifting the key in the vertical direction will reveal all the secrets. Instead of generating two shares in the traditional visual cryptography, one share is combined from various shares using the master key. It has the ability to compose any size of shares.

2. **Joint Sharing:** In joint sharing, a user has to generate two shares based on the original visual cryptography scheme, like the disjoint sharing with the secure key. There are three different techniques for Joint Sharing.

Contrast Based Joint combination of Shares: To make the combined share, we write the pixels from the corresponding patterns of black pixels of the first secret onto a blank image as a combined share using visual cryptography. For the second secret, we write the similar pixels on the blank region of the combined share. Left over regions on the combined share, filled using the sharing patterns of white pixels.

The disadvantage of this scheme is that it cannot share the secrets which have been made up fully of black pixels since the second secret will have no place to be embedded in the rest space.

Even-Odd Joint Combination of Shares: To deal with the limitation of contrast based scheme, scanning lines based even-odd joint combination of shares scheme is proposed. Two secret of same size shared via two shares using a randomly generated master key. Merge the shares by filling the first share to the even rows of the combined image and the second share to the odd rows. The resultant share will be twice the size of the secrets. Therefore, the master key has to be adjusted to generate a new key, the key will be employed to restore the secrets. The difference between even-odd joint combination and the disjoint combination of shares is that the key is of the same size as the resultant share with the two hidden secrets. This helps to increase the capacity and security of the scheme as it gives away no indication to the amount of secrets hidden, based on the key size.

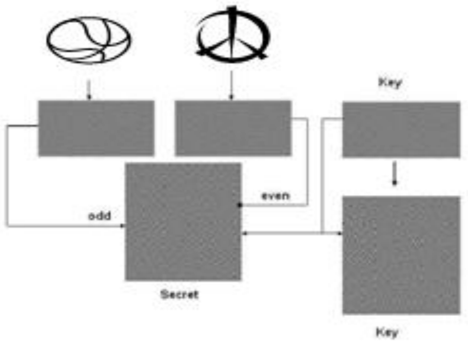


Figure 5: The mechanism for even odd joint combination

When the combined key is superimposed on the final share and shifted up and down, the secrets within are revealed.

Multiple Joint Combinations of Shares: This scheme hides multiple images of a sequence within one share and moving the master key over the share reveals the secrets. Multiple joint combinations of shares works as follows: one pixel from a secret is expanded into a 2 × 2 array. When these arrays are generated, they are moved to a larger image. The same process is repeated for all other pixels in secret one. The same is done for the other three secrets, but they are offset by a certain amount. We hide four secrets within the final share, which is four times as large as the shares which get created per image. The same process is done for creating the key share from the master key, but the ordering is reversed. If it wasn't reversed then simply superimposing the key would reveal all four secrets at once. As such, we have to shift the key by four pixels in each case to reveal the hidden secrets.

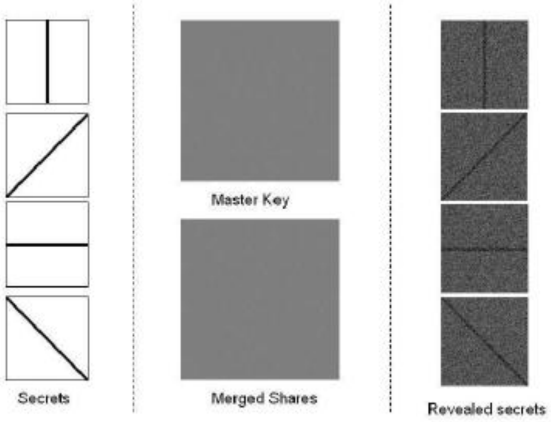


Figure 6: Joint visual cryptography with multiple secrets

4. CONCLUSION

The main drawback of VCS given by Naor and Shamir is; Share's sizes are greater than main secret image, so the transmission of shadow images needs too much storage space and bandwidth. In traditional VCS only one secret is embedded in the shares. In this paper, a no. of multi secret sharing schemes for visual cryptography are revised that hides 2 or more secrets.

In (2,2)-threshold and (3,3) visual cryptographic scheme, secrets images are decrypted by rotating one share and stacking with another which make it limited in use. Multi secret sharing scheme using Master key is highly advantageous and more secure. After moving the key over combined share secret images are recovered. The most interesting and secure thing in Even odd joint combination of share is; key size is same as merged share. As equal key size makes it harder for intruders to determine the number of secrets. For hiding multiple images of a sequence multiple joint combinations of shares is used.

5. FUTURE WORK

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 forge 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. Using the key, secret is first encrypted and then divided into shares. If intruder has k number of shares, he/she is not able to reveals secrets until the intruder doesn't have the symmetric key. Here, the symmetric key used for encryption and decryption may be a small image.

REFERENCES

[1] A. Shamir, How to Share a Secret. Communications of the ACM. Vol:22, 1979, pp : 612-613.

[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] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[4] E. Verheul, H.V. Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs,Codes and Cryptography, 1997, pp.179–196.

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

[6] M. Gnanaguruparan, S. Kak, "Recursive Hiding of Secrets in Visual Cryptography". Cryptologia Vol: 26, 2002, pp: 68-76.

[7] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt '94, vol. 950, pp. 1 – 12, 1994.

[8] Rezvan Dastanian, Hadi Shahriar Shahhoseini," Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares," In Proceedings of IPCSIT 2011 International Conference on Information and Electronics Engineering, Volume.6, Singapore, 2011.

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

[10] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644 – 654, November 1976.