Visual Secret Sharing Scheme Using Separable Reversible Data Hiding

Mrs.Neha S.Patil[1], Mrs.Vaishali L.Kolhe[2]
[1, 2] Department of Computer Engineering
[1, 2] D.Y.P.COE, Akurdi, Pune,India

Abstract- *To ensure information safety in today's electronic era is very much needed. Previous crypto-graphic techniques are usually used to protect the data. In traditional cryptographic techniques data become disordered after encryption and at the receiver side decryption can be done by correct key only. So this all process is difficult to handle. The basic idea of the visual cryptography model proposed by Naor and Shamir is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. It is perfectly secure and simple way which allows secret sharing without any cryptographic knowledge. To encode a secret image into n shadow images or shares, a (k, n) threshold visual cryptography scheme is used, where k or more than k shares can recover original secret otherwise failure occurs. Main benefit of visual cryptography is that to recover secret image no computation overhead is required. Main drawback in visual cryptography is pixel expansion in share generation. Using graphical masking, shares created are exactly of same size of original image and it will reduce processing overhead also. The overhead of storage and communication can be reduced as there is no pixel expansion and it also raises the capacity of secret communication.*

Our main contribution to the proposed system contains
- *avoiding the pixel expansion through Graphical Masking*
- *generating more secure secret shares using Separable Reversible Data Hiding.*

Keywords- visual cryptography; secret sharing; graphical masking; pixel expansion; entropy Embedding.

I. INTRODUCTION

A secret sharing method which encrypts a secret image into number of shares but requires no calculations or mathematical computations is Visual Cryptography. Simply by stacking the shares together original secret is reconstructed. Visual cryptography was first introduced by Naor and Shamir in 1994, permitting one or images to be encrypted and decrypted. In traditional cryptography decryption requires computational overhead but in visual cryptography no mathematical calculations or knowledge of cryptography is required. The original image becomes visible simply by stacking the shares together.

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 nCk-1 such combinations and in our scheme thus forms the mask of size nCk-1, which repeatedly ANDing 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 secretin italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. LITERATURE SURVEY

Visual cryptography is popular technique for image encryption. Shares are created using secret secret sharing concept in image encryption. Shares created are noise like secure images which are transmitted or distributed over an untrusted communication medium. Decryption of shares created in encryption is done using the properties of HVS and there is no need of any knowledge of cryptography.

A. Sharing Single Secret

Visual Secret Sharing Scheme(VSSS) is developed by Naor and Shamir in 1994[1]. A 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 cannot reveal the secret by any combination of less than k sheets. 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.

B. Sharing Multiple Secrets

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.

H.-C.Hsu, T.S. ChenY.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, secret images can be obtained from the two share images at aliquot stacking angles.

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 types developed by Fang[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.

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. Any existing visual cryptography scheme with random-looking shares can be easily modified to utilize meaningful shares by using matrix extension algorithm,

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 expansions reversible visual cryptography styles[13].

III. PROBLEM STATEMENT DEFINITION

While transmitting the secret data in military application, they need to send a secret map of geographical area to reveal where the action is to be taken. They also need to embed a secret audio or textual file which will reveal a message that contains the action and how the action is to be taken. This secret data is to be sent over media by creating secret shares with the fact that none of the shares will individually reveal the secret. The secret sharing scheme used, must have to adopt the (k, n) scheme that is, any number of k out of n shares can collectively reveal the secret.

Further it is required that the size of each secret share should be as minimum as possible. In fact the size of each share should be as same as the input. And the most important is at the receiver end the received data have to be noise free and with a better quality or we can say that original data must be received.

IV. IMPLEMENTATION DETAILS

A. Design

Using graphical masking shares are created from both the images and audio files then these shares are embedded together using Entropy embedding to increase the strength of secret shares and to get final shares.These shares are divided into two sets, qualified set and forbidden set. When kshares are stacked together then only secret will be revealed otherwise no secret will be revealed. Here we concentrated on achieving original data as it is.

B. Architecture

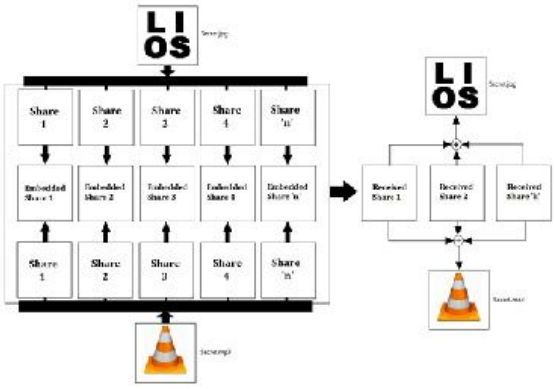

Figure 1. gives proposed system architecture where an image and an audio file are taken as input. Using graphical masking shares will be created separately and by using Entropy embedding, these shares are together and sent over the compromised media. At the receiver side secret will be revealed only if K number of shares received.

In next section we will see the algorithms used for secret share generation and embedding. We will also look for retrieving the original secret.

C. Algorithms

1) Graphical Masking :

Step-1: List all row vectors of size n having the combinationof (k-1) numbers of 0's and (n-k+1) numbers of 1's andarrange them in the form of a matrix. Obvious dimension of thematrix will be $nCk\text{-}1 \times n$.

Step-2: Transpose the matrix generated.

Step-3: Obviousdimension of the transposed matrix will be $n \times nCk\text{-}1$. Each rowof this matrix will be the individual mask for n different shares.The size of each mask is $nCk\text{-}1$ bits, i.e. the size of the maskvaries with the value of n and k.

Step-4: Now create pre-shares as follows:Take the row's bits and Mask 1's bits. Put 1 in pre-share if rows bit and Mask 1's bit are same else put 0.

For 1st bit of rowi.e. 1 and1st bit of mask 1 i.e. 1 so put 1, and for 4th bit 0 and 1 so put 0.
Do this for all the masks.

Step-5: Now do **ANDing** of each mask and corresponding pre-shares i.e. 1st mask and 1st pre-share to get final share.

Step-6: Now if we take any k shares (Tqual) from final shares, **ORing**they will give us the original image row bits.

2) Algorithm for Separable Reversible Data Hiding:

Step-1: Select an Image.

Step-2: Encrypt the image by RC4 encryption method using a key. Let K_{enc}.

Step-3: Calculate number of pixels. Simply height*width.

Step-4: Let K_{perm} is a key for generating pseudo random number generator; create a pseudo random number for each pixel index.

Step-5: Permute the image corresponding to pseudo random numbers.

Step-6: Now take the Data bits to embed.

Step-7: Select a Key to embed the data bits. Let K_{emb}

Step-8: Now replace least two significant bits (2 LSB) of pixel selected by pseudo random value by the data bits.

Here we had done with the embedding process.

3) Algorithm for Decryption and Extracting Data:

Step-1: Reverse permute the Encrypted Image by the K_{perm}.

Step-2: Apply RC4 decryption to decrypt the encrypted Image. Use K_{perm} for decryption.

Step-3: For extracting Data, we need K_{emb}, depending on pseudo random values generated, select the pixel index and take least two significant bits (2 LSB), we get the embedded data bits.

V. RESULTS

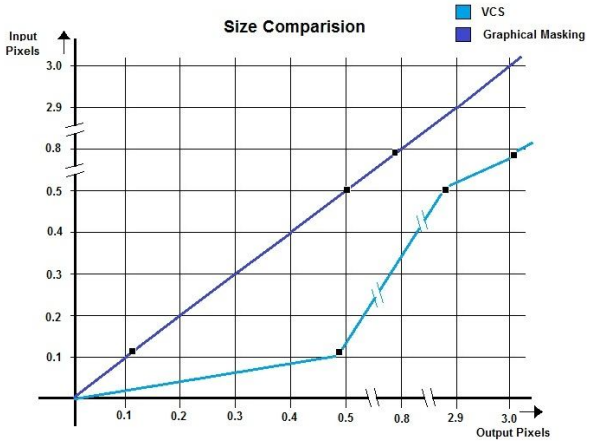

Figure 2.

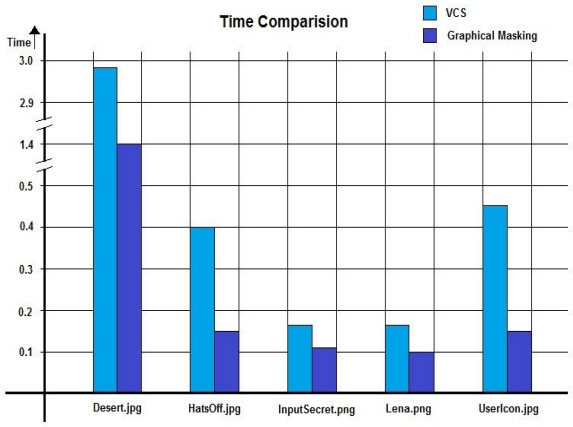

Table 1. TABLE STYLES

a. Sample of a Table footnote. (Table footnote)

VI. CONCLUSION`

In this paper, a(k, n) visual multiple secrets sharing scheme without pixel expansion has been proposed with a combination of Entropy embedding. As, there is no pixel expansion in share generation, we overcome the problem of noise addition. We also avoid the need of noise removal algorithm at the receiver end. We applied embedding phase to increase the strength of secret share. As there is no pixel expansion the overhead of storage, the reduced size also raises the capacity of secret communication. Recovered secret images are having better visual quality as compared to previous results present in the literature.

VII. ACKNOWLEDGMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

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] 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.

[8] 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.

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

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

[11] Xinpeng Zhang,” Separable Reversible Data Hiding in Encrypted Image”, IEEE TRANSACTIONS ON

INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012