Multimed Tools Appl (2017) 76:815–834
DOI 10.1007/s11042-015-3066-7

Adaptive halftoned visual cryptography with improved quality and security

Srividhya Sridhar[1] · **R. Sathishkumar**[2] · **Gnanou Florence Sudha**[1]

Received: 23 June 2015 / Revised: 4 November 2015 / Accepted: 8 November 2015 /
Published online: 20 November 2015

Abstract Visual Cryptography Scheme (VCS) is a cryptographic technique which can hide image based secrets. Even though VCS has the major advantage that the decoding can be done with the help of Human Visual System (HVS), yet it does not provide sufficient reconstruction quality. Hence, Two in One Image Secret Sharing Scheme (TiOISSS) is used which provides two decoding phases. However, the existing TiOISSS method has several limitations. In this work, a Modified TiOISSS is proposed in which an adaptive threshold is used for halftoning, which changes depending on the nature of the pixels present in image. By this, the quality of reconstructed secret image is improved in the first decoding stage compared to the existing scheme. In addition, the security is also enhanced by pixel and bit level permutation with a 64 bit key and embedding the key in Gray VCS shadows. To verify the authenticity of the image, a secret message is also embedded in the shadows. Security analysis shows that the Modified TiOISSS is robust to Brute Force and Man-in-Middle attacks.

Keywords Visual cryptography · Halftoning · Adaptive halftoning · Polynomial image secret sharing

✉ Gnanou Florence Sudha
gfsudha@pec.edu

Srividhya Sridhar
srividhya2207@gmail.com

R. Sathishkumar
sathish.pkiet@gmail.com

[1] Department of Electronics & Communication, Pondicherry Engineering College, Puducherry, India

[2] Department of Electronics & Communication, Perunthalaivar Kamarajar Institute of Engineering & Technology, Puducherry, India

1 Introduction

Rapid advances in technology have enabled information services to be accessed anytime and anywhere. This has paved the need for secure communication between two parties or multiple parties. Hence, cryptographic techniques have evolved which can provide authentication, confidentiality and integrity between the users. These cryptographic techniques are computationally very complex. Visual Cryptography Scheme (VCS) is one such cryptographic technique which can hide image based secrets and in which the decoding can be done without computations.

VCS was first proposed by Moni Naor and Shamir in 1994 [13]. The basic concept of VCS is to split the secret image into n shares and distribute these shares to n users. The secret image can be revealed only by stacking the n shares together. The decoding process can also be relaxed to k users in (k, n) threshold scheme [1]. VCS can also be applied to grayscale images for which it should be first halftoned to convert to a binary image and then the shares should be created [6, 10, 21]. The shares created in this process are noise like shares which may be subject to many attacks. Hence, Extended VCS (EVCS) with meaningful shadows was created [2, 16, 20]. Multiple secret images can also be shared in VCS [11, 18]. In addition, VCS without pixel expansion has also been developed where the secret image and the share are of the same size. [3–5].

Polynomial Image Secret Sharing Scheme (PISSS) is also used for protecting image based secrets. This can provide perfect reconstruction of secret image, but the decoding here requires computations [15]. This PISSS is evolved from Shamir scheme [14]. In [7], the Shamir scheme was implemented for binding cryptographic keys in Fuzzy vault. In [12], an Enriched Secret Sharing Visual Cryptography Scheme (ESSVCS) has been developed which combines VCS, PISSS and a private key encryption scheme to share more secrets and to improve the security. However, only vague image and plain text reconstruction is possible and the method does not produce perfect reconstruction of the secret image.

Although the decoding process of VCS is simple, it does not provide sufficient quality of the secret image at the reconstruction phase. Lin *et al.* proposed a new approach which combines PISSS and VCS with two decoding options and has larger pixel expansion [9]. The combined approach called as Two in One Image Secret Sharing Scheme (TiOISSS) without pixel expansion is developed in [19]. During the second decoding phase, PISSS shadows have to be extracted and if this extraction is made incorrectly, it leads to speckled reconstruction of secret image. In [8], this problem is overcome and in addition, the quality of secret image is improved in first decoding phase by replacing sub-pixels in Gray VCS (GVCS) by q bit gray value where $1 \leq \boldsymbol{q} \leq 8$. However, the size of the shadow increases and smaller the value of q, better is the quality of the secret image.

Thus, the existing TiOISSS scheme still has certain limitations. The shadows in TiOISSS have gray values unlike the shadows in VCS which are binary in nature. Hence, the reconstructed secret image at the first decoding phase in TiOISSS is degraded compared to VCS. In addition, it is susceptible to Brute Force attacks and Main-in-Middle attacks. Hence, in this paper, three modifications to the existing scheme are proposed to improve the quality and security. First, to improve the quality of reconstructed secret image, an adaptive halftoning technique is proposed which adapts depending on the pixels present in the image, whether constantly changing or having abrupt transition. Secondly, the security is enhanced by two levels of permutation and embedding the secret key in the GVCS shadows. Thirdly, to verify the authenticity of users, a secret message is embedded in the shadows.

The paper is organized as follows. The existing TiOISSS and its limitations are discussed in Section 2. The Modified TiOISSS using the proposed method is dealt in Section 3. The

simulation results are discussed in Section 4. Performance analysis like Contrast, Peak Signal to Noise Ratio and Structural Similarity Index are discussed in Section 5. The security analysis of the proposed scheme is discussed in Section 6. Finally, the conclusion is made in Section 7.

2 Existing work and its limitations

The objective of the proposed method is to improve the quality and to provide higher security and authenticity to the secret image. This is done by proposing modifications to the existing TiOISSS scheme. This section discusses the existing TiOISSS and its limitations.

2.1 Existing TiOISSS

TiOISSS [8] is a method in which the secret image to be encrypted is split into n shares separately using two methods; VCS and PISSS. The shadows of VCS are binary images whereas in PISSS, the shadows are grayscale images. The black pixels in the VCS shadows are replaced by corresponding gray value pixels of PISSS shadows. After this replacement, the shadows obtained are termed as Gray VCS (GVCS) shadows. These shadows are distributed to the users. In the first decoding phase, the users have to simply stack the GVCS shadows by which a vague image is obtained. In the second decoding phase, the PISSS shadows are extracted from GVCS shadows by discarding the white pixels in shadows and the secret image is reconstructed perfectly by computations from this extracted PISSS shadows.

2.2 Weakness of Existing TiOISSS

2.2.1 Weakness 1

The grayscale secret image has to be halftoned for the shares to be created. Traditional schemes use AM halftoning which is suitable for constantly varying image, however this does not produce the continuous illusion of secret image. So, the existing TiOISSS scheme uses FM halftoning technique [8, 9, 19] with error diffusion and this adds error to the neighboring pixel. The Fig. 1(a) is cameraman image and Fig. 1(b) is FM halftoned cameraman image. It is observed that FM halftoning is not able to produce fully black pixels as in the coat of cameraman and there are scattered white pixels. It is already known that, in VCS on overlapping two shares, wherever there is a black pixel in the secret image a complete black is produced whereas white tends to produce half black and half white pixel. Therefore, for every white pixel in the secret image, there is 50 % loss for each white pixel in the reconstructed secret image. So, when the shares are created from the FM halftoned image, it is not able to reproduce a full black pixel at the reconstruction phase. Thus, the contrast of the image in the reconstruction phase gets degraded due to the FM halftoning technique. Therefore, FM halftoning is not suitable for constantly varying pixels of the secret image.

2.2.2 Weakness 2

In the existing TiOISSS scheme, to create the PISSS shadows, the secret image has been permuted using any one of the permutation method with a 32 bit key. This 32 bit key is also communicated to the end user by means of a secure channel. This small key size may be

(a) (b)

Fig. 1 Results for FM halftoning: a Secret image b FM halftoned secret image

subject to attacks like Brute Force attack and Man-in-Middle attack in which the attacker tends to change or capture the key.

3 Proposed modified TiOISSS scheme

To overcome the limitations of the existing scheme, three modifications are proposed. Better quality is achieved using adaptive halftoning and security is enhanced using both pixel and bit permutation with a larger 64 bit key. In addition, the proposed work embeds a secret message which is used for authentication of the secret image.

3.1 Adaptive halftoning

This paper proposes a halftoning method which combines the advantages of existing halftoning methods, namely AM and FM halftoning. This is referred to as Adaptive halftoning. Adaptive halftoning overcomes the disadvantages of both the AM and FM halftoning and it is suitable for images with sharp transition pixel values as well as constantly varying pixels.

The steps for the Adaptive Halftoning are given as follows:

1. The secret grayscale image S of size M×N is taken as input. The image is divided into z× z window blocks. The window block must be a square matrix.
2. Window size (z) should be optimal such that a larger window size does not leave out fine details and a smaller window is not suitable for constantly varying image.
3. The mean value of pixels for each window ($\overline{w}$) is calculated using (1)

$$\overline{w} = \frac{1}{Z \times Z} \sum_{i,j}^{Z} w_s(i,j) \tag{1}$$

4. The mean is then reduced by dividing it by a factor l, **where** $l = 1, 2, \ldots\ldots\ldots\ldots \overline{w}$

5. The mean ($\overline{w}$) for each window is checked if it is greater or smaller than 127. The value 127 is chosen because the median value of the grayscale pixel is 127, as pixel values range from 0 to 255.
6. If the mean ($\overline{w}$) is less than 127, then add the reduced mean value ($\frac{\overline{w}}{l}$) with 127 else subtract from 127. The resultant value is referred to as Adaptive threshold value t and is given by (2).

$$Adaptive\ threshold,\ t = \begin{cases} 127 + \dfrac{\overline{w}}{l}, \overline{w} \leq 127 \\ 127 - \dfrac{\overline{w}}{l}, \overline{w} > 127 \end{cases} \tag{2}$$

   This is taken as the threshold value for that corresponding window and this value adaptively changes depending on the pixels within the window. Thus, by doing this, one can overcome the problem of FM halftoning thereby achieving good quality for a constantly varying image.
7. The Adaptive threshold is compared with each element of the window to determine the halftone pixel. That is, the error between the current pixel value and threshold is computed.
8. The error is added to the neighboring pixel. This makes it suitable for images of sharp transition.
9. The steps from 3 to 8 are repeated for all the windows and the window is made to traverse through the entire image.

By following the steps 1 to 9, the secret image is halftoned using the proposed Adaptive halftoning and then shadows are generated. Thus, the proposed algorithm adapts the threshold depending on the nature of the pixels i.e. constantly varying or sharp transition resulting in better quality of the reconstructed image.

3.2 PISSS shadow generation

In the proposed work, two stages of permutation are performed. For PISSS shadow generation, the secret image is permuted using pixel permutation, in addition to bit permutation. As the proposed work performs an additional pixel permutation, another 32 bit key is required; hence the proposed method uses totally 64 bit key unlike 32 bit key in the existing scheme.

The steps for PISSS shadow generation are as follows:

1. The secret image is permuted first by using bit permutation with a 32 bit key. For the bit permutation, each pixel value is converted to a 8 bit binary number and these 8 bits are permuted according to the key.
2. Next, the bit permuted secret image is permuted using pixel permutation using another 32 bit key. For the pixel permutation, group of 8 pixels are taken and they are permuted according to the key. This order of permutation can also be carried out alternatively. This is indicated by a bit used in the key given to the user.
3. Finally, the PISSS shadows are generated from this permuted image as per Thien *et al.* scheme [15]. After the PISSS shadows are generated, the replacement of pixels between VCS and PISSS shadows is done to generate the GVCS shadows.

When the secret image is reconstructed by stacking the GVCS shadows, a degraded visual quality secret image is produced. This problem arises during the replacement of pixels between the shadows. Since the black pixels in VCS are being replaced, the replacing gray pixel value of PISSS shadows should be nearer to the black pixel value. But the gray pixels of PISSS shadows are in the range of (0–255) and therefore a degraded visual quality secret image is obtained in the first decoding phase. Hence, the proposed method modifies all the gray pixels of PISSS shadows, by dividing it by a constant value of 2^r (where r=0,1,2…7). By dividing all the pixels, they are reduced to smaller values, which resemble the black pixels and therefore this method can provide better visual quality of reconstructed image.

It should be noted that in the decoding phase, after the extraction of PISSS shadows from GVCS shadows, all the pixels of PISSS shadow have to be multiplied with the same 2^r which is used in encoding phase and then inverse PISSS operation has to be applied. Unlike Yang *et al.* scheme [19], the proposed method does not increase the size of the GVCS shadows and yet it provides better visual quality.

3.3 Enhanced GVCS shadows (EGVCS)

The GVCS shadows are created by replacing black pixels of VCS shadows by gray value pixels of PISSS shadows. To enhance the security further, the secret key and a secret message are embedded in all the GVCS shadows and the finally generated shadows are termed as Enhanced GVCS shadows (EGVCS). This secret message which is embedded can be used to verify the authenticity of image.

3.4 Key distribution

The Fig. 2 shows the key distribution for the (2, 2) scheme. The total key size is 64 bits for each user.

The following steps explain the distribution of the key.

1. The 64 bit permutation key is partitioned into two parts such that shadow1 contains 32 bits of Bit Permutation Key and shadow2 contains 32 bits of Pixel Permutation Key. To perform bit level permutation, each pixel is represented by 8 bits. Therefore, the bit positions range from 1 to 8. The bit position value is represented using 4 bits. Hence, the number of bits (8) and its positional references bits (4) requires 8×4=32 bits of key for bit level permutation. This Bit Permutation Key is embedded in shadow 1. Similarly, for pixel level permutation, pixels in the image are considered as blocks of 8 pixels. The pixel position in the block ranges from 1 to 8. This is represented using 4 bits. Hence, the number of pixels (8) and its positional reference in the block generates 8×4=32 bits of key for pixel level permutation. This Pixel Permutation Key is embedded in shadow 2.
2. When the shadow is distributed to user, the user do not know which of the shadows contain Bit or Pixel Permutation Key. The “Type of key” bit represents if the permutation key in the shadow represents “Bit Permutation Key” or “Pixel Permutation Key”. One bit is assigned for this purpose. Hence, if “Type of key” bit is 0, it identifies that the shadow has Bit Permutation key and if it is 1, it implies that the shadow has Pixel Permutation Key.
3. The end user should know which permutation has to be done first such that the secret image can be reconstructed efficiently. The bit “Type of Permutation” in the Fig. 2

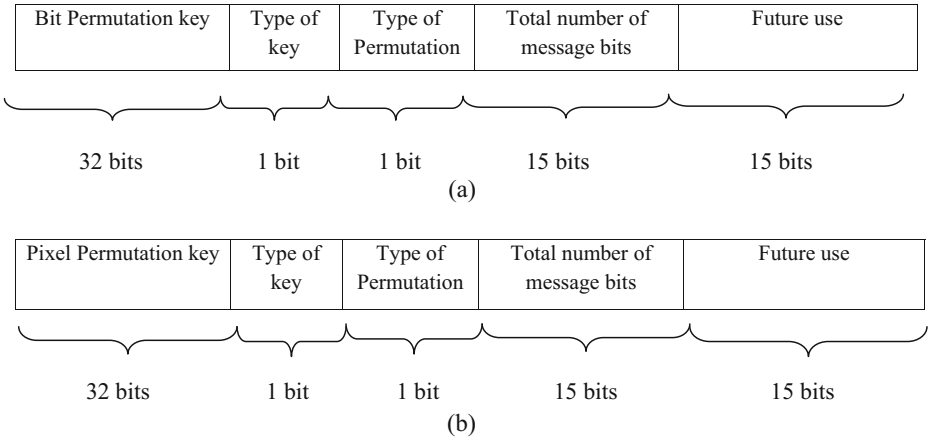

Fig. 2 Key distribution of (2, 2) scheme: a shadow1 b shadow2

represents the order of permutation to be carried out during the decoding process (i.e., to perform bit permutation first or pixel permutation first). This is assigned one bit.

4. In the proposed scheme, to authenticate the image, a part of a secret message is embedded in the Least Significant bit (LSB) of some pixels of the GVCS shadows. This should be communicated to the end user, else the user may decode all the LSB of the pixel values which may lead to the incorrect message. So the total number of message bits which are embedded in shadows is given as part of the key. The proposed (2, 2) scheme uses 15 bits which is 1.5 KB of information.
5. The last 15 bits are reserved for the future use so that the sender can use block permutation in addition to bit and pixel permutation. The sender can also increase the total number of message bits thereby sharing information up to 10 KB by using images of larger size.

3.5 Decoding

As stated above, Two in One Image Secret Sharing Scheme (TiOISSS) has two decoding phases and they are illustrated separately below.

3.5.1 First Decoding Stage

When the end users stack all their EGVCS shadows together, a vague image can be visually recognized without aid of any computations. In VCS, the simple OR operation is used to decode the secret image from shadows. Since the GVCS shadows contain the gray value they cannot be decoded by OR operation which can operate only on 0 and 1. Hence, the decoding of TiOISSS can be performed as follows:

Let *g1* and *g2* be two grayscale values of EGVCS shadows. Stacking the shadows, the value *g3* can be approximately expressed as in [9] as

$$\mathrm{g3} = \mathrm{int}\frac{(\mathrm{g1} \times \mathrm{g2})}{255} \tag{3}$$

where the int (.) function approximates its argument to the nearest integer. It is seen that the resultant vague image obtained provides better quality than the existing methods as Adaptive halftoning is used in the proposed scheme.

3.5.2 Second Decoding Stage

The second decoding stage should be done with the help of computation. Before reconstructing the secret image, the key which is embedded should be retrieved. This key provides the information such as Bit Permutation Key, Pixel Permutation Key, type of permutation key in each shadow, type of permutation that should be carried out first and total number of message bits that gets embedded in each shadows. From the total number of message bits, one can reveal the secret message from each shadow and thus by combining the entire message of all the shadows, the user gets the complete information of secret message.

Now by discarding the white sub-pixel from EGVCS shadows, PISSS shadows are extracted. This provides perfect reconstruction of the secret message using Lagrange Interpolation which is illustrated in [15]. After extracting the PISSS shadows, the following steps are carried out to reveal the secret image.

1. Take the first non-used k pixels from each of the shadow images. k corresponds to the threshold for a user having shadows$\geq k$, to reconstruct the secret image.
2. Use the k pixels and Lagrange's interpolation to solve for the coefficients and constant term. The Lagrange interpolation formula to obtain the coefficients $\boldsymbol{l_i}$ is given by

$$\boldsymbol{l_i} \equiv \prod_{\substack{1 \leq j \leq k \\ i \neq j}} \frac{\boldsymbol{x} - \boldsymbol{x_j}}{\boldsymbol{x_i} - \boldsymbol{x_j}} \tag{4}$$

In the Eq. (4), to obtain corresponding $\boldsymbol{l_i}$ coefficient, the variable x is used such that k pixels are identified from it. This implies that x^0 is first pixel, x^1 is second pixels …. and x^{k-1} is k^{th} pixel.

Then the polynomial function f(x) is determined as,

$$\boldsymbol{f(x)} = \sum_{\boldsymbol{i}=1}^{\boldsymbol{k}} (\boldsymbol{s_i} \times \boldsymbol{l_i}) \ \boldsymbol{mod}\ \boldsymbol{q} \tag{5}$$

where q is a prime number, $\boldsymbol{l_i}$ is Lagrange coefficient and $\boldsymbol{s_i}$ is pixel of extracted PISSS shadow from EGVCS shadows.

3. These coefficients are the corresponding k pixel values of the permuted image.
4. Repeat above steps, until all pixels of the k shadow images are processed.
5. When all pixels of image get processed, apply the inverse permutation operation to get the secret image. The key required for the inverse permutation should be obtained from EGVCS shadows as stated before and secret image has to be reconstructed.

4 Results and discussion

This section discusses the experimental results of the Modified TiOISSS. The results are discussed here for (2, 2) and (4, 4) scheme. The secret image taken here is cameraman image of size 256×256 as shown in Fig. 3(a). The Adaptive halftoned secret image which is of size 256×128 is shown in Fig. 3(b). It should be noted that the Adaptive halftoned secret image can provide complete black pixels in the coat of cameraman unlike the FM halftoned image in Fig. 1(a). From the Adaptive halftoned secret image, the shadows are generated with pixel expansion m=2 using VCS of size 256×256. For PISSS shadow generation, the secret image is permuted using bit and pixel permutation using a 64 bit key. Shadows are created from this permuted image using PISSS of size 256×128 shown in Fig. 3(c) and (d). The GVCS shadow are obtained by replacing black pixels of VCS shadow with corresponding gray pixels of PISSS shadows. In the proposed method, the secret message and key are embedded in GVCS shadows. The finally obtained EGVCS shadows of size 256×256 shown in Fig. 3(e) and (f) are distributed to the users.

In the first decoding phase, by stacking the EGVCS shadows a vague secret image is obtained as shown in Fig. 3(g). It is clear from Fig. 3(g) that the contrast of reconstructed secret image is higher since it is able to recover full black pixels. For second decoding phase, first the secret key and secret message are recovered. By using the key, one can perfectly reconstruct the secret image shown in Fig. 3(h). The proposed method also reveals the secret message at the decoding phase which is useful to verify the authenticity of the image. The secret message which is embedded in GVCS shadows during encoding process is 1.5 KB size. It should be noted that the size of the secret message can be increased with the size of the secret image.

5 Performance analysis

The proposed method was analyzed with various parameters to demonstrate the improvement in quality of the reconstructed secret image and its enhanced security compared to the existing methods.

5.1 Quality analysis

The proposed Adaptive halftoning is compared with traditional halftoning methods like AM and FM halftoning using quality parameters such as Contrast, Structural Similarity Index Measure (SSIM) and Peak Signal to Noise Ratio (PSNR).

5.1.1 Contrast

Contrast is often used to evaluate the visual quality of VCS. Contrast is defined as the difference between the average gray values of white and black secret pixels in the reconstructed image as in [8]. In the proposed method, the contrast is taken between the blocks of reconstructed pixels greater than 127, (C_0) and the blocks of reconstructed pixels lesser than 127, (C_1) and hence the contrast of the reconstructed image is defined as,

$$\alpha = \frac{\boldsymbol{C}_0 - \boldsymbol{C}_1}{255} \tag{6}$$

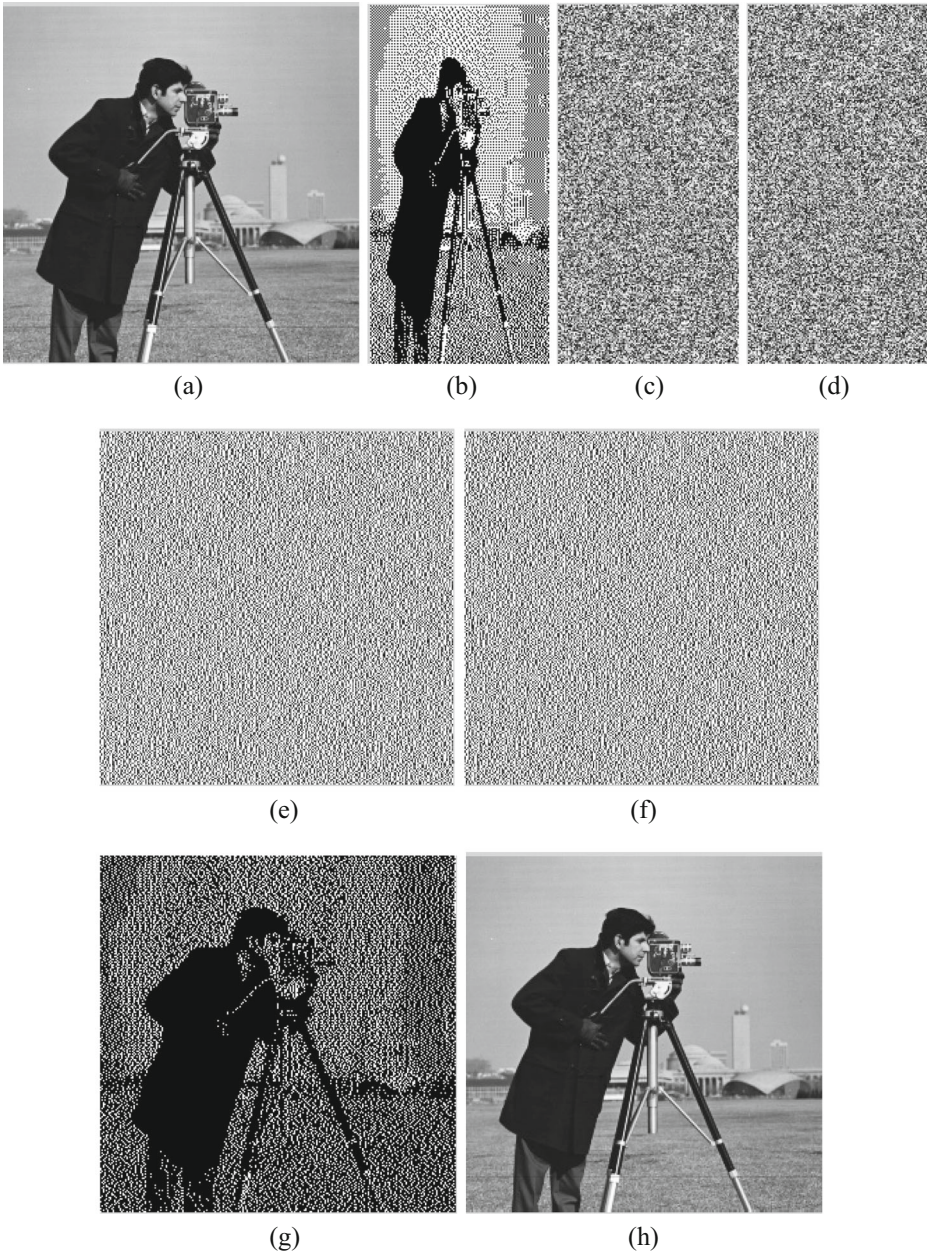

Fig. 3 Results of (2, 2) Modified TiOISSS: a secret image, b Adaptive halftoned secret image, c and d PISSS shadows, e and f EGVCS shadows, g Vague image by stacking GVCS shadows, h Reconstructed secret image by computations

As stated earlier in Section 3.2, in order to provide better visual quality of reconstructed image all the pixels of PISSS shadow are divided by 2^r (where r=0,1,2,….7). Table 1 shows the contrast between original secret image and reconstructed secret image after first decoding

Table 1 Comparison of Contrast for different halftoning techniques for (2, 2) decoding with different values of *r*

r	AM	FM	Adaptive
0	0.0532	0.0591	0.0648
1	0.1190	0.1209	0.1324
2	0.1580	0.1660	0.1809
3	0.1797	0.1884	0.2073
4	0.1915	0.2004	0.2237
5	0.1976	0.2068	0.2276
6	0.2009	0.2098	0.2318
7	0.2013	0.2133	0.2334

phase, for different values of *r*. Higher the contrast value, better is the visual quality. As can be observed, the contrast value is improved for Adaptive halftoning technique compared to AM and FM halftoning. It is also seen that the contrast also increases with *r*.

5.1.2 SSIM

The Structural Similarity Index Measure (SSIM) is used to measure the similarity between two images. The SSIM metric is calculated for various windows of an image. The measure between two windows *x* and *y* of common size $N \times N$ is given by

$$\boldsymbol{SSIM}(\boldsymbol{x},\boldsymbol{y}) = \frac{\left(2\mu_x\mu_y + \boldsymbol{c}_1\right)\left(2\boldsymbol{\sigma}_{\boldsymbol{xy}} + \boldsymbol{c}_2\right)}{\left(\mu_{\boldsymbol{x}}{}^2 + \mu_{\boldsymbol{y}}{}^2 + \boldsymbol{c}_1\right)\left(\boldsymbol{\sigma}_{\boldsymbol{x}}^2 + \boldsymbol{\sigma}_{\boldsymbol{y}}^2 + \boldsymbol{c}_2\right)} \tag{7}$$

where

$\boldsymbol{\mu_x}$ and $\boldsymbol{\mu_y}$ are the average of *x* and *y*
$\boldsymbol{\sigma_x^2}$ and $\boldsymbol{\sigma_y^2}$ are the variance of *x* and *y*, $\boldsymbol{\sigma_{xy}}$ is the covariance of *x* and *y*
$\boldsymbol{c}_1=(\boldsymbol{k}_1\boldsymbol{L})^2$ and $\boldsymbol{c}_2=(\boldsymbol{k}_2\boldsymbol{L})^2$ are two variables to stabilize the division, *L* is the dynamic range of the pixel values and $\boldsymbol{k}_1=0.01$ and $\boldsymbol{k}_2=0.03$ by default.

Table 2 Comparison of SSIM for different halftoning techniques for (2, 2) decoding with different values of *r*

r	AM	FM	Adaptive
0	0.0151	0.0166	0.0197
1	0.0362	0.0346	0.0424
2	0.0394	0.0528	0.0682
3	0.0485	0.0610	0.1126
4	0.0535	0.0628	0.1421
5	0.0517	0.0590	0.1175
6	0.0402	0.0537	0.0838
7	0.0478	0.0501	0.0612

Table 2 shows the comparison of SSIM between existing AM and FM halftoning and the proposed Adaptive halftoning method for (2,2) VCS scheme. SSIM is calculated between original secret image and vague reconstructed image after first decoding phase. From the table, it is observed that the visual quality of the reconstructed vague image is improved using Adaptive halftoning compared to the existing halftoning methods since it retains black pixels. Table 4 shows the SSIM for various natural images using the proposed Adaptive halftoning method.

5.1.3 PSNR

The Peak Signal to Noise Ratio (PSNR) is a measure of image quality based on the pixel difference between two images. It is a measure to estimate of quality of reconstructed image compared with original image. PSNR is defined as

$$\boldsymbol{PSNR} = 10\boldsymbol{log}\frac{\boldsymbol{s}^2}{\boldsymbol{MSE}} \tag{8}$$

where s=255 for an grayscale image and *MSE* is Mean Square Error.

Table 3 shows the comparison of PSNR between existing AM and FM halftoning and the proposed Adaptive halftoning method for (2, 2) VCS scheme. The PSNR has been calculated between the secret image and reconstructed vague image of first decoding phase.

The Modified TiOISSS has been simulated for the various images which are tabulated in Table 4. The experiment was also conducted for (4, 4) Modified TiOISSS scheme. Tables 5 and 6 shows the results obtained for (4, 4) scheme. In this case also the contrast and SSIM value is increased compared to the existing method. It should be noted that contrast and SSIM are taken for vague image and PSNR values are taken for both first decoding phase and perfect reconstructed image obtained by PISSS in the second decoding phase.

6 Security analysis

VCS and PISSS are secure cryptographic techniques as described in [13] and [15] such that one can reconstruct the secret information only by using greater than or equal to k shadows in (k, n) scheme, and one cannot retrieve any information from less than k shadows. Since the proposed Modified TiOISSS combines the techniques of VCS and PISSS, it can provide high level of security. But the existing TiOISSS method has limitations in security. In the existing work, for

Table 3 Comparison of PSNR (first decoding phase) for the different halftoning techniques for (2, 2) decoding with different values of r

r	AM	FM	Adaptive
0	6.53 dB	6.36 dB	6.65 dB
1	6.55 dB	6.48 dB	6.68 dB
2	6.61 dB	6.62 dB	6.84 dB
3	6.72 dB	6.64 dB	6.84 dB
4	6.92 dB	6.89 dB	7.05 dB
5	7.31 dB	7.28 dB	7.43 dB
6	7.86 dB	7.76 dB	7.98 dB
7	7.36 dB	7.31 dB	7.41 dB

Table 4 Comparison with different images for (2, 2) decoding with r=4

Different images	Contrast (First decoding)	SSIM (First decoding)	PSNR (first decoding)	PSNR (Second decoding)
Mandril	0.1259	0.0385	5.62 dB	36.65 dB
Cameraman	0.2237	0.1421	7.05 dB	39.98 dB
Lake	0.2358	0.0562	6.27 dB	40.42 dB
Lena	0.1498	0.0343	6.14 dB	35.36 dB

the PISSS shadows to be created, the secret image is permuted using only one permutation method with a 32-bit key. This may lead to Brute Force and Man-in-Middle attack.

In this proposed Modified TiOISSS scheme, the permutation is done both at bit level with a 32 bit key and at pixel level with another 32 bit key, and both the keys are embedded in the GVCS shadows. The order of the permutation is also decided in the encoding phase and a separate bit is assigned for the use of decoding by the user. Thus, the security of the scheme is enhanced not only by increasing the key size but also by performing two levels of permutations.

In VCS schemes, after the generation of shadows, it is distributed to the users. During the distribution, if an attacker gets any of the shadows it should be robust to any attack. Hence, in the proposed Modified TiOISSS scheme, the permutation keys are evenly distributed in all the EGVCS shadows. In addition, a secret message is embedded in the EGVCS shadows to verify the authenticity of the secret image.

6.1 Contrast test

The security of the proposed scheme is analysed by using the parameter Contrast. Contrast, used in quality analysis, determines the visual quality of reconstructed secret image and this can also be used in security analysis. The contrast between halftoned and reconstructed secret image determines how much the decoded secret image is reconstructed similar to halftoned image and so it is used as a quality evaluation parameter. Therefore, by determining the contrast between halftoned and EGVCS shadow one can determine how much the shadow image is dissimilar to halftoned image.

In traditional VCS scheme [4] which involves only binary pixels, the light transmission has been used to analyze the security of the proposed method. This light transmission cannot be used in our proposed method since our method involves gray pixels in shadows. Therefore, we have used the parameter Contrast from [8] to determine the security of the proposed method. It should be noted that the contrast value which is determined between shadow and halftoned secret cannot reach the value of 0 as in [4]. This is because of gray value pixels of EGVCS shadow. Hence, the value of contrast between the halftoned secret image and shadow image

Table 5 Comparison of Halftoning techniques for (4, 4) decoding with r=4

Types of Halftoning	Contrast (First Decoding)	SSIM (First Decoding)	PSNR (First Decoding)	PSNR (Second decoding)
AM	0.0785	0.0256	5.36 dB	17.87 dB
FM	0.0819	0.0306	5.58 dB	17.87 dB
Adaptive	0.1298	0.0315	6.27 dB	17.87 dB

Table 6 Comparison with different images for (4, 4) decoding with r=4

Different images	Contrast (First decoding)	SSIM (First Decoding)	PSNR (First Decoding)	PSNR (Second decoding)
Mandril	0.0775	0.0276	5.03 dB	17.69 dB
Cameraman	0.1298	0.0315	6.27 dB	17.87 dB
Lena	0.1002	0.0306	5.41 dB	17.28 dB
House	0.9941	0.0280	5.26 dB	16.27 dB

should be closer to zero to ensure the level of security such that if an attacker gets any one of the shadow he/ she cannot retrieve any information regarding the secret image.

Hence, a smaller contrast value between the secret image and share means there is no relationship between the secret image and the share. Tables 7 and 8 show the Contrast between EGVCS shadow and secret image for the proposed (2, 2) and (4, 4) scheme respectively.

From the Tables 7 and 8, it is clear that the contrast between EGVCS shadow and secret image approaches to 0 which means that if an attacker gets any of the shadows, he/she cannot retrieve any information from the shadows. It should be noted that the negative sign in Contrast value indicates that the gray pixel get oppositely replaced, which means that in place of black pixel in secret image, the corresponding gray pixel nearer to white colour gets replaced in the shadow and vice versa for the white pixel of secret image.

In addition to Contrast, various other security features have been analyzed to prove the improved level of security of the proposed method.

6.2 Key space

Key space is the set of all possible values that can be used to generate the key and it determines the strength of the cryptosystem. The proposed (2,2) scheme uses 128 bit key, i.e. 64 bits per user, and so the key space is given by $2^{128}=3.4\times10^{38}$ which is enough to resist all kinds of Brute Force attacks. In addition, it uses two levels of permutations, thereby providing sufficient extent of confusion.

6.3 Key sensitivity test

A minor alteration in the key should cause a substantial change in the cipher image. To test this influence, two common quantitative measures are used. They are,

- Number of Pixels Change Rate (NPCR)
- Unified Average Changing Intensity (UACI)

Table 7 Contrast for share images for (2, 2) scheme with r=4

Images	Contrast
EGVCS shadow 1 & secret image	0.0007
EGVCS shadow 2 & secret image	−0.0005

Table 8 Contrast for share images for (4, 4) scheme with r=4

Images	Contrast
EGVCS shadow 1 & secret image	0.00000041
EGVCS shadow 2 & secret image	−0.000085
EGVCS shadow 3 & secret image	−0.000025
EGVCS shadow 4 & secret image	0.000017

They are defined as follows,

$$\boldsymbol{NPCR} = \sum_{i,j} \frac{\boldsymbol{D}(\boldsymbol{i},\boldsymbol{j})}{\boldsymbol{M} \times \boldsymbol{N}} \times 100\% \tag{9}$$

$$\boldsymbol{UACI} = \frac{1}{\boldsymbol{M} \times \boldsymbol{N}} \left(\sum_{i,j} \frac{|\boldsymbol{C}_1(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{C}_2(\boldsymbol{i},\boldsymbol{j})|}{255} \right) \times 100\% \tag{10}$$

where C_1 and C_2 are the two GVCS shadows whose corresponding key have only bit difference, M and N are the dimension of the shadows. $D(i, j)$ is determined from C_1(i, j) and C_2(i, j) as in [17].

$$\mathrm{D(i,j)} = \begin{cases} 1, & \mathrm{C_1(i,\ j) = C_2(i,\ j)} \\ 0, & \textit{otherwise} \end{cases} \tag{11}$$

From the simulation results, the average NPCR and UACI for minor changes in Bit Permutation Key after 100 trials are 90.65 % and 35.75 % respectively. Similarly, the average NPCR and UACI for minor changes in Pixel Permutation Key are 90.72 % and 35.65 %. This shows that the proposed scheme has a good ability to anti differential attack.

6.4 Statistical analysis

The following statistical tests have been performed to prove the strength of the cryptosystem.

- Histogram
- Correlation of adjacent pixels

The histogram of the EGVCS shadows (for r=1) shown in Fig. 4 is uniform implying that the proposed scheme has good statistical property. It should be noted that in Fig. 4, all the pixels are uniformly distributed up to 127 (i.e. $255/2^r$) where r=1. Hence, by taking different values of r, the distribution of pixels is limited to corresponding value of $255/2^r$.

The Correlation coefficient is calculated between original secret image and EGVCS shadows by using the Eqs. (12) and (13).

$$\boldsymbol{cov}(\boldsymbol{x},\boldsymbol{y}) = \boldsymbol{E}(\boldsymbol{x} - \boldsymbol{E}(\boldsymbol{x})).\boldsymbol{E}(\boldsymbol{y} - \boldsymbol{E}(\boldsymbol{y})) \tag{12}$$

$$\boldsymbol{r_{xy}} = \frac{\boldsymbol{cov}(\boldsymbol{x},\boldsymbol{y})}{\sqrt{\boldsymbol{D}(\boldsymbol{x})}.\sqrt{\boldsymbol{D}(\boldsymbol{y})}} \tag{13}$$

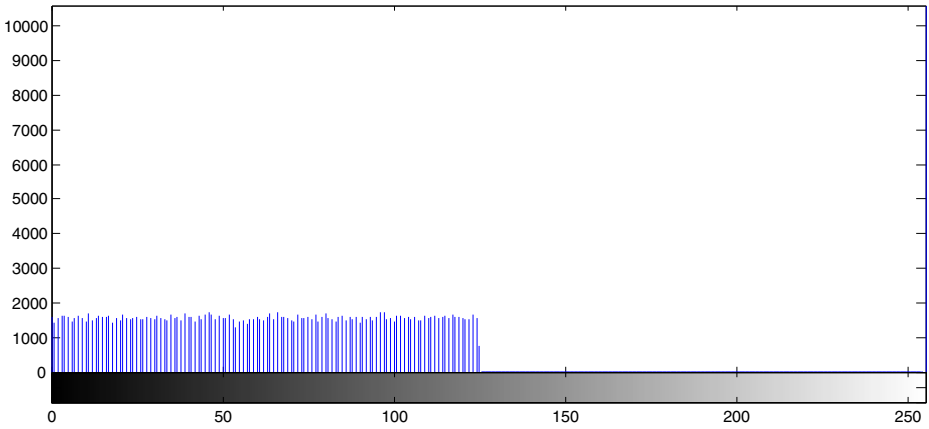

Fig. 4 Histogram of EGVCS shadow

where x and y are gray level values of two images, $E(x)$ and $E(y)$ are mean of x and y, $D(x)$ and $D(y)$ are variance of x and y. The Correlation coefficient between original secret image and EGVCS shadows is obtained as 0.0015, which means there is almost negligible correlation between secret image and shadows. In addition, Fig 5(a) and (b) shows the correlation distribution of adjacent pixels in secret image and EGVCS shadows (for $r=1$) respectively. This reveals that the adjacent pixels in secret image are highly correlated whereas EGVCS shadows are uncorrelated.

6.5 Resistance to other attacks

It is understood from the Fig. 4 that the shadows are not susceptible to the Brute force attack since all the pixel values get uniformly distributed. In addition, the key is embedded in EGVCS shadows unlike communicating to the end user in a secure channel in the existing scheme. Hence, the proposed scheme can overcome Man-in-Middle attack.

6.6 Merits of the Proposed scheme

1. In this paper, the Modified TiOISSS uses proposed Adaptive halftoning in which an adaptive threshold is used depending on constantly varying or abrupt transition pixel. This improves the quality of the first phase decoded image. From the Fig. 6, it is clear that the adaptive halftoning can reconstruct black pixels better than FM halftoning. Hence, Adaptive halftoning is more suitable for VCS.
2. To improve security, larger key size (64 bits per user) is used to resist Brute force attacks. Permutation is done both at bit level with a 32 bit key and at pixel level with another 32 key. The order of the permutation can also be decided in the encoding phase. For this, a separate bit is assigned to aid decoding by the user. In addition, the key is embedded in the EGVCS shadows itself. This prevents Man-in-Middle attack.
3. The existing TiOISS scheme [8] can share only a secret image. The proposed scheme embeds a secret message in the EGVCS shadows for authenticating the secret image.

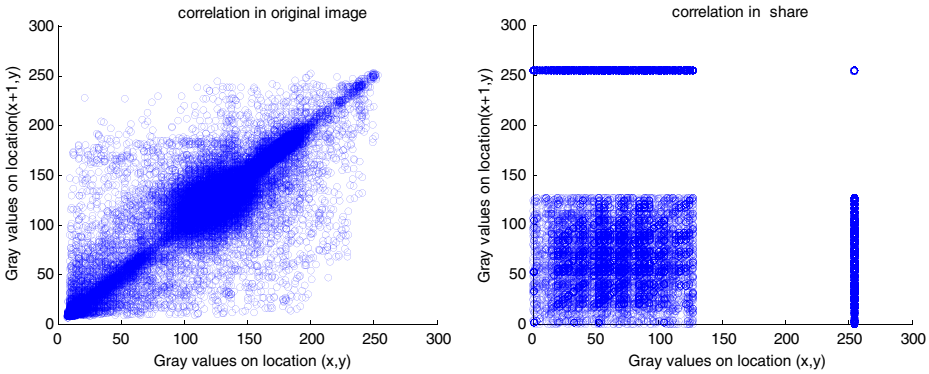

Fig. 5 Correlation of adjacent pixels: a secret image b EGVCS shadow

4. The proposed scheme can share both the secret image and plain text simultaneously. In the first decoding phase a vague image is reconstructed, and in the second decoding phase perfect reconstruction of secret image and plain text is obtained. In Enriched Secret Sharing Visual Cryptography Scheme (ESSVCS) [12] however, only vague image and plain text reconstruction is possible and the method is not able to produce perfect reconstruction of the secret image.
5. Compared to ESSVCS [12], the size of the message shared is larger in the proposed scheme. In addition, in the proposed scheme, the size of the message increases with size of the shadows whereas in ESSVCS the size of message remains constant even if the number of shadows increases.

7 Conclusion

Visual Cryptography is used for protecting image based secrets. To overcome the disadvantages in VCS, Modified TiOISSS is proposed. By applying Adaptive halftoning to the TiOISSS, the Contrast, SSIM and PSNR of the reconstructed secret image at the first decoding

Fig. 6 Comparison of halftoned images: a FM halftoned image b Adaptive halftoned image

phase is improved. Thus, quality of the reconstructed secret image gets improved by using proposed Adaptive halftoning. The Modified TiOISSS uses 128 bit key (64 bit per user) and part of this key gets embedded in all EGVCS shadows, thereby making Modified TiOISSS impervious to Brute force attack and Man-in-Middle attack. In addition, the proposed method was analyzed with various security aspects such as Key Space, Key sensitivity test and statistical analysis thereby proving that the Modified TiOISSS is highly secure. In the proposed scheme, secret message is shared in addition to the secret image which is useful for fraud prevention and authentication. Thus, the proposed Modified TiOISSS method has improved both the quality and security of the secret image.

References

1. Arumugam S, Lakshmanan R, Nagar AK (2014) On (k, n) visual cryptography scheme. J Des Codes Crypt 71(1):153–162
2. Arya KV, Rishiwal V, Yadav AK (2014) An efficient halftone visual secret sharing scheme, Proceedings of 9th International Conference on Industrial and Information Systems (ICIIS), 2014
3. Askari N, Heys HM, Moloney CR (2013) An extended visual cryptography scheme without pixel expansion for halftone images, Proceedings of 26th Annual IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2013
4. Chen T-H, Tsao K-H (2011) User-friendly random-grid-based visual secret sharing. IEEE Trans Circ Syst Video Technol 21(11):1693–1703
5. Guo T, Liu F, Wu CK (2013) Threshold visual secret sharing by random grids with improved contrast. J Syst Softw 86(8):2094–2109
6. Lee C-C, Chen H-H, Liu H-T, Chen G-W, Tsai C-S (2014) A new visual cryptography with multi-level encoding. J Vis Lang Comput 25(3):243–250
7. Leng L, Beng A, Jin T (2015) Alignment-free row-co-occurrence cancelable palmprint Fuzzy vault. Pattern Recogn 48(7):2290–2303
8. Lia P, Maa P-J, Sua X-H, Yang C-N (2012) Improvements of a two-in-one image secret sharing scheme based on gray mixing model. J Vis Commun Image Represent 23(3):441–453
9. Lin S-J, Lin J-C (2007) VCPSS:A two-in-one two-decoding options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches. J Pattern Recognit Lett 40(12):3652–3666
10. Lin C-C, Tsai W-H (2002) Visual cryptography for gray-level images by dithering techniques. J Pattern Recognit Lett 24(4):349–358
11. Lin T-L, Horng S-J, Lee K-H, Chiu P-L, Kao T-W, Chen Y- H, Ray-Shine R, Jui-Lin L, Rong-Jian C (2010) Novel multiple secret sharing. J Expert Syst Appl 37(12):7858–7869
12. Liu F, Yan WQ, Li P, Wu C (2014) ESSVCS: an enriched secret sharing visual cryptography. Trans Data Hiding Multimed Secur IX 8363:1–24
13. Naor M, Shamir A (1994) Visual cryptography, Alfredo De Santis (ed), Advances in cryptology proceedings of Eurocypto'94, lecture notes in computer science, vol. 950, pp. 1–12
14. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
15. Thien C-C, Lin J-C (2002) Secret image sharing. J Comput Graph 26(5):765–770
16. Wang D, Yi F, Li X (2009) On general construction for extended visual cryptography schemes. J Pattern Recognit 42(11):3071–3082
17. Wang Y, Wong K-W, Liao X, Chen G (2011) A new chaos-based fast image encryption algorithm. J Appl Soft Comput 11:514–522
18. Wu H-C, Chan C-C (2005) Sharing visual multi-secrets using circle shares. J Comput Stand Interfaces 28(1): 123–135

19. Yang C-N, Ciou C-B (2010) Image secret sharing method with two-decoding- options: lossless recovery and previewing capability. J Image Vision Comput 28(12):1600–1610
20. Yang C-N, Yang Y-Y (2014) New extended visual cryptography schemes with clearer shadow images. J Inf Sci 271(4):246–263
21. Yang C-N, Chen P-W, Shih H-W, Kim C (2013) Aspect ratio invariant visual cryptography by image filtering and resizing. J Pers Ubiquit Comput 17(5):843–850

Ms. Srividhya Sridhar has completed her post graduate programme in Electronics & Communication Engineering in Pondicherry Engineering College affiliated to Pondicherry University. She has completed her B. Tech in Electronics and Communication Engineering in 2013 in Pondicherry University. Her areas of interest in Cryptography and Image processing.

Mr. R. Sathish Kumar is currently working as Assistant Professor in the Dept. of Electronics & Communication Engineering in Perunthalaivar Kamarajar Institute of Engineering and Technology affiliated to Pondicherry University, Puducherry, India. He has completed his BTech and MTech in Electronics and Communication Engineering. He is pursuing his PhD with specialization in Image Security. He has 10 years experience in teaching.

Dr. Gnanou Florence Sudha is currently working as Professor in the Dept. of Electronics & Communication Engineering in Pondicherry Engineering College affiliated to Pondicherry University, Puducherry, India. She has completed her B. Tech and M. Tech in Electronics and Communication Engineering in 1992 and 1994. She completed her PhD with specialization in Image Processing in 2005. She has 20 years experience in teaching. She has several journal and conference proceedings to her credit. She is member of the Indian Society of Technical Education, Optical and Biomedical Society of India. Her areas of research and interest are Image Processing, Biomedical signal processing and Information Security. She has carried several research project with All India Council for Technical Education and Dept. of Science and Technology, India.