Multiple Secret Sharing Using Graphical Masking

Neha Patil[1], Seema Bhardwaj[2]
[1, 2] Department of Computer Engineering
[1, 2] AISSMS IOIT, Pune

Abstract- *Information transfer via internet is very common. To ensure information safety in todays electronic era is very much needed. Traditional cryptographic techniques are usually used to protect the data. By this techniques data become disordered after encryption and decryption can be done by correct key only. So this all process is computationally difficult.*

Visual cryptography was first introduced by Naor and Shamir in 1994, which requires only human visual system(HVS) to decrypt data instead of any computation. To encode a secret image into n shadow images (shares), they suggested a (k,n) threshold visual cryptography scheme, where only k or more than k shares can recover original secret otherwise failure occurs. Advantage of this scheme is that there is no computation overhead to recover secret image.

Main drawback in visual cryptography is pixel expansion in share generation. Again lot of work is going on in this area. Using graphical masking share created are exactly of same size of original image and it will reduce processing overhead also. As there is no pixel expansion the overhead of storage and communication can be reduced but also raises the capacity of secret communication.

Keywords- secret sharing, graphical masking, pixel expansion

I. INTRODUCTION

Naor and Shamir established visual cryptography as a visual variant of the k out of n secret sharing problem. In a secret sharing scheme, one wishes to randomly divide a secret amongst a group of n individuals in such a way as to allow any k < n of them (or, in certain cases, only a qualified subset of them), to recover the secret from their individual shares. However, any number of individuals less than k should be prevented from obtaining any information about the original secret by combining their individual shares. Similarly, in a VC scheme, shares are generated from the original image according to rules of the scheme in such a way as to provide no information about the encrypted image individually, but to produce a reasonable depiction of the original image when superimposed. The original image should be visible after overlaying its shares.

While VCS has its own strengths, visual cryptography schemes are typically lossy and produce decrypted images that are often noisy or suffer from diminished contrast and resolution. VCS also suffer from pixel expansion leads to the space requirements. And most important is that the VCS is unable to achieve the original image as it is.

Here in this paper we have proposed an algorithm to overcome the problems faced by VCS. We tried to protect pixel expansion and at the end, retrieving original image with better quality.

Our basic idea is based on the fact that every share should have some bits missing and those missing bits will be replenished by exactly (k-1) other shares but not less than that. So every individual bit will be missed from exactly (k-1) shares and must be present in all remaining (n-k+1) shares, thus the bit under consideration is available in any set of k shares but not guaranteed in less than k shares. Now for a group of bits, for a particular bit position, (k-1) number of shares should have the bit missed and (n-k+1) number of shares should have the bit present and similarly for different positions there should be different combinations of (k-1) shares having the bits missed and (n-k+1) number of shares having the bits present. Clearly for every bit position there should be ${}^{n}C_{k}\text{-}1$ such combinations and in our scheme thus forms the mask of size ${}^{n}C_{k}\text{-}1$, which will be repeatedly ANDed over the secret in any regular order. Different masks will produce different shares from the secret. Thus 0 on the mask will eliminate the bit from the secret and 1 in the mask will retain the bit forming one share. Different masks having different 1 and 0 distributions will thus generate different shares. Next just ORing any k number of shares we get the secret back but individual share having random numbers of 1's & 0's reflect no idea about the secret

II. LITERAURE SURVEY

Popular solution for image encryption is Visual cryptography. Image encryption is done using secret sharing concept and shares are created. Shares created are noise like secure images which are transmitted or distributed over an untrusted communication medium. Decryption of secure

image is done using the properties of HVS and there is no need of any knowledge of cryptography.

1. Sharing Single Secret

Recently visual cryptography is implemented by using many new methods. Visual Secret Sharing Scheme(VSSS) is developed by Naor and Shamir in 1994[1]. An binary image (picture or text) is transformed into n sheets of transparencies of random images in k out of n VSSS. When any k sheets of the n transparencies are put together, the original image becomes visible. but it can not reveal the secret by any combination of less than k sheets. In this scheme, one pixel of the original image is reproduced by m subpixels on the sheets. if the number of transparent subpixels is more than a constant threshold , the pixel is considered on (transparent) and if the transparent subpixels is less than a constant lower threshhold, it is considered as off, when the sheets are stacked together The difference between the on and off threshold number of transparent pixels is contrast. A visual cryptography scheme is a broad spectrum method which is based upon general access structure. Any k shares will decode the secret image, in k-out-of-n secret sharing scheme, which reduces security level.

Xiao-Qing and Tan[5] suggested threshold visual secret sharing schemes based on binary error correcting code. Simple XOR and OR operations are used for stacking of images. This scheme have much better resolution than OR based counterparts. General k out of n schemes based on binary linear error-correcting code is suggested and showed that these two schemes are ideally contrast. Share generation is random.

2. Sharing Multiple Secrets:

H.-C.Hsu, T.-S. Chen,Y.-H.Lin[6] proposed a scheme based on angle rotations to encrypt secret image.To indicate the encryption functions a stacking relationship graph of secret pixels and share blocks is generated and two share images are generated according to this graph by defining a set of visual patterns. Based on the stacking properties of these patterns, the secret images can be obtained from the two share images at aliquot stacking angles. As a result, the proposed scheme increases visual secret sharing schemes' ability for multiple secrets. Random shares are generated during encryption.

Angle restriction drawback of above scheme is removed by Wu and Chang[7] by encoding shares to be circles. Wu and Chang refined this idea in 2005. To embed two sets of confidential messages into different angle degrees of the shares, it adapts circular shares.

Idea of multiple secrets sharing in visual cryptography is first introduced by S J Shyu in 2007[8]. Encoding a set of n 2 secrets into two circle shares is introduced here. With n different rotation angles the n secrets can be obtained one by one by stacking the first share and the rotated second shares. This scheme is very helpful to encode unlimited shapes of image and to remove the limitation of transparencies to be circular. This is the first true result that shows the sharing ability in visual cryptography up to any general number of multiple secrets in two circle shares.

Reversible visual cryptography scheme is offered by Fang in 2007[9]. Two secret images are encoded into two shares in this scheme. One secret image appears with just stacking two shares and the other secret image appears with stacking two shares among which one is reversible. VC in reversible style is one of the brand new type developed by Fang[10].

In 2008 Bang Feng et al developed a visual secret sharing scheme for hiding multiple secret images into two shares. This new scheme analyzes the secret pixels and the corresponding share blocks to construct a stacking relationship graph, in which the vertices denote the share blocks and the edges denote two blocks stacked together at the desired decryption angle. The proposed scheme improves visual secret sharing schemes ability for multiple secrets by generating random shares[10].

To provide more randomness for generating shares Mustafa Ulutas[11] proposed secret sharing scheme based on the rotation of shares. Here shares are rectangular in shape and random in nature. In first step stacking the two shares reconstructs the first secret.In second step rotating the first share by 90 counterclockwise and stacking it with the second share reconstructs the second secret. This is new novel algorithm to create both shares from two secrets with improved randomness.

Tzung-Her Chen proposed the multiple image encryption schemes by rotating random grids[12]. Beauty of this scheme is that there is no pixel expansion and codebook redesign. As there is no pixel expansion the overhead of storage and communication can be reduced but also raises the capacity of secret communication. Wen-Pinn Fang proposed a novel reversible visual secret sharing method. If we stack two transparencies directly, a secret image will appear without any computing. Another secret image will unveil, when stacking of two transparencies after reversing one of transparencies.

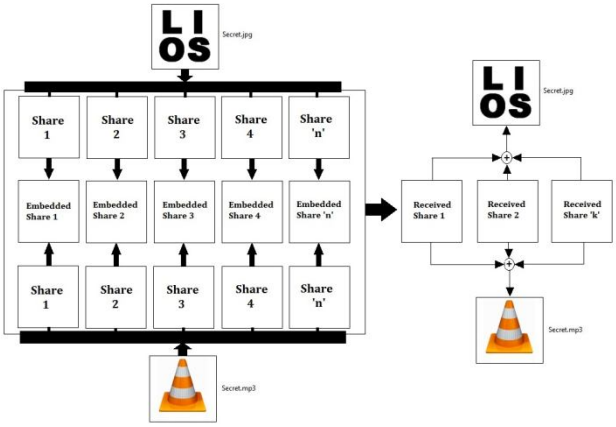
This is one of the best non expansion reversible visual cryptography style[13].

A new scheme based on correlative matrices set and random permutation is presented by Zhengxin Fu and Bin Yu in 2009[14]. This scheme is called as rotation of visual cryptography scheme which can be used to encode four secret images into two shares. Experimental results show that four secrets can be recovered clearly by stacking two shares with different angles and the shapes of the reconstructed images do not have distortions. Based on concept of master key Jonathan Weir suggested sharing multiple secrets using visual cryptography. A master key is generated for all the secrets and secrets are shared using the master key and multiple shares are obtained[15].

Daoshun Wang, Feng Yi, XiaoboLi[28] developed a general construction method for single or multiple and binary, gray scale, color secret images using matrix extension utilizing meaningful shares with of suggested. To utilize meaningful shares by using matrix extension algorithm, any existing visual cryptography scheme with random-looking shares can be easily modified.

III. IMPLEMENTATION DETAILS

Architecture:



IV. CONCLUSION

In this paper, a visual multiple secrets sharing scheme with no pixel expansion has been proposed. In multiple secret sharing using graphical masking , there is no pixel expansion in share generation. As there is no pixel expansion the overhead of storage and communication can be reduced but also raises the capacity of secret communication. Recovered secret images are having better visual quality as compared to previous results present in the literature.

REFERENCES

[1] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). “Visual ryptography for general access structures”, Information and Computation, 129, 86–106.

[2] Blakely, G. R. (1979). “Safeguarding cryptography keys”, Proceedings of the National Computer Conference, 48, 313–317.

[3] Chang, C.C., Lin, C.C., Le, T.H.N., & Le, H.B. (2008). “A new probabilistic visual secret sharing scheme for color images”, Intelligent information hiding and multimedia signal processing. In IIHMSP ’08 international conference on August 15–17, 2008, pp. 1305–1308.

[4] Chen, Y. F., Chan, Y. K., Huang, C. C., Tsai, M. H., & Chu, Y. P. (2007). “A multiple-level visual secret-sharing scheme without image size expansion”, Information Sciences, 177, 4696–4710.

[5] Feng, J. B., Wu, H. C., Tsai, C. S., Chang, Y. F., & Chu, Y. P. (2008). “Visual secret sharing for multiple secrets”, Pattern Recognition, 41, 3572–3581.

[6] Hou, Y. C. (2003). “Visual cryptography for color images”,. Pattern Recognition, 36, 1619–1629.

[7] Iwamoto, M., & Yamamoto, H. (2003). “The optimal n-out-of-n visual secret sharing scheme for gray-scale images”,IEICE Transaction Fundamentals, E86–A(10), 2238–2247.

[8] Naor, M., & Shamir, A. (1995). “Visual cryptography.”,In A. De Santis (Ed.). Advances in cryptology: eurprocrypt’94 (Vol. 950, pp. 1–12). Lecture Notes in Computer Science.

[9] Shamir, A. (1979).” How to share a secret.”,Communications of the ACM, 22, 612–613.

[10] Shyu, S. J. (2006). “Efficient visual secret sharing scheme for color images”, Pattern Recognition, 39, 866–880.

[11] Shyu, S. J., Huang, S. Y., Lee, Y. K., Wang, R. Z., & Chen, K. (2007). “Sharing multiple secrets in visual cryptography”, Pattern Recognition, 40, 3633–3651.

[12] Verheul, E. R., & van Tilborg, H. C. A. (1997). “Constructions and properties of k out of n visual secret

sharing schemes", Designs, Codes and Cryptography, 11, 179–196.

[13] Wang, D., Zhang, L., Ma, N., & Li, X. (2007). "Two secret sharing schemes based on Boolean operations", Pattern Recognition, 40, 2776–2785.

[14] Wu, H. C., & Chang, C. C. (2005). "Sharing visual multi-secrets using circle shares", Computer Standards & Interfaces, 28, 123–135.

[15] Yang, C. N. (2004)," New visual secret sharing schemes using probabilistic method", Pattern Recognition Letters, 25, 481–494.

[16] Yang, C. N., & Chen, T. S. (2006). "New size-reduced visual secret sharing schemes with half reduction of shadow size",IEICE Transaction Fundamentals, E89-A(2), 620–625.

[17] Prabir Kr. Naskar, Hari Narayan Khan, Ujjal Roy, Ayan Chaudhuri , Atal Chaudhuri", Shared Cryptography with Embedded Session Key for Secret Audio", International Journal of Computer Applications (0975 – 8887) Volume 26– No.8, July 2011