An Intelligent 2D Secret Share Construction using Visual Cryptography for Secure Transmission

N. Rajesh Kumar[1*], R. Bala Krishnan[2], G. Manikandan[3] and N. R. Raajan[4]
[3] School of Computing
[4] School of Electrical and Electronics Engineering
[12] SRC
[1234] SASTRA Deemed University
[12] Kumbakonam, [34] Thanjavur - India
[e-mail:rajeshkumar.rb@src.sastra.edu]
*Corresponding author: N. Rajesh Kumar

Received December 27, 2018; revised June 9, 2020; accepted June 17, 2020; published July 31, 2020

Abstract

Data Security is the most challenging area in Internet communication, where most of the secret sharing schemes are proposed for binary images. But still it lacks in providing security for data communication, especially in image transmission. Traditional visual cryptography scheme generate meaningless diwies and the reconstruction phase leads to quality degradation over the secret image. In this work, an intelligent two dimensional secret share construction scheme is proposed. A secret image is expanded into n diwies with the choice of scheme selection. By Stacking all the qualified diwies to revert the secret image without content loss and less than s* - 1 shares could not reveal any information about the secret image. The experimental results emphasize that the proposed secret share scheme is highly secured for image transmission.

Keywords: Diwy, secret sharing, image transmission, bound level, visual cryptography

1. Introduction

In data communication and network, visual communication plays a key role in making an extraordinary potential development in worldwide communication. This digital transmission has an increasing demand for higher data transfer rate with a larger bandwidth. According to the higher bandwidth demand, optical network communication is introduced to strengthen the data bandwidth. An optical network consists of a network setup where optical fiber serves as the central medium of digital transmission. There is a wide range of optical technology that are typically applied to achieve the following result.

- To increase the data transfer rate.
- Improve the efficiency of the network.
- Reduce the duration of time for data conversion.

However, data communication [5] has recently become a major issue in across the globe due to the development of multimedia application. It requires more security to transmit the data from sender to receiver. In order to achieve a secure data communication, earlier investigators focused on various types of protection mechanisms such as cryptography and information hiding. Cryptography is the process of storing and masking confidential data into mysterious format for data protection [16]. But information hiding [6, 20] is another way of secure communication for secret information by embedding it and extracting from cover media. These main disciplines are further broadly classified into several categories. Secret key, public key and hashing are part of cryptography techniques. Information hiding consists of steganography [15] and watermarking algorithms. Information hiding techniques include the key elements such as Secret data, Cover object, Data embedding function, Stego-object, Stego-key and Data extraction function. All these security systems originated for the protection of multimedia element. Nowadays, multimedia data transmission has a significant growth in many web-enabled environments. Especially, multimedia communication [18] used in mobile applications, web conferences, social networks, e-banking and engineering applications. At present, it is widely used in intelligent highway applications and mobile ad-hoc networks.

However, the developments of multimedia communications systems still lack in protection of [9] the transmitted data over the network. Classical cryptosystems conceal the context of secret information from all excluding the sender and receiver. Secret splitting [1] pertains to methods for disseminating a secret image among a group of different participants [13]. The secret sharing mechanism for numerical domain was proposed by Blackley and Shamir [11] in 1979.

Blackley investigated high for high dimensional space from the intersections of some higher dimensional planes. Shamir's [14] scheme was based on polynomial interpolation. The construction of secret sharing scheme for numerical domain was extended to image domain by Naor [10] and Shamir in 1994. This novel construction of sharing scheme is termed as visual secret sharing (VSS) or visual cryptography (VC) technique. The secret visual information in the form of text and pictures are encrypted in such a way that decryption becomes a mechanical process without the intervention of a computer. Approaches to visual secret sharing scheme could be classified into two categories:

- *Computational:* secret sharing and revealing process are based on numerical computation.
- *Non computational:* Conceal the confidential information in the form of transparencies and decipher it by superimposition. This stacking process doesn't require any mathematical computation.

The basic idea of visual secret sharing scheme is to transform an image into n shadow images that are transmitted to different participants. At the receiving end the original image could be revealed only if the sufficient number of shadow images are gathered.

Generally, the visual cryptographic technique implementation was the chaotic model for generating meaningful shares [3]. The researcher followed either expanding the original pixels (pixel expansion) or pixel non-expansion method to construct meaningful shares.

Numerous visual cryptography [2] approaches have been formulated by several cryptographers at different stages. These investigations were made for binary images and gray-level images, but still limitations exist. They are as follows:

- Low visual quality image.
- Noisy reconstruction.
- No scheme selection to generate diwy.
- Computation cost is high.

The remaining part of this paper is organized as follows. Section 2 briefly describes the related work of visual cryptography scheme. Section 3 explains the bound structure for proposed visual secret sharing scheme. The experimental results are shown in Section 4. Finally, conclusions are presented in Section 5.

2. Related Work

The first threshold scheme (k, n) proposed by the Israeli cryptographer Adi Shamir was based on polynomial interpolation. This numerical domain is expressed as follows:

S: Secret information
n: Number of participants
p: Prime number

The construction of Shamir threshold scheme is represented in Equation 1.

$$q(x) = S + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \quad (1)$$

Where $a_1, a_2, \ldots, a_{k-1}$ are randomly picked integers and $0 \le a_1, a_2, \ldots, a_{k-1} < p$. Then S is divided into n shares like $S_1, S_2, \ldots S_n$ and the shares are distributed to n participants. Where $S_1 = q(1) \bmod p, \ldots, S_i = q(i) \bmod p, \ldots, S_n = q(n) \bmod p$. This scheme requires k qualified subsets to reconstruct the secret information. It is represented in Equation 2.

$$S = q(x) - a_1 x - a_2 x^2 - \ldots - a_{k-1} x^{k-1} \quad (2)$$

In 1987, Kafri and Keren proposed visual secret sharing scheme through random grid without code book. Their efficient method avoids pixel expansion and does not require the structure of basic matrix [7]. An example of secret sharing is shown in **Fig. 1**.

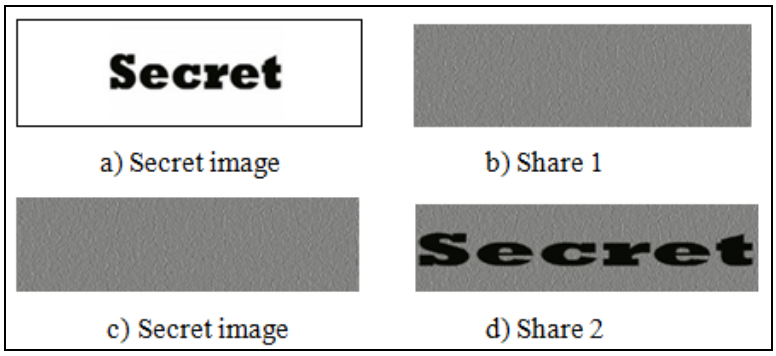


Fig. 1. Traditional visual secret sharing scheme

A new random grid [17, 19] method was proposed by Shyu based on the algorithm of Kafri and Keren. The scheme was extended to grayscale and color images. It applied on both random and secret images and attempted to increase the quality of image which is not focused in pixel expansion based visual cryptography scheme [4]. Pattern dithering technology was proposed by K. Oka, Y. Nakamura and K. Matsui in 1996. In this method, the grayscale image is converted into a binary image of m times the size. The white and black pixels are simulated into one pixel of the grayscale pattern and the transformation of black and white pixels is expanded to m dot matrix.

The pixel value of grayscale image is between 0 and 255. The graylevels are substituted by *t* levels and the obtained variations are for transformation of original grayscale image. The grayscale [8] value is represented in Equation 3.

$$n\times\lfloor 256/t\rfloor+1\sim(n+1)\times\lfloor 256/t\rfloor \tag{3}$$

Where, $0 \le n < t;$

$$2 \le t \le m+1; \quad \text{where} \quad n, m, t \in N;$$

When n=0, the level contains the grayscale value is zero. If the threshold [18] value is $n=t-1$ the maximum grayscale of this level is not larger than maximum value 255. Finally, this transformation leads to generate binary image of m times the size. Chao and Fan [21, 22] proposed an XOR-based progressive VSS scheme. This scheme used generalized random grids for sharing the secret and recovered the secret image using XOR operator. T Bhattacharjee et al. [23] presented threshold based secret image sharing scheme using affine boolean classification. This technique decoded the secret image after a large set of operations with PSNR value 30.5 dB. Some visual cryptography secret scheme was proposed to generate the shares for secure [12] data transmission. But the shares are meaningless and still some disadvantages do exist.

3. Proposed System

In this section, an intelligent two dimensional secret share construction using visual cryptography is proposed for secure image transmission. We developed an intelligent secret share construction scheme, presented in Algorithm 1 and reconstruction scheme presented in Algorithm 2. Firstly, we determine the bound structure for both lower and upper levels. Then the secret image is expanded into *n* number of diwies based on the choice of scheme selection in different orientation. In the reconstruction phase, by stacking all the qualified diwies to

revert the secret image without the loss of originality and less than s* - 1 reveal no information about the secret image.

3.1 Bound Structure

Generally the bound structure deals with the security level of the visual cryptography scheme. To know the detailed bound structure for the proposed scheme we can use set theoretical concept. To improve the security of the visual cryptography scheme the end user should determine the bound level of the secret image. The rough structure of bound level is illustrated in **Fig. 2-a**, **2-b and 2-c**.

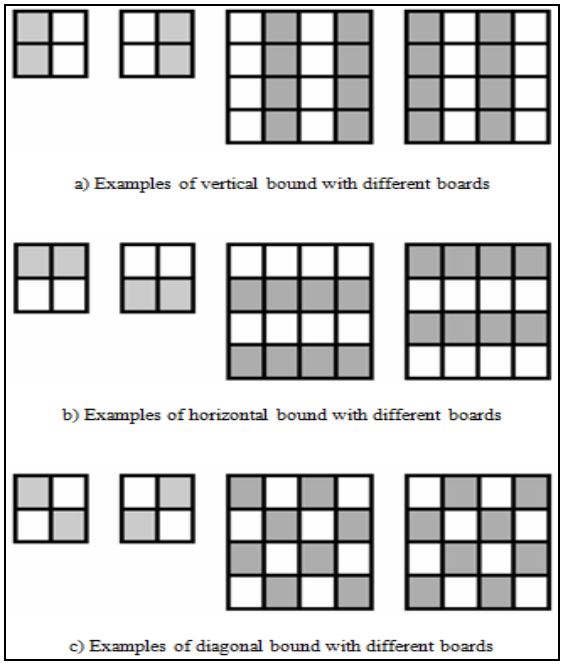


Fig. 2. Rough structure of bound level on 2×2 and 4×4 board

Lemma 1: To determine the lower bound of the secret image, it must satisfy the following conditions: The secret image dimension is defined in Equation 3.

$$S = \{(x, y) : x, y = 0,...N-1\}, \forall \{x, y\} \in S \tag{3}$$

The lower bound of secret image is denoted by L and satisfies the following conditions.

- $S\{x, y\} \neq \varnothing, \forall\ x, y \in \mathrm{N}$
- If $S\{x, y\} \neq \varnothing, L = 2^i$ for i=1,2,3,….N.
- If L=2 for i=1; is the lower bound for all $S\{x,y\}$;

Lemma 2: To determine the upper bound of the secret image, it must satisfy the following conditions. The upper bound is denoted by U.

- $\{x : x \in S\}$ and x is an odd number = {1, 3, 5, . .}

The first level upper bound is denoted in Equation 4.

$$U_1 = x, \forall S\{x, y\} \in \mathrm{N} \tag{4}$$

- $\{x : x \in S\}$ and x is even number= {2, 4, 6,. . .}

The second level upper bound is denoted in Equation 5.

$$U_2 = x, \forall S\{x, y\} \in \mathrm{N} \tag{5}$$

It is clearly stated that both upper and lower bound levels deal with secrecy of the proposed intelligent 2-Dimensional share construction scheme (I2DSCS). The proposed scheme ensures both levels of bounds attaining in Lemma 1 and Lemma 2.

3.2 Intelligent Two Dimensional Share Construction Scheme

The rough idea of bound structure is described in the above section. Now, an intelligent two dimensional share construction scheme is proposed in this section. The intelligent scheme consists of two cases.

- Case 1: for bound level 8
- Case 2: for bound level 16

The notations used in the proposed scheme are listed in **Table 1**.

Table 1. The notations

Notation	Description
S	The secret image to be shared
I	Weighed factor to determine the bound level
H	Horizontal scheme selection for share generation
V	Vertical scheme selection for share generation
D	Diagonal scheme selection for share generation
N	Total number of shares to be shared
S^*	Number of shares to reconstruct the secret image

3.2.1 The case when bound level L=8, when i=2

Let $L= 2^i =2^3=8$. If the scheme selection is vertical (v), bound level L=8, the secret image contains gray-levels, the construction for secret sharing is followed as:

A Secret image S of size $m \times n$ is represented as a two dimensional matrix and pixel locations are denoted by the index values i and j.

Let $S = \bigcup_x \bigcup_y S_{x,y}$ where $x = 0, 1, 2,\ldots, M-1$

where $y = 0,1, 2,\ldots, N-1$

If the secret image is grayscale, the pixel elements are located in single channel and the index values range between 0 and 255. The maximum value of pixel intensity range R = 256,

{R : R is natural number}= {0, 1, 2, 3,…, R-1}

r is an element of set R. $\therefore r \in R$.

To construct the meaningful share, the secret image is resized into the nearest even series of dimension. When bound level L= 8, dimension D= 8 ×8,

Let $D_k = S$, where k = 1, 2,…, D. The pre-computation for the share generation process is denoted in Equation 6.

$$S_1 = S(mod)8 \; \forall \; D \tag{6}$$

The share generation and verification process is defined in Equation 7.

$$\begin{aligned}
Share\,1 &= \begin{cases} S_{(x,y)} & \text{when } S_1 = 0; \\ 0 & \text{when } S_1 = 1; \end{cases} \\
Share\,2 &= \begin{cases} S_{(x,y)} & \text{when } S_2 = 0; \\ 0 & \text{when } S_2 = 2; \end{cases} \\
&\bullet \\
&\bullet \\
Share\,7 &= \begin{cases} S_{(x,y)} & \text{when } S_7 = 0; \\ 0 & \text{when } S_7 = 7; \end{cases} \\
Share\,8 &= \begin{cases} S_{(x,y)} & \text{when } S_8 = 0; \\ 0 & \text{when } S_8 = 8; \end{cases}
\end{aligned} \tag{7}$$

Theorem 1: The share generation method satisfies the construction scheme $\left(\left\{S,(2\hat{}3)\times i\right\}^{HVD}, n, S^*\right)$, 2$D$ for every incremental value of i and the reminder value of the bound level 8 and its dimension series.

3.2.2 The case when bound level L=16

When i=4, $L = 2^i = 2^4 = 16$. If the scheme selection is vertical (v), bound level L=16, the number of meaningful shares are sixteen from the original image. The vertical share generation scheme is denoted by 'v'.

The secret Image is S, dimension of the original Image is D = D= 16 ×16 and the bound level L= 16. Let $D_t = S$, where t=1, 2,...,D. The pre-computation process is defined in Equation 8.

$$S_1 = S(mod)16 \; \forall \; D \tag{8}$$

The share generation and verification process is defined in Equation 9.

$$
\begin{aligned}
Share\ 1 &= \begin{cases} S_{(x,y)} & when\ S_1 = 0; \\ 0 & when\ S_1 = 1; \end{cases} \\
Share\ 2 &= \begin{cases} S_{(x,y)} & when\ S_2 = 0; \\ 0 & when\ S_2 = 2; \end{cases} \\
&\bullet \\
&\bullet \\
Share\ 15 &= \begin{cases} S_{(x,y)} & when\ S_{15} = 0; \\ 0 & when\ S_{15} = 15; \end{cases} \\
Share\ 16 &= \begin{cases} S_{(x,y)} & when\ S_{16} = 0; \\ 0 & when\ S_{16} = 16; \end{cases}
\end{aligned}
\tag{9}
$$

Theorem 2: The share generation method satisfies the construction scheme is $\left(\left\{S,\left(2\hat{}3\right)\times i\right\}^{HVD},n,S^{*}\right)2D$ for every incremental value of i and the reminder value of the bound level 16 and its dimension series for both odd and even index. An intelligent secret share construction is explained in Algorithm 1:

Algorithm 1*: Intelligent secret share construction*

Input: Image $I=\left(I[x,y]\right)_{x,y=0}^{N-1}$ with size of *m* × *n*

Output: Meaningful secret shares from S_1 *to* S_N

Step 1: Read the size of input Image.

Step 2: Determine the maximum number of shares with scheme selection.

` *Step 3: Compute the reminder value for each index value.*

Step 4: If reminder is zero, retain the pixel values.

Step 5: If reminder is non-zero, change the pixel values into white pixels

Step 6: Repeat step 3 to 5 until the number of shares are reached.

The reconstruction algorithm is explained in Algorithm 2:

Algorithm 2: Intelligent secret image reconstruction

Input: Secret share $S_1=\left(S_1[x,y]\right)_{x,y=0}^{n-1}$ *with size of m* × *n*

•

•

Secret share $S_N=\left(S_N[x,y]\right)_{x,y=0}^{n-1}$ *with size of m* × *n*

Output: Reconstructed secret image I.

Step 1: Collect the number of secret shares from S_1 to S_N

Step 2: Compute the number of stacking operations.

Step 3: Stack the collected shares one by one with the result of previously stacked operation.

Step 4: Repeat step 3 until the number of stacking operations get completed.

Step 5: Reveal the secret image.

4. Experimental Observations

The performance of proposed scheme is tested with different type of grayscale images. The scheme selection phase determines the generation of number shares to enable the secure image transmission and ensure its protection. The construction scheme is well secured and the shares are meaningful. This computational method proves the properties of both theorems. The calculation of share image PSNR value is represented in Equation 10.

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \tag{10}$$

The PSNR values in **Table 2** show that the proposed scheme can restore a secret image with high visual quality.

Table 2. Experimental observations

Test Image	Image Size	PSNR (dB)	Correlation
fingerprint1.tif	128 × 128	53.27	0.8286
fingerprint2.tif	256 × 256	68.27	0.8880
tissue1.tif	128 × 128	50.87	0.8296
tissue2.tif	256 × 256	57.11	0.8251

The results of the share construction scheme in different orientations are shown in the **Fig. 3** and **Fig. 4**. **Table 3** shows the comparison of size between the secret 2*D* image and generated shares. The values show that the proposed scheme takes less amount of storage space because, the size of the share images are downsized.

Table 3. Comparison of model size in different orientation.

Types of orientation	2D model	Original Size (in kb)	No. of shares	Share Size (in kb)
Horizontal	tissue.tif	10.3	16	5
Vertical	fingerprint.tif	13	16	8
Diagonal	lena.tif	14	16	8

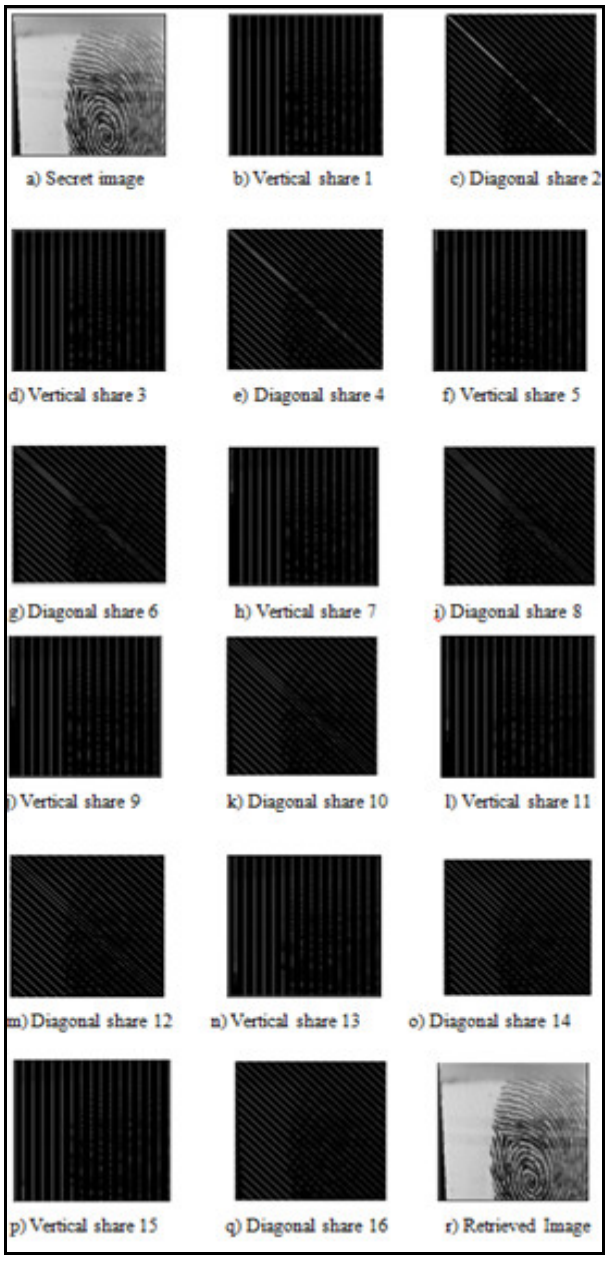


Fig. 3. Vertical and Diagonal secret sharing scheme

Fig. 4. Horizontal and Diagonal secret sharing scheme

The calculation of correlation coefficient is denoted in Equation 11.

$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

where x and y are the values of two adjacent pixels in an image. The $cov(x, y)$ and $D(x)$ are defined in Equation 12.

$$cov(x,y)=\frac{1}{m\times n}\sum_{i=1}^{m\times n}(x_i-E(x))(y_i-E(y)),$$

$$D(x)=\frac{1}{m\times n}\sum_{i=1}^{m\times n}(x_i-E(x))^2,\quad E(x)=\frac{1}{m\times n}\sum_{i=1}^{m\times n}x_i \tag{12}$$

The correlation coefficient between original image and sixteen share images in different orientations are summarized in **Table 4**.

Table 4. Comparison between various correlation coefficients

Type of Image	Horizontal	Vertical	Diagonal
Share 1	0.9722	0.9818	0.9645
Share 2	0.9750	0.9805	0.9598
Share 3	0.9724	0.9817	0.9624
Share 4	0.9725	0.9815	0.9623
Share 5	0.9722	0.9816	0.9629
Share 6	0.9717	0.9802	0.9638
Share 7	0.9716	0.9795	0.9637
Share 8	0.9723	0.9799	0.9627
Share 9	0.9731	0.9801	0.9641
Share 10	0.9726	0.9818	0.9638
Share 11	0.9734	0.9818	0.9630
Share 12	0.9746	0.9818	0.9622
Share 13	0.9733	0.9818	0.9610
Share 14	0.9731	0.9816	0.9616
Share 15	0.9738	0.9827	0.9616
Share 16	0.9733	0.9817	0.9601
Original Image	0.9458	0.8179	0.9260
Restored Image	0.9457	0.8178	0.9260

The comparison of correlation coefficients is illustrated in **Fig. 5**. From **Table 4**, the correlation of restored image has the same value that indicates the proposed scheme, provides high visual quality reconstruction.

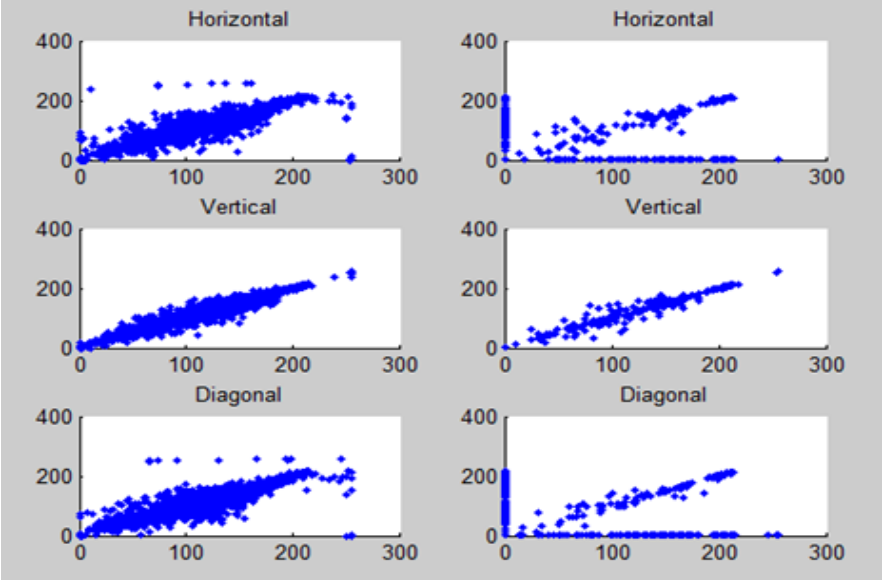
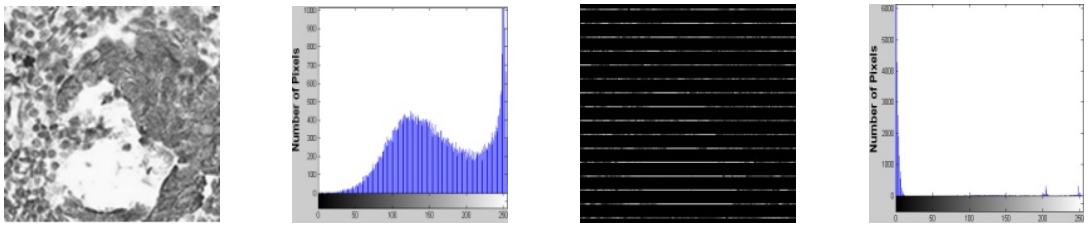


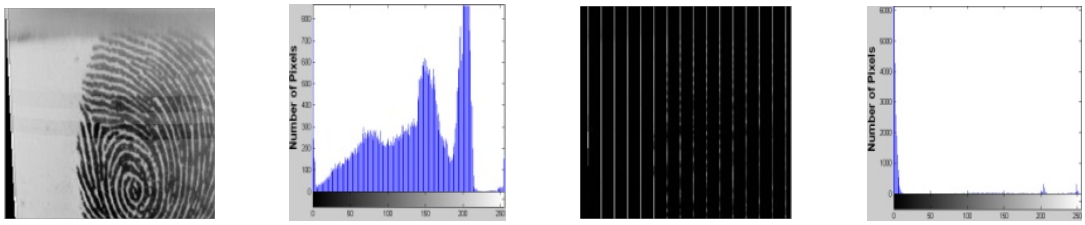
Fig. 5. Comparison of secret image and shares

The gray-level distributions are calculated for both secret image and generated shares. Histogram technique shows the gray variations of these images in different orientations. Histogram demonstrates the strength of encryption process. Histogram comparison is depicted in **Fig. 6**, **Fig. 7**, **Fig. 8**.



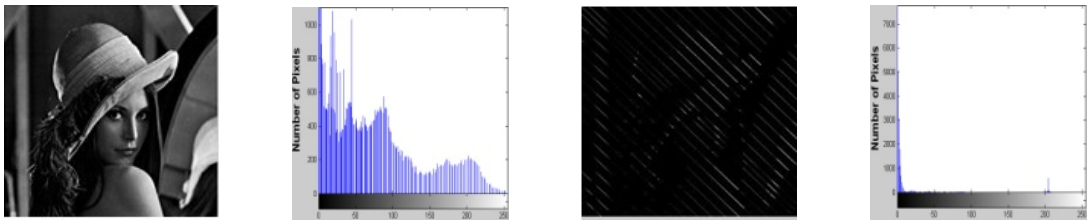
a) Tissue b) Histogram c) Share d) Histogram

Fig. 6. Histogram comparison of secret image and horizontal shares



a) fingerprint b) Histogram c) share d) Histogram

Fig. 7. Histogram comparison of secret image and vertical shares



a) Lena b) Histogram c) share d) Histogram

Fig. 8. Histogram comparison of secret image and diagonal Shares

Table 5. Comparison of performance and complexity analysis with exiting schemes

Schemes	Share Generation	No. of Secret Shares	Security	PSNR (dB)	Visual Quality	Computation	Storage
Shamir (1979)	Threshold based expansion	*n* shares	Low	N/A	Low	O (n $\log^2$ n)	O (n $\log^2$ n)
Shamir et al. (1994)	Pixel expansion	*n* shares	Low	N/A	Low	N/A	N/A
Tsai et al. (2004)	Threshold based	*n* shares	Low	39.21	Medium	O (n log^2 n)	O (n log^2 n)
Lou D et al. (2007)	Pixel expansion	3 shares	Moderate	29.2	Medium	O ($4n^2$ log^2 n)	O ($4n^2$ log^2 n)
Tsai et al. (2008)	Visual patterns	*n* shares	Moderate	26.49	Medium	O (n log^2 n)	O (n log^2 n)
Lin et al. (2012)	Non-pixel expansion	2*n* shares	Moderate	43.33	High	O (n log^2 n)	O (n log^2 n)
Hsu C et al. (2014)	Polynomial based	*n* shares	Moderate	NA	NA	O ($h.lgh + s.k$)	O ($h.lgh + s.k$)
Avci et al. (2016)	Probabilistic XOR	3 shares	High	51.67	High	O ($4n^2$ log^2 n)	O ($4n^2$ log^2 n)
Chao et al. (2017)	Progressive XOR	*n* shares	Moderate	33.0	Medium	O (n^2 $-2n+p)/n^2$	O (n^2 $-2n+p)/n^2$
Bhattacharjee et al. (2017)	Threshold based	8 shares	Moderate	32.5	Medium	O ($n.2^n{}_{C2}$ $.2^{2n}$)	O ($n.2^n{}_{C2}$ $.2^{2n}$)
Hao et al. (2018)	Random Grid based	n shares	Moderate	24.65	Medium	O (n log^2 n)	O (n log^2 n)
Proposed	Non-pixel expansion	8*n* shares	High	68.27	High	O (n)	O (log n)

Table 5 compares the features of proposed scheme with number of existing secret sharing schemes. As listed in **Table 5**, the pixel expansion based schemes are restored low quality secret image with moderate security level. The PSNR value of pixel expansion method was 26.49 *db*. Furthermore, compared with Lin et al. 2012, Avci et al. 2016, Chao et al. 2017, Bhattacharjee et al. 2017, Hao et al. 2018, the proposed scheme reveals the secret image with high visual quality. The computational complexity of schemes using pixel expansion and polynomial based sharing schemes is order of O (n log^2 n) and O ($h.lgh$ + $s.k$), while computational complexity of proposed scheme is O (n).

According to the above analysis, merits of the proposed scheme are described as follows:

- The proposed scheme split the secret image into 8n shadow images in different orientations with scheme selection.
- The novelty of the proposed scheme lies in scheme selection and bound level based on the mathematical expression $\left(\left\{S,\left(2\text{^}3\right)\times i\right\}^{HVD},n,S^*\right)$
- Meaningful shadow images are constructed in different orientation.
- The size of the shadow images is downsized.
- The proposed schemes can lossless recover the secret image with high visual quality.
- The computational complexity of proposed scheme is of order $O(n)$, so that this scheme is implemented with low computational complexity.
- This intelligent scheme requires less storage space other than previous methods.

5. Conclusion

It is implicit that the foremost requirement of information hiding is robustness and imperceptibility and therefore this system has been formulated by considering these rudiments. In this paper, a new eminent and lossless image steganography approach is proposed based on Contours and Clustering. Our investigational outcomes have revealed that the proposed method provides an improved means to conceal data without producing perceptible distortions and thus enhances the stego-image quality (i.e. the PSNR value). The proposed embedding strategy has been assessed and compared with a few popular on hand approaches with respect to stego-image quality. It is very heartening to find that the suggested approach always performs better than the compared standard approaches. We conclude that our scheme is straightforward and realistic for steganography applications. Even though our approach has produced good results, some betterment is possible. Our future work will concentrate on ameliorating the effectiveness of the proposed technique particularly, by utilizing color images. Thus, on the whole, this system is one that satisfies all requisites meticulously and does the intended function for which it has been designed.

References

[1] J. Anbarasi and A. Mala, "Verifiable Multi Secret Sharing Scheme for 3D Models," *The International Arab Journal of Information Technology*, vol. 12, no. 6A, pp. 708-713, August, 2015. Article (CrossRef Link)

[2] C. Blundo, A. De Santis, and M. Naor, "Visual Cryptography for grey level Images," *Information Processing Letters*, vol. 75, no. 6, pp. 255-259, October, 2000. Article (CrossRef Link)

[3] C. Chen, W. Chen, C-C. Chen, Y. Lai, and K. Tseng, "A Secure Visual Secret Checking of Meaningful Sharing Images," *Applied Mathematics & Information Sciences*, vol. 8, no. 5, pp. 2327-2335, September, 2014. Article (CrossRef Link)
[4] Y. Han, Y. Hu, and W. He, "A Digital Signature-Based Visual Cryptography Scheme for Image Discrimination and Management," *Journal of Electronics (China)*, vol. 26, no. 5, pp. 631-636, December, 2009. Article (CrossRef Link)
[5] J. Hemanth and S. Uma Maheswari, "Performances enhanced image steganography systems using transforms and optimization techniques," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 415-436, November, 2017. Article (CrossRef Link)
[6] C. Hsu and S. Tu, "Protecting secret documents via a sharing and hiding scheme," *Information Sciences*, vol. 279, pp.52-59, March, 2014. Article (CrossRef Link)
[7] W. Lee, I. Kim, and C. Kwon, "New Watermarking Technique Using Data Matrix and Encryption Keys," *Journal of Electrical Engineering & Technology*, vol. 7, no. 4, pp. 646-651, July, 2012. Article (CrossRef Link)
[8] P. Li, C. Yang, Q. Kong, Y. Ma and Z. Liu, "Sharing more information in gray visual cryptography scheme," *Journal of Visual Communication and Image Representation*, vol. 24, no. 8, pp. 1380-1393, November, 2013. Article (CrossRef Link)
[9] D. Lou, H.-L. Tso and J. Liu, "A copyright protection scheme for digital images using visual cryptography technique," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 125-131, January, 2007. Article (CrossRef Link)
[10] M. Naor and A. Shamir, "Visual Cryptography," in *Proc. of International Conference on the Theory and Application of Cryptographic Techniques Perugia, Italy*, pp. 1-12, May, 1994. Article (CrossRef Link)
[11] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, November, 1979. Article (CrossRef Link)
[12] D. Taghaddos and A. Latif, "Visual cryptography for gray-scale images using bit-level," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no.1, pp. 90-97, January, 2014. Article (CrossRef Link)
[13] C.-S Tsai, J. Feng, H. Wu, Y. Chang and Y. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognition*, vol. 41, no. 12, pp. 3572- 3581, December, 2008. Article (CrossRef Link)
[14] D. Tsai, Y. Chen and G. Horng, "A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography," *Journal of Visual Communication and Image Representation*, vol. 23, no. 8, pp. 1225-1233, November, 2012. Article (CrossRef Link)
[15] W-H. Tsai and C-C. Lin, "Secret image sharing with steganography and authentication," *The Journals of Systems and Software*, vol. 73, no. 3, pp. 405-414, December, 2004. Article (CrossRef Link)
[16] S. Tu, and C. Hsu, "A Joint Ownership Protection Scheme for Digital Images Based on Visual Cryptography," *The International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 276-283, May, 2012. Article (CrossRef Link)
[17] S. Wang, X. Yan, A. El-Latif and X. Niu, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," *Multimedia Tools and Applications*, vol.74, no. 9, pp. 3231-3252, May, 2015. Article (CrossRef Link)
[18] H. Hao, S. Gang, F. Zhengxin and Y. Bin, "Improved Contrast for Threshold Random-grid-based Visual Cryptography," *KSII Transactions on Internet and Information Systems*, vol.12, no. 7, pp. 3401-3420, July, 2018. Article (CrossRef Link)
[19] L. Long, W. Wei, L. Xianli, P. Yafeng and S. Houbing, "Visual Attention Model Based on Particle Filter," *KSII Transactions on Internet and Information Systems*, vol.10, no. 8, pp. 3791-3805, August, 2016. Article (CrossRef Link)
[20] P-C. Huang, Y-H. Li, C-C. Chang and L. Yanjun, "Efficient Scheme for Secret Hiding in QR Code by Improving Exploiting Modification Direction," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 5, pp. 2348-2365, May, 2018. Article (CrossRef Link)

[21] E. Avci, T. Tuncer and D. Avci, "A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain," *Arabian Journal of Science and Engineering*, vol. 41, no. 8, pp. 3153-3161, April, 2016. Article (CrossRef Link)
[22] H-C. Chao and T-Y. Fan, "XOR-based progressive visual secret sharing using generalized random grids," *Displays*, vol. 49, pp. 6-15, September, 2017. Article (CrossRef Link)
[23] T. Bhattacharjee, R. K. Rout and S. P. Maity, "Affine Boolean Classification in Secret Image Sharing for progressive quality access control," *Journal of Information Security and Applications*, vol. 33, pp. 16-29, April, 2017. Article (CrossRef Link)

N. Rajesh Kumar received Master degree in Computer Applications from Alagappa University, Karaikudi in 2009. He is an Assistant Professor in the Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam from June 2010 to now. And he now is research scholar at SASTRA Deemed to be University, Thanjavur. His research interests include information hiding, image processing and cryptography. He has published over 18 research papers in journals and conferences of repute.

R. Bala Krishnan is working as an Assistant Professor in SASTRA Deemed to be University in School of Computing and has teaching experience for about 7 years. He obtained his M.Tech. at SASTRA Deemed to be University. He has published more than 25 technical articles in international journals. His area of interest is Network Intrusion Detection and Prevention, Cryptography and Steganography.

G. Manikandan is a Faculty Member in the School of Computing, SASTRA Deemed University, Tamil Nadu, India. He received his Master degree in Computer Science from SASTRA, Tamil Nadu, India. He has published more than 45 technical articles in international journals. His Research interest includes Steganography, Data Mining and Cryptography.

N. R. Raajan now working as Senior Assistant Professor in SASTRA University in department of ECE and has teaching experience for about 10 years. He obtained his Ph.D. at SASTRA University. He has published more than 200 papers in national and international journals. His area of specialization is Augmented Reality, Hydrophone communication (under water acoustics), Image & Video processing, Signal processing, Wireless communication.