Two in One Image Secret Sharing Scheme with Increased Scalability

Parvathy Vijay
M. Tech Scholar, CSE
LBS Institute of technology for Women
Poojappura, Trivandrum, India

Sreelatha S H
Associate Professor, CSE
LBS Institute of technology for Women
Poojappura, Trivandrum, India

ABSTRACT

Secret sharing schemes allows information to be shared among a group of participants so that all together (or qualified subsets) of participants can recover the information. A visual cryptography scheme (VCS) is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The performance of any visual cryptography scheme depends on various measures such as pixel expansion, contrast, security, accuracy, computational complexity etc. This work throws light on the theoretical background and the comparison on the various visual cryptography schemes. Here introduces a 2 in 1 scheme which can embed additional information with reduced shadow size and better visual quality of revealed image. Compared with the two-in-one image secret sharing scheme (TiOISSS), this scheme might achieve smaller shadow size with acceptable visual quality. The paper discusses Sharing More Information Gray Visual Cryptography Scheme (SMIGVCS) which can embed additional information with reduced shadow size and better visual quality of revealed image. The main results of this paper include implementation of a visual cryptographic scheme with a reduced share size.

General Terms

Image Processing, Visual Cryptography

Keywords

Bit Level Decomposition; Polynomial Based Image Secret Sharing; Scalability; Shadow Size; Visual Cryptography.

1. INTRODUCTION

As new technologies emerge more personal data are digitized and these data’s are stored electronically. Thus emphasis on data security increases. Protecting the secret data’s in a secure way from unauthorized access and does not impede authorized access becomes important. Many data security methods were introduced but the common disadvantages of these were single point failure i.e. if communication channel fails entire secret cannot be recovered. Thus a new technique called secret sharing is introduced. This scheme allows us to effectively and efficiently share secret between a numbers of secret parties. In this scheme secret data is divided into n pieces called shares, in such a way that only qualified subset can reconstruct the secret. Number less than this qualified subset cannot reveal the secret information. While these shares are separate no information about the secret can be accessed i.e. shares are useless when they are separate. Image secret sharing is a subset of secret sharing scheme. Secrets in this case are concealed images. This secret sharing scheme can be classified into two areas: visual cryptography and polynomial based secret sharing.

Visual cryptography is a technique by which one secret can be distributed into two or more shares. The important characteristic of visual cryptography is that the decryption is non- computational. The shares are printed on transparencies and when these shares on the transparencies are super imposed exactly together the secret can be discovered without computer participation. Naor and Shamir introduce Visual Cryptography Scheme (VCS) in 1994. It is a new type of scheme which decodes concealed images without any cryptographic computation [1]. It is related to human visual system which means the decoding process is non-computational. The secret can be revealed by properly stacking the shares. In (k, n) VCS, secret image is first shared into n shadow images for n participants. When k out of these n shares is stacked together the human eyes do the decryption. This mechanism is secure and can be easily implemented. Any person who has no information about cryptography can use it very easily. However VCS faces two challenges - large size expansion of shadows and low visual quality of revealed image.

Another category of image secret sharing is called polynomial based image secret sharing scheme (PISSS). It was first introduced by Shamir in 1979. In this scheme there is a polynomial of degree (k-1). The constant coefficient of this polynomial is replaced by the secret value and the rest of the coefficients are random numbers and thus generate n shares [2]. Out of this n shares, k shares, $k \leq n$, are needed to decode the secret value. This can be done by Lagrange’s interpolation. The shadow size is same as that of the original secret image. Thien and Lin introduced another scheme from Shamir in which all the coefficients of this (k-1) degree polynomial is replaced with the k pixel values of secret image [3]. Thus the shadow size is reduced by 1/k times of original image.

Lin and Lin combined VCS and PISSS into one scheme. This is called two-in-one Image Secret Sharing Scheme (TiOISSS). This scheme has two decoding options. In this scheme the shadows obtained from PISSS is embedded into the shadows of VCS [4]. In the decoding process a vague binary secret image is obtained by stacking the shadows when computer resources are not available, like VCS. Then a perfect gray valued image is obtained from the values hidden in the shadows by using polynomial based scheme when computer resources are available. The size expansion of shadow is much large in this scheme. Further methods were introduced [5-6] in order to reduce the shadow size and visual quality of revealed secret image.

Then another improvement is done in this two-in-one scheme in which we can share more information in gray visual cryptography scheme SMIGVCS. This becomes building blocks for all two-in-one schemes. In this scheme sub pixels of VCS contain gray pixels. Depending upon the gray sub pixels generated from the black or white sub pixels of VCS we can embed p or q bit gray value [7]. In decoding a vague secret image is visually decoded by stacking k shadows. When computational resources are available k shadows of (k, n) PISSS are retrieved from k shadows of SMIGVCS and then reveal additional information by Lagrange's Interpolation. Since SMIGVCS is based on gray VCS the quality of the revealed image is worse than that of VCS. As the shadow size decreases the visual quality of the revealed secret image deteriorates. But additional information can be embedded in this two-in-one scheme.

So, a two-in-one image secret sharing scheme with reduced shadow size and better visual quality of revealed secret image is introduced. This is an improvement over VCS, that is, the image obtained by stacking the shares is better than the one obtained by VCS with reduced share size. Since SMIGVCS is based on gray VCS the visual quality of the revealed image is worse than that in VCS. As the shadow size decreases the visual quality of the revealed secret image deteriorates. But we can embed additional information in this two in one scheme. So improve the visual quality of the revealed secret image with reduced shadow size along with embedding additional information is of major concern here. Another area of enhancement here is that in traditional VCS binary images can be processed. VCS for gray scale images were also introduced but the success of the schemes lies in the underlying half toning techniques used to convert this gray scale image to binary. Here we propose an enhanced VCS in which bit level decomposition can be used. By this scheme for VCS the visual quality of the stacked secret image increases. All the two in one scheme uses basic (k,n)PISSS scheme. But the size of shadows and visual quality of revealed image is important. So here we propose a scheme instead of (k,n) PISSS which incorporates scalability. The shadow size is less than that of the original secret image and the quality of the revealed secret image increases with increase in the number of participants. Thus we proposed an enhanced two in one scheme in which we can embed additional information by which the visual quality can be improved by bit level decomposition and shadow size reduction by incorporating scalability.

The rest of this paper is organized as follows: below in section 2 we first review some background knowledge used in this paper and in section 3 we introduce our method. The experimental results and discussions are in section 4. Finally we conclude in section 5.

2. BACKGROUND

2.1 Naor and Shamir's Visual Cryptography Scheme (VCS)

Moni Naor and Adi Shamir introduced "Visual Cryptography"[1] as a new type of cryptographic scheme which described a secure way of encrypting images and decoded directly by the human visual system. The scheme suggested consists of a printed transparency and a printed page of cipher text that could be used to reveal the image by simply stacking the printed transparency over the printed cipher text. This method was simple as it could be used by anyone (without any knowledge of transparency) but individually each one of the images look like a pattern of random dots to the human eye (security). Naor and Shamir extended this basic scheme into a variant - k out of n secret sharing where at least k transparencies (of the total n transparencies) generated from the original image are required to be stacked together to reveal the original image. The original problem stated by Naor and Shamir is a specific case of k by n scheme that is, 2 by 2.

The scheme uses the concept of pixel expansion. Each pixel (black or white) in the original image is encoded into m sub-pixels on each share (total number of shares is n), where m is called the parameter of pixel expansion of the scheme. Thus each share image is a Boolean matrix of order [n x m] which can be defined as below,

S_{ij} = 1 if the j^{th} sub-pixel in the i^{th} share is black.

S_{ij} = 0 if the j^{th} sub-pixel in the i^{th} share is white.

The value m is referred to as the pixel expansion of the scheme. The grey level of the resulting image by stacking individual shares is proportional to the Hamming weight of the vector obtained by OR-ing the rows of the share matric associated with the transparencies we stack. This grey level is interpreted by the visual system of the participants as black, as grey, or as white according to some rule of contrast. Different techniques were used in this basic VCS to improve the visual quality and shadow size [8-10] such as probabilistic method, color VCS etc.

2.2 Shamir's Secret Sharing Scheme

Shamir developed the idea of a (k,n) threshold based secret sharing technique [2] where k≤n. This scheme is based on polynomial interpolation. The technique allows a polynomial function of order (k-1) is constructed as

$$f(x) = (a_0+a_1x+\ldots+a_{k-1}x^{k-1}) \bmod p \qquad (1)$$

where the value a_0 is the secret and p is a prime number but it is not necessary. The coefficients a_0, $a_1 \ldots a_{k-1}$ are integers randomly chosen form {1, 2 . . . p}. n shares can be then generated by using (x_i, f (x_i)) where i=1,2…n. Any k out of these n shares can be used to reconstruct the original information. This can be done by using Lagrange's Interpolation by which the coefficient a_0 can be calculated. However, any k-1 or fewer shares cannot get any information about the secret. Thus the secret data can be reconstructed. In image sharing, a_0 is taken as the gray value of the first pixel, then the corresponding output f (0) to f (n) is obtained; after that, a_0 is replaced by the gray value of the second pixel, and the process repeats until all pixels of the secret image are processed. Hence, each shadow image is of same size as that of the original image.

2.3 Thien and Lin's Image Secret Sharing Scheme

Shamir's secret sharing scheme use random coefficients and the size of shadows obtained by this scheme is same as that of original secret image. So a new scheme is proposed [3] which use gray values of r pixels in the original image as r coefficients of (r-1) degree polynomial. Therefore, the major difference between this method and Shamir's is that this method does not use random coefficient.

To apply the method, truncate all the gray values 251–255 of the secret image to 250 so that all gray values are in the range 0–250. In the sharing phase first the secret image is divided into several sections such that each section has r pixels and each pixel of the image belongs to one and only one section. Then (r-1) degree polynomial is defined for each section.

$$q_j(x) = (d_0+d_1x+d_2x^2+\ldots+d_{r-1}x^{r-1}) \bmod 251 \qquad (2)$$

where d_0 to d_{r-1} are the r pixels of the section, and then evaluate $q_j(1)$, $q_j(2) \ldots q_j(n)$. The n output pixels $q_j(1)$ to $q_j(n)$ of this section j are sequentially assigned to the n shadow images. Since for each given section (of r pixels) of the secret image, each shadow image receives one of the generated pixels; the size of each shadow image is 1/r of the secret image.

In the reveal phase using any r (of the n) shadow images: Take the first non-used pixel from each of the r shadow images. Use these r pixels and the Lagrange's interpolation to solve for the coefficients $d_0$to d_{r-1} in Equation (2). The coefficients d_0 to d_{r-1} are then the corresponding r pixel values of the permuted image. Repeat until all pixels of the r shadow images are processed. Advantages of this scheme are:

- Perfect reconstruction of secret.
- Shadow image is smaller than that of original image.

2.4 Two in One Image Secret Sharing Scheme

This scheme combines the two image secret sharing scheme VCS and PISSS. If the decoding computer is not available temporarily then the shadows are stacked to get a vague black and white view of the secret image immediately. When the decoding computer is available then a finer gray valued view of the secret image can be obtained using computation. In short each of the shadow is a two-in-one information carrier and it has two decoding options. This is the main characteristics of this two-in-one scheme.

The method is explained as follows: S is the secret image that we want to transmit. Let H be a halftone version of the image S. so this scheme needs two images: one gray scale image and a halftone version of the gray image. Then the binary image is first shared into n shadows {r1, r2 . . . rn} using (k,n) threshold VCS scheme. Here the shadows are also known as transparencies. Then the gray scale image S is shared into n shadows {s1, s2 . . . sn} using (k,n) threshold PISSS scheme. The n transparencies of VCS scheme can hide the information obtained from the shadows of PISSS scheme so that any k of these n transparencies can be stacked to view the enlarged version of the secret information and also to extract the information of S hidden in the k received transparencies.

2.5 Image Secret Sharing with Two Decoding Options

This scheme [5] is similar to the basic two-in-one image secret sharing scheme. In the previous two-in-one scheme the size expansion of shadow is very high. In order to reduce the shadow size concept of gray pixel is introduced here. In this method gray sub pixel is adopted into VCS. This gray scale information represents the output of the (k-1) degree polynomial in PISSS. The main concept behind this scheme was that when a sub pixel is stacked by a white pixel its intensity remains unchanged. Similarly when two gray sub pixels are stacked together a much grayer color will be obtained. When a dark sub pixel in VCS is replaced with gray sub pixels in the shadow it still distinguishes the black color from the white color in the reconstructed image. This was used in this two-in-one scheme. This scheme replaces the black sub pixels of VCS by 8-bit gray values. This gray value comes from the corresponding shadow of PISSS. This scheme of replacing the black sub pixels with 8-bit gray value is called Gray Visual Cryptography Scheme (GVCS).

2.6 Improvements of a Two-in-One Image Secret Sharing Scheme Based on Gray Mixing Model

In order to avoid the weakness of the previous method a new scheme is introduced here. In the previous method it replaces the black sub-pixels of VCS by 8-bit gray values. These values are between 0 and 255. The white sub-pixels are remains unchanged. So the gray sub-pixel replaced with 255 is confused with the other white sub-pixels in the shadow. Therefore on reconstruction the positions of gray pixels cannot be located correctly results in some speckles in the reconstructed image. Since it replaces the black pixels with gray, the stacking result is still gray. So the contrast of the reconstructed image is degraded. This makes the preview capability ineffective.

In this scheme to avoid the weakness of speckled reconstruction of Yang's TiOISSS it uses two values to represent the gray value in the shadows of PISSS. The weakness of the speckled reconstruction comes from the confusion between the gray sub-pixels with value 255 and the white sub-pixels in the shadows of GVCS. The proposed scheme restricts the gray values smaller than 255. If the value of gray sub-pixel p is ≥ 254 then split it into two values 254 and (p-254) and stored as new shadows. Then generate the shadows of GVCS with the gray sub-pixels chosen from the values of new shadows. Therefore, all the gray sub-pixels values in the shadows of GVCS are smaller than 255, and the correct gray values in the shadows of GVCS can be easily extracted. Next weakness in the previous scheme, low preview capability, is improved by gray mixing model. The gray sub-pixels in the GVCS are replaced by q-bit gray values, where $1 \leq q \leq 8$. This is called qGVCS. Therefore, by using smaller q in qGVCS, the contrast between the gray sub-pixels and white sub-pixels will increase, which means the better visual quality of the revealed image.

2.7 Sharing More Information in Gray Visual Cryptography Scheme (SMIGVCS)

SMIGVCS [7] is generated by replacing all the sub-pixels of the corresponding shadow of VCS by gray pixels. In Gray visual cryptography scheme additional information can be shared. The additional information that is to be shared is represented as a gray scale image I. This image I is shared using (k,n)- PISSS into n shadows. Each shadow of SMIGVCS is generated by replacing all the sub-pixels of the corresponding shadow of VCS by gray pixels. And the gray pixels information comes from the shadows of (k,n)-PISSS. The gray sub-pixels generated from the white sub-pixels of VCS as bright sub-pixels, and the gray sub-pixels generated from the black sub-pixels of VCS as dark sub-pixels. In each bright sub-pixel, embed a p-bit gray value. In each dark sub-pixel, embed a q-bit gray value. In the revealing process, a vague secret image is visually decoded by stacking k shadows. When computation resources are available, k shadows of (k,n)-PISSS are retrieved from k shadows of SMIGVCS, and then reveal additional information I by Lagrange's interpolation.

3. PROPOSED SYSTEM

A two-in-one image secret sharing scheme which has two decoding options is proposed here. A vague secret image is obtained by stacking the shadows and a perfect secret is revealed with computation. The vagueness of the reconstructed image is due to the pixel expansion. When a single pixel is replaced with more than 1 sub-pixel the quality of the reconstructed image deteriorates. Perfect reconstruction with reduced shadow size is not obtained in previous methods. Thus a two-in-one scheme is introduced which incorporates two techniques to embed additional information into the shadows. The important characteristics of this are reduced shadow size and better visual quality of revealed image.

Here two gray scale images are used. One is the secret information S and another one is the additional secret information I that is embedded into the first one. On decoding vague secret information is first obtained by stacking the shadows. The information thereby obtained is used to prove the authenticity or the validity of the additional information shared.

3.1 Main Idea

In previous SMIGVCS secret image is the binary version of gray scale image and additional information is gray scale image. Binary image is shared using (k,n) VCS and gray scale image by (k,n) PISSS. Each shadow of SMIGVCS is obtained by replacing all the sub pixels of corresponding shadow of VCS by gray pixels.

In this work two gray images are used. The secret information is shared by using bit level decomposition of gray image. Main advantage of using this is when (k, n) VCS is used the gray scale image have to be converted to binary by using half toning techniques. The clarity of the image obtained depends on the novelty of this technique. To avoid this gray scale image is decomposed to its bit planes. The original image is decomposed into eight bit planes. A (2, 2) scheme is described here. Original image with size m×n is scanned. Two shares S1 and S2 are defined. Then the bit planes of original image are considered. For example original matrix is:

S = $\begin{bmatrix} 12 & 15 \\ 24 & 147 \end{bmatrix}$. Then A=$\begin{bmatrix} 00001100 & 00001111 \\ 00011000 & 10010011 \end{bmatrix}$

The bit planes of A are A1=$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ A2=$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ A3=$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ A4=$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ A5= $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$ A6= $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ A7= $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ A8=$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Then each bit plane of A is encrypted by using VCS scheme. i.e. we randomly choose any basis matrix as in the case of (k,n) VCS. Then for each bit in the bit plane depending on its value i.e. 0 or 1 we distribute the rows of the basis matrix for each share

For example in a (2,2) scheme the random matrix is $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ then if the first bit of bit plane A1 is 0, the sub pixel for share 1 is the same matrix and its complement for share 2. If it is 1, then use same matrix for both the shares. Thus all the bits in the bit plane are shared. Superposition of these two shares will produce the original secret image S. The shadow size is proportional to pixel expansion. In the (2,2) scheme the shares are twice that of original image.

In SMIGVCS the additional information to be shared is represented as a gray scale image I which is shared into n shadows by (k,n) PISSS. As is known, PISSS has a perfect reconstruction and spends the competition for reconstruction it is reasonable to adopt in a two in one scheme where the secret image and host image can be revealed both by stacking the transparencies and by competition. In this method instead of traditional PISSS, polynomial scheme based on scalability is introduced. In our method as the number of participants for computational decryption increases the clarity of the revealed secret image increases with a reduction in the shadow size. Thus the overall shadow size of this two in one scheme further reduces.

3.2 Construction

Here (k, n, p, q) scheme is constructed where,

n= number of participants

k= threshold value

p,q=bits used for embedding additional information

Algorithm for sharing phase

Input: Gray scale secret image S and additional secret information I

Output: n shadows G1, G2…Gn

Step 1: Convert the matrix of S into bit planes.

Step 2: Each bit planes of the image is encrypted by using VCS.

Step 3: Obtain n shadows of S by using binary VCS as V1, V2…Vn

Step 4: Additional secret information I is partitioned into j disjoint partitions.

Step 5: Each partition is then shared into 2 shares K_j^1 and $K_j^2$by using (2, 2) PISSS.

Step 6: n shadow images {P1, P2…Pn} is now constructed from either of the 2 shares in the previous step such that

$P_i = \bigcup_j K_j^t$ and t=$\begin{cases} 1 & if\ i = j \\ 0 & otherwise \end{cases}$

Step 7: Take each unprocessed sub pixel r in Vi

7.1: if this is a white pixel (0), then read p-bit information l1, l2…lp from Pi and convert it into decimal value, val

7.2: store 255-val as the corresponding sub pixel of output shadow Gi

7.3: otherwise (1) then read q-bit information l1, l2…lq from Pi and convert it into decimal value val

7.4: store this value as corresponding sub pixel of Gi

Step 8: repeat step 9 until all sub pixels are processed.

Step 9: distribute G1, G2…Gn to n participants.

Algorithm for reconstruction phase

Input: n shadows G1, G2…Gn and matrix R

Output: stacked image S and additional secret I

Step 1: Stacking any k shadows of this n shadows will give vague secret image S

Step 2: Read first sub pixel r in Gi

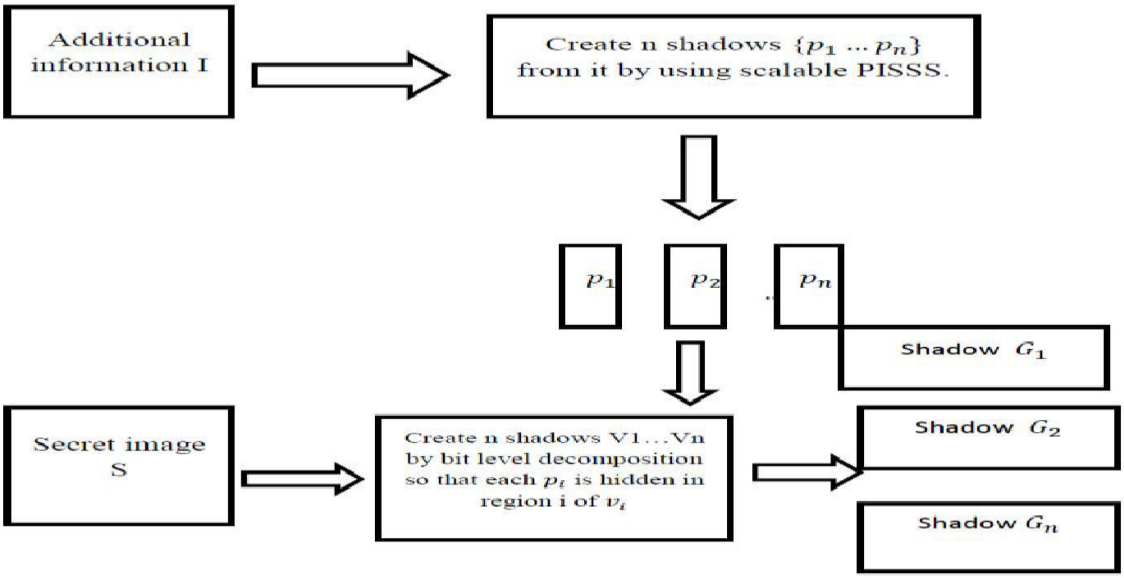

Additional information I
Create n shadows $\{p_1 \dots p_n\}$ from it by using scalable PISSS.
p_1
p_2
p_n
Shadow G_1
Secret image S
Create n shadows V1…Vn by bit level decomposition so that each p_i is hidden in region i of v_i
Shadow G_2
Shadow G_n

Fig 1: Sharing Phase

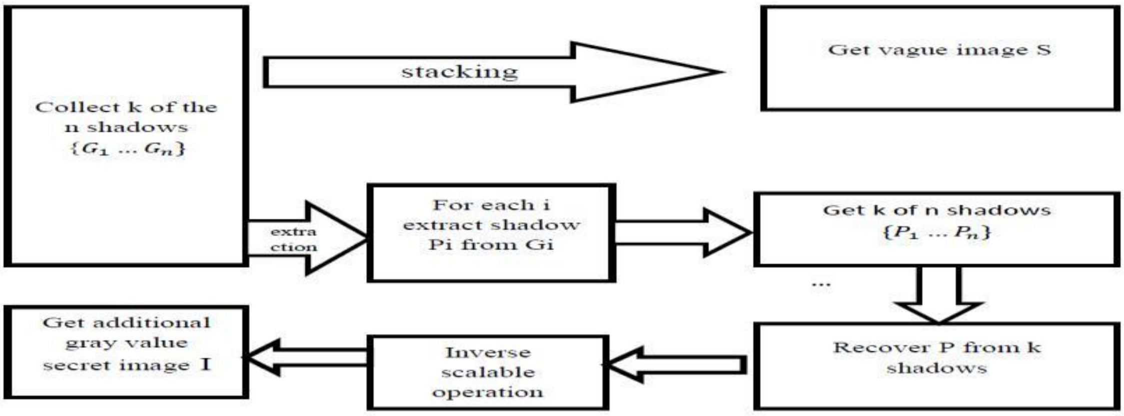

Collect k of the n shadows $\{G_1 \dots G_n\}$
stacking
Get vague image S
extraction
For each i extract shadow Pi from Gi
Get k of n shadows $\{P_1 \dots P_n\}$
…
Recover P from k shadows
Inverse scalable operation
Get additional gray value secret image I

Fig 2: Reconstruction Phase

2.1: if r> 255-2^p convert 255-r back to p bit binary sequence and add to shadow Pi

2.2: if r<2^q convert r to q bit binary sequence and add to shadow Pi

Step 3: Repeat step 2 until all sub pixels in Gi

Step 4: From the n shadows P1, P2…Pn collect k shadows P1, P2…Pk.

Step 5: For each participant fetch the 2 shares back.

Step 6: From each of these 2 shares take each unprocessed bit y_1 and y_2 and compute 2 pixels a_0=y_1-y_2 and a_1=y_2-y_1.

Step 7: Assign a_0 and a_1 as 2 pixels in the output partition.

Step 8: Repeat step6 and step7 for all pixels and step5 for all the j partitions.

Step 9: Assemble the j partitions to get the output image I.

The sharing and reconstruction phase is shown in Figure1 and Figure2:

4. RESULTS AND DISCUSSIONS

In this section, the experimental results are discussed and evaluated. The resultant images shown in this paper has been scaled down to fit in page and are not of the actual size. In this work a (2, 2) two-in-one image secret sharing scheme is demonstrated that satisfies two general criteria of accuracy and shadow size.

4.1 Shadow Size

In the case of basic two in one scheme each shadow of (k,n) PISSS is embedded into shadows of (k,n)VCS. Secret image in this method is gray scale image I. For VCS we are using half tone version of I i.e. I'. Let 'b' and 'w' be the number of 1 and 0 in every row of basis matrix. Thus size expansion of VCS is m. In order to embed the shadow of PISSS to corresponding shadow of VCS the size of halftone image used for VCS should satisfy:

$$|I'| \geq (8n/ (\log\binom{m}{w}.k)).\ |I| \qquad (3)$$

Shadow size of TiOISSS is m×|I'| i.e. shadow size is dramatically large

i.e.(2,2) TiOISSS

$$B0=\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix} B1=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

$$\binom{m}{w}=\binom{2}{1}=2,\quad \log\binom{m}{w}=\log 2=1$$

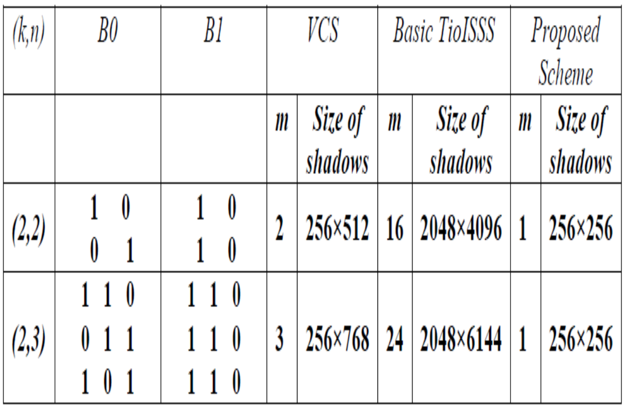
Suppose secret image I is 512×512 gray image. By equation 3 size of halftone image is 8×|I'| size expansion is 2 therefore shadow size is m×|I'|= 2×8×|I|=16×|I| i.e. shadow is 16 times of secret image.

In our proposed method we are using gray scale image for both VCS and scalable PISSS. Therefore the size of the secret image for VCS is also |I|. If the pixel expansion m=2 then the size of the shadows obtained by bit level decomposition VCS scheme is m×|I| i.e. 2×|I|, twice that of secret image which is much less than that of basic TiOISSS.

The secret image I is then shared by using (k,n)PISSS in the previous method. The shadow size of that scheme is same as that of original image, i.e. each pixel of the original image is converted into exactly one pixel in the shares. Thus the size does not change. In our proposed method scalable PISSS is used. In this scheme the size of the shadows should be 1/2 of the original image. When the image is partitioned into n partition the size becomes size (I)/n. Then each partition is shared into 2 shares. Then the size becomes size (I)/2n=1/2*size (I)/n. These two partition is then shared into n shadow images, thus the size becomes ½*size (I)/n*n= ½*size (I)/n. thus the shadow size is ½ of the original image.

In this (k, n, p, q) scheme on embedding shadows from both the schemes the shadow size depends on the value of both p and q bits selected from the shadows of scalable PISSS. Suppose our shadow size of PISSS is ½ of I and bit level VCS is 2×I. on embedding using our scheme if we are selecting the values of p=2 and q=2 then for each pixel for VCS shares 2 bits from the PISSS scheme is taken and stores as corresponding single pixel in output shadow. Thus shadow size further reduces. As the value of p and q increases the shadow size further decreases. But as the shadow size decreases the visual quality in terms of contrast decreases. Consider the size of original image as 256×256. Table 1 shows the size comparison of shadows.

Table1: Comparison of size of shadows



(k,n)	B0	B1	VCS		Basic TioISSS		Proposed Scheme	
			m	Size of shadows	m	Size of shadows	m	Size of shadows
(2,2)	1 0 0 1	1 0 1 0	2	256×512	16	2048×4096	1	256×256
(2,3)	1 1 0 0 1 1 1 0 1	1 1 0 1 1 0 1 1 0	3	256×768	24	2048×6144	1	256×256

4.2 Contrast of the Revealed Image

In the previous two in one scheme we are using the binary version of the gray scale image for VCS. Since using this binary version, it will reduce the contrast of the revealed image. By converting gray scale image to binary many information about the image is lost. Thus the recovered image also does not possess these information, so a vague image is obtained. In our proposed method we are using gray scale image directly in bit level decomposition. So the clarity of the revealed secret image is better than that of the traditional VCS. By properly selecting the value of (p,q) we can obtain revealed secret image with better visual quality and reduced shadow size. Scalability is the most important property of our scheme. All the previous two in one scheme reconstruct the image with single clarity. If we are using all the shares for reconstruction, then by using the previous methods only a given clarity is obtained. But in our scheme by increasing the number of participants we can increase the contrast of the revealed image.

Structural Similarity Index is used to evaluate the quality of the reconstructed images in this scheme. If one of the images being compared is regarded as perfect quality then Mean Structural Similarity Index (MSSIM) can be considered as the quality measure of the other image. If image1=image2 then MSSIM=1. The Mean Structural Similarity Index value of some of the original and reconstructed images is shown in Figure 3:

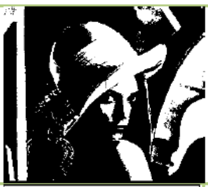
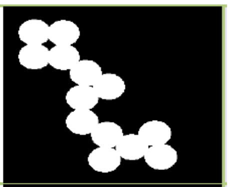
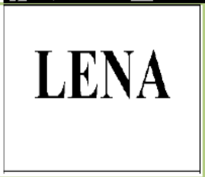
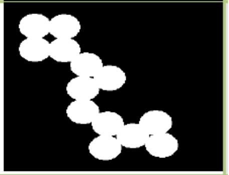
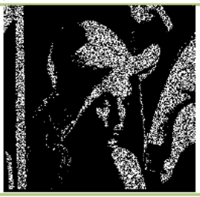
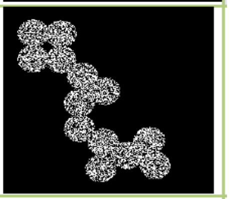
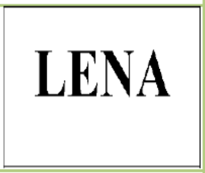
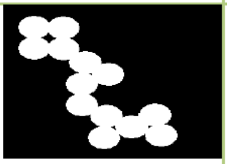
Original Secret Image S		
Additional Information I		
Reconstructed Image by Stacking the Shares S'		
Mean Structural Similarity Index between S and S'	0.6330	0.7616
Reconstructed Image by Computation I'		
Mean Structural Similarity Index between I and I'	1	1

Fig 3: Mean Structural Similarity Index of different secret images

A comparison between VCS and proposed scheme based on shadow size and reconstructed image quality based on MSSIM is shown in Table 2. All the images used here are of same size [256×256]. All the examples shown here are (2, 2) scheme. Different schemes can be used and as the number of shares for retrieval increases the visual clarity of the reconstructed image also increases.

Table2: Comparison between VCS and proposed scheme based on shadow size and image quality

	Shadow size		*Visual quality (MSSIM)*	
	VCS	*Proposed Scheme*	*VCS*	*Proposed Scheme*
	256×512	256×256	0.6273	0.7616
	256×512	256×256	0.3354	0.6361
	256×512	256×256	0.0536	0.2362
	256×512	256×256	0.0166	0.0782

5. CONCLUSION

Here introduce some visual cryptographic schemes. Many VCS schemes are premeditated and their performance is analyzed on four criteria: number of secret images, pixel expansion, image format and type of share generated. Security is the primary concern of today's communication world. Visual cryptography scheme does not consider the revealed image quality. Secret sharing scheme is computationally complex but it reveals the secret image with better quality. Thus combine both VCS and secret sharing scheme in two in one image sharing scheme. Image quality and shadow size is improved by embedding additional information in two in one secret sharing scheme

Here propose a two in one scheme using two techniques: bit level decomposition and scalable PISSS. Here the major concern is shadow size, visual quality and scalability of shares. Our aim is to develop an image secret sharing scheme with reduced shadow size, better visual quality of revealed image and scalability. Main advantage of this scheme is that as the number of participants increases the contrast of the revealed secret image increases with reduced shadow size. Most important application of this technique is that it can be used in many military applications. One image can be used as authentication i.e. the vague image obtained by stacking the shadows can be used to verify the validity of the secret information shared. If this is not valid cannot waste computational resources to decrypt the secret.

Future scope of this scheme is that a weightage scheme can be included in this two in one scheme. This technique can be used to deal with participants with different importance. The shares can be divided into two types such as essential shares with higher importance and non-essential shares with lower importance. Main advantage of this is that shares can be used depending upon the application. Weightage can be applied to each share such that certain application needs both essential and non-essential shares to retrieve the information. This will increase the security of the system.

6. ACKNOWLEDGMENTS

First and foremost I extend my immense gratitude to two of my teachers, my thesis coordinator Dr. Shreelekshmi R, Head of Department, Dept. of Computer Science & Engineering and my guide Smt. Sreeletha S H, Associate Professor, Dept. of Computer Science & Engineering for helping me in their own individual ways to successfully complete this research work. I am greatly indebted to my guide Smt. Sreeletha for continuously encouraging and motivating which made me confident. I am thankful to Dr. K.C Raveendranathan, Principal, LBS Institute of Technology for Women for providing all the required resources for the completion of this work. I would like to express my sincere gratitude to all the teachers of the Department of Computer Science for their moral and technical support throughout the course of this work.

I would like to thank my family especially my beloved husband who was always my support in the moments when there was no one to answer my queries. I would also like to express my heartfelt gratitude to all my friends who have directly or indirectly contributed their time and effort towards completion of this work. Last but not the least I thank Almighty for his blessings who had been my guiding light in tough times.

7. REFERENCES

[1] M. Naor, A. Shamir, Visual cryptography, in: EUROCRYPT‟94, LNCS, vol. 950, Springer-Verlag, 1995, pp. 1–12

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

[3] C.C. Thien, J.C. Lin, Secret image sharing, Computer & Graphics 26 (2002) 765–770.

[4] S.J. Lin, J.C. Lin, VCPSS: a two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches, Pattern Recognition 40 (2007) 3652–3666.

[5] C.N. Yang, C.B. Ciou, Image secret sharing method with two-decoding-options: lossless recovery and previewing capability, Image and Vision Computing 28 (2010) 1600–1610.

[6] P. Li, P.J. Ma, X.H. Su, C.N. Yang, Improvements of a two-in-one image secret sharing scheme based on gray mixing model, Journal of Visual Communication and Image Representation 23 (2012) 441–453.

[7] P.Li, C.N Yang, Q.Kong, Y.Ma, Z.Liu, Sharing more information in gray visual cryptographic scheme, Journal of Visual Communication and Image Representation, Volume 24, Issue 8, November 2013, Pages 1380-1393.

[8] C.N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognition Letters, Volume 25,, November 2003, Pages. 481–494.

[9] Y.C. Hou, Visual cryptography for color images, Journal of Pattern Recognition, Volume 36, January 2003, Pages 1619-1629.

[10] C.N. Yang, T.S. Chen, Colored visual cryptography scheme based on additive color mixing, Journal of Pattern Recognition, Volume 41, March 2008, Pages 3114–3129.