ABSTRACT

Visual secret sharing is the technique that divides the secret image into n multiple shares. Each share contains some information and when k shares out of n stack together the secret will reveal. However, less than k shares are not work. The beauty of the visual secret sharing scheme is its decryption process i.e. to decrypt the secret using Human Visual System (HVS) without any computation. We have proposed the new algorithms for the (2, 2) visual cryptography and (3, 3) visual secret sharing. Our proposed schemes are for gray scale image and by stacking the shares; the resultant image achieved in same size with original secret image. We used randomization and pixel reversal approach in all methods.

Categories and Subject Descriptors
D.3.3 [Computer Security]: secret sharing, cryptography.

General Terms
Experimentation, Security, Theory, Verification.

Keywords
Visual secret sharing, visual cryptography

1. INTRODUCTION

The concept of secret sharing was developed many years back, when Adi Shamir has shown this idea in his paper in 1979 [1]. In this paper he shows that "How to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D". He utilized this idea to save the key for using the encryption. In 1994, Naor & Shamir shows a new concept using images in their paper "Visual Cryptography". They extend their new scheme to secret sharing problem. That paper is the seed of the visual cryptography and visual secret sharing and every work was published in this area with the reference of this paper. In this paper abstract they said "We extend it into a visual variant of the k out of n secret sharing Problem in which a dealer provides a transparency to each one of the n users any k of them can see the image by stacking their transparencies, , but any k-1 of them gain no information about it [2]".

After this basic concept many researcher find out different schemes for the visual cryptography [3]. This improvement goes to gray scale image to color images and different ways and techniques were developed with amazing ideas. We will discuss these all in our literature survey. However this field is still growing and needs to be flourishing in future based on the demand. The major demands are the security and low power computations at the time of decryption. Now days for the data security very famous and powerful algorithm use, e.g. 3DES, RSA, ECC, AES and Rijndal etc. The major problem is the power consumption at the time of decryption of these algorithms. We use many portable devices e.g. Laptop computer, mobile phone etc. these and many others are low battery power devices and need to consume less there battery power for increasing life time of the power continuation.

For this purpose the utilization of this technology is promising. The locations of this field in the hierarchy of the Steganography are shown in the following Figure.

![Figure 1. The classification tree of Steganography](image-url)

1.1 Visual cryptography Model

The model for visual cryptography is given by Naor & Shamir as follows [2]:

A printed page of ciphertext and a printed transparency (which serve as a secret key). The original cleartext is revealed by placing the transparency with the key over the page with the cipher, even though each one of them is indistinguishable from random noise. The model for visual secret sharing is as follows [4]. There is a secret picture to be shared among n participants. The picture is divided into n transparencies (shares) such that if any m transparencies are placed together, the picture becomes visible. If fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately.

2. PREVIOUS WORKS

Visual cryptography is a popular solution for image encryption. Using secret sharing concepts, the encryption procedure encrypts a secret image into the shares which are noise-like secure images which can be transmitted or distributed over an untrusted
communication channel. Using the properties of the HVS to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography.

2.1 Basic concept of 2-out-of-2 VC scheme
Visual cryptography scheme where 2 shares are generated from the original secret image and by stacking together the secret is reveal. This is the basics of the technique, however if we create more than 2 shares and some or all of them staked for getting the real secret is called visual secret sharing. Following Figure shows the basic behind this scheme.

<table>
<thead>
<tr>
<th>Pixel</th>
<th>White</th>
<th>Black</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prob.</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Share 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>share 1 &amp; 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2: Basic concept of 2-out-of-2 VC**
In this concept one white or black pixel will divide into two sub pixel. One way combination of the pixel division is shown in above Figure. It is mention that the shares 1 and 2 are stacked together and get the result in the form of complete black or gray (it's partially white and black but visualizes as gray). Because of this when we stacked the shares the white in original secret image become gray in the stacked result.

2.2 (k, n) secret sharing scheme
Naor-Shamir, 1994 [2] shows (k, n) secret sharing in his paper. They explained as "an N-bits secret shared among n participants, using m subpixels per secret bit (n strings of mN), so that any k can decrypt the secret":

Contrast: There are d<m and 0<α<1:
If pixel=1 at least d of the corresponding m subpixels are dark (“1”).
If pixel =0 no more than (d-αm) of the m subpixels are dark
Security: Any subset of less than k shares does not provide any information about the secret x.
All shares code “0” and “1” with the same number of dark subpixels in average. may have to improvise.

2.3 Generalization of (k, n) secret sharing scheme
Naor-Shamir [2] generalized their results by using the following theorem/lemma.
**Lemma:** There is a (k, k) scheme with m=2^k-1, α=2^1-k and r=(21-k).
We can construct a (5, 5) sharing, with 16 subpixels per secret pixel and 1 pixel contrast, using the permutations of 16 sharing matrices.
**Theorem:** For any n and k, there is a (k, n) visual secret sharing scheme with m=log n 2^k log k, α=2 -Ω(k).

2.4 Extensions: General Access Structure
Ateniense et.al. 1996, define the general access structure as shown below [5].
Let P = {1,2,...,n} be a set of elements called participants, and let 2^P denote the set of all subsets of P. Let Λ_{Qual} ⊆ 2^P and Λ_{Forb} ⊆ 2^P where Λ_{Qual} ∩ Λ_{Forb} = Ø, where Λ_{Qual} = Qualified set
Λ_{Forb} = Forbidden set
And the pair (Λ_{Qual}, Λ_{Forb}) called the General Access structure of scheme. Where Λ define all minimal qualified set.

A_0 = {A ∈ Λ_{Qual} : A' ⊆ Λ_{Qual} for all A' ⊆ Λ_{Forb}}

Through this scheme, define arbitrary sets Λ_{Qual} and Λ_{Forb} as subsets of participants. Any set in Λ_{Qual} can recover the secret by stacking their transparencies and any set in Λ_{Forb} has no information on the shared image.
They show constructions satisfying these requirements, with mild restrictions on the sets.

2.6 Extended VSS – Gray Scale
Naor & Shamir [2] describe that many extension from his basic work can be possible. Further he extends his work with following suggestions: Use partially filled circles to represent grey values. It is mention below. In the following Figure.

**Figure 3: Extended VC scheme**
Above Figure shows that for the continuous tone gray image we can use the pixels in the form of the circle. For example in above two shares the superimposition of first two gives the third one.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Conference'04, Month 1–2, 2004, City, State, Country.
Copyright 2004 ACM 1-58113-000-0/00/0000...$5.00.

**Figure 4: Example of the extended Visual cryptography**
For the image dividing into the rotating circles as above can gives the color impression from gray color to black based on there adjustment or superposition. Example of the above extension is shown below [6].

Other extension was discussed by the Noar and Shamir is concealing the very existence of the secret data. In this scheme they consider the 2 x 2 array and take white if the two subpixels are white and two are black. Similarly take black if three subpixels are black. This suggested scheme is shown below.

3. EXPERIMENTAL DESIGNS

3.1 Randomized Visual cryptography scheme

We have design some schemes on visual cryptography and visual secret sharing. Our approach for these schemes is randomization and pixel reversal. We have done several experiments and came up some new approaches of (2, 2) visual cryptography and (3, 3) visual secret sharing schemes. First we explain the approach for the (2, 2) visual cryptography scheme.

In (2, 2) visual cryptography scheme we have one secret gray scale image (SI) as input to the algorithm. Where SI is consider as a matrix $S_{ij}$ where i and j shows pixel positions and i, j= 1, 2, 3, ..., n. All steps of algorithm in this scheme are shown below.

Step1- Pixel $S_{ij}$ with position i and j is the input called original pixel.
Step2- Apply pixel reversal i.e $S_{ij}^{-} = 255 - S_{ij}$.
Step3- Use random number generator (0.1 to 0.9) to reduce $S_{ij}^{-}$ randomly.
Step4- Take the difference of $S_{ij}^{-}$ with original pixel $S_{ij}$.
Step5- Use random number generator to reduce reversed value of $S_{ij}^{-}$ randomly.
Step6- Apply pixel reversal i.e $S_{ij}^{''} = 255 - S_{ij}^{-}$.
Step7- Store in matrix as image called share 1.
Step8- Take the difference of two random number generators with original pixel $S_{ij}$.
Step9- Apply pixel reversal i.e $S_{ij}^{'''} = 255 - S_{ij}^{''}$.
Step10- Store $S_{ij}^{'''}$ in matrix as image called share 2.
Step11- Repeat point 1 to 10 for all pixel from original image (i.e matrix of original image).

This algorithm is shown in Figure 5. This VC scheme use gray scale secret image. In (2, 2) visual cryptography by Naor & Shamir was implemented in [7]. Where the decoded image is twice that of original secret image because the pixel p expanded into two subpixels this effect is called pixel expansion. That affects the contrast of the resulting image. The problem for the pixel expansion and contrast was discussed majorly in literature. The previous work on pixel expansion and contrast optimization shows that researcher did efforts to reduce the expansion and optimize the contrast of the secret picture [8, 9, 10]. Further they portrait the process of creating the shares using mathematical representations and mainly they focus the security and contrast condition [11].

In our scheme the decoded image is same in size of original secret message there is no pixel expansion effect found. However the nature of the algorithm as in general as with many other schemes the decrypted image is darker and contains a number of visual impairments. Our decoded secret image is darker then the original. The decoded secret image has increase the spatial resolution however mostly of visual cryptography scheme has shown the same effect in their decoded image [7].

After testing many different images from light to dark in resolution it was observed that the proposed algorithm could not take dark true image significantly with high contrast and then generate the meaningless share. Majorly found that the shares reveal the information. However on light contrast we have seen it that algorithm generates the perfect meaningless shares as shown in Figure 6.

3.2 Improvement

Based on our observation that proposed algorithm could not give perfect meaningless shares in case of the dark or high contrast secret image, we have added preprocessing elements to change the dark or high level of gray image into lighter one (called preprocessed image or halftone image). This is to be done before giving input secret image to proposed algorithm. We define two way of preprocessing of the input image as follows:

We change the pixel values to white (255) on the bases of the position of the pixel. We use odd and even combination of the pixel values in the matrix as follows:

**Method 1:** If $i=j$=odd and $i=j$=even

pixel $(i, j) = 255$

**Method 2:** if $i$=odd & $j$=even OR $i$=even & $j$=odd

pixel $(i, j) = 255$
This preprocessing converts the secret image into a lighter one in contrast and then gives to the proposed algorithm for processing. The result of these added elements with both type of preprocessing is shown in Figure 7.

![Figure 7: Randomize Visual Cryptography results with preprocessing in sharp edges pictures](image)

**3.3 Results**

Figure 7 shows that after giving the true gray scale picture as secret image has better results in comparison of algorithm without preprocessing. Because for secret image (true gray scale image) will reveal the secret completely in shares in case of without preprocessing. However using preprocessing (half toning) the shares shows some information about the secret. This can be improving further by using extended preprocessing on the same processed image. The purpose of preprocessing is to preparing the image on a certain level that the algorithm must not reveal the secret words from the image. Figure 7 shows that the perfect meaningless shares and after stacking we get the secret. The input image is the preprocessed secret image. The result from stacking of share is so perfect in case of the preprocessing i.e. shown in Figure 7.

**3.4 Further improvement**

For further improvement, we use three stage preprocessing cycle and divide the phase I (used for producing the share 1) into three stages and process the image. The result of this technique is good as compare to the previous algorithms because we can give the original true gray color image to this algorithm and get the two meaningless shares. The results shows that this algorithm is perfect for the dark contrast secret image and also there is not much pixel expansion occur in the stacked image.

**4. CONCLUSIONS AND FUTURE WORK**

We have shown that the (2, 2) randomize visual cryptography in practice where the shares are generated based on pixel reversal, random reduction in original pixel and subtractions of the original pixel with previous shares pixel. The original secret image is divided in such a way that after OR operation of qualified shares we reveal the secret image. Our scheme has shown less pixel expansion which is desirable and good for the final retrieval of the secret image. Some contrast change and impairments are still visible in the results of these schemes. However by dividing the pixels into two or more sub pixel retrieve the secret picture with more impairments and bad resolutions. In our scheme the results are better then and the size of the retrieve image is the same as the original. However size of pixel increases provides more easiness for alignment of the shares. This is the still researchable area to reduce this effect. Also our proposed schemes have shown high level of security because of randomness.

The future work is to improve the contrast and reduce the pixel expansion in the resultant secret image. Further extend this work to use this technique with color images. Also consider 3D images for creating the shares that have partial secret and reveal that secret by stacking to each other.

**5. ACKNOWLEDGMENTS**

Our thanks to King Fahd University of Petroleum & Mineral for providing facilities for this research work.

**6. REFERENCES**


