ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 3, March 2017

Multiple Secret Sharing in Visual Cryptography with Perfect Reconstruction

[1]R. Sathishkumar, [2]Gnanou Florence Sudha
[1]Perunthalaivar Kamarajar Institute of Engineering & Technology,[2]Pondicherry Engineering College

***Abstract:* -- Visual Cryptography Scheme (VCS) is an image based secret sharing technique which encrypts the secret image into binary shares. These binary shares are then overlapped to decrypt the secret image, but with a reduction in the image quality. In Extended Visual Cryptography Scheme (EVCS), shares are embedded with different cover images to generate meaningful shares. Two in One Image Secret Sharing Scheme (TiOISSS) was implemented to improve the decoded image quality, which perfectly retrieve of the secret image. In this proposed scheme, the TiOISSS implemented to share multiple secret images with perfect reconstruction made possible. Adaptive Halftoning was implemented to improve the image quality. Additionally, a textual message is also embedded in GVCS shares to protect the secret images from the intruders. The quality and the security of the reconstructed secret images are enhanced, in the proposed scheme.**

***Index Terms*——Adaptive Halftone, Multiple Secret Sharing, Polynomial Image Secret Sharing,Visual Cryptography Scheme.**

I. INTRODUCTION

Digital communication has become essential in the present scenario. Every day, a huge amount of data is being transmitted over the internet. These data are vulnerable to attacks from the hackers. Hence, the security of the data transmitted must be ensured such that only the valid receiver must be able to access it. Most of the encryption techniques requires huge processing both at the transmitter and at the receiver end. In general, the data will be encrypted by a security key and the receiver needs to use the same key to retrieve the data.

VCS is an image based encryptionscheme proposed by Naor and Shamir [1-2] to hide text based secret image in the form of *n* noisy imagestermed as shares, such that the secret imageis retrieved by Human Visual System (HVS) by stacking *n* shares. The traditional VCS is relaxed for threshold VCS in which any *k*or more number of shares are sufficient to decode the secret image [3-4]. The VCS wasimplemented to secure the gray images by suitably converting it to binary images [5-7]. These schemes were proposed with noisy shares, that may invite intruders' attention. By suppressing this weakness, VCS were implemented with meaningful shares from the cover images, and is referred as Extended Visual Cryptography Scheme (EVCS) [8-10].

In [11], Wu et al. proposed a VCS to share two secret images in two square shares. By stacking two square shares, the 1st secret image was decoded, and the 2ndsecret image could be decoded by stacking the share 1 and the share 2 with a 90^{o} rotation angle.In [12], Wu et al. developed a multiple secret sharing scheme to secure two secret images in two circle shares. The rotation angle of shares, in this scheme, was a factor of 360^{o}, and not limited to 90^{o}, 180^{o}, and 270^{o} as in [11].In [13], Shyu et al. proposed to share multiple images in two circular shares. Each secret images could be revealed one by one by stacking the first circular with the rotated second share with different rotation angles. In[14], Feng et al. implemented a (2,2)-x-VSSM scheme to share multiple images by using two cylindrical shares such that the secret images could be decoded from two cylindrical shares by stacking with an aliquot angle.In [15], Chien et al.proposed a different type of secret sharing scheme, in which the secrets are reconstructed stage-by-stage in predetermined order. The scheme allows parallel secret reconstruction and the user can dynamically determine the number of distributed secrets.

Polynomial image secret sharing (PISS) was implemented with perfect retrieval of the secret image [16]. In [17], Sian et al. implemented Two in One Image Secret Sharing Scheme (TiOISSS) wherein the vague secret image is decoded by HVS in the 1st decoding stage and the better quality secret image is decoded using computations. In [18], Peng et al.modified the TiOISSS using Gray-VCS shares. The scheme was implemented for sharing a single secret image and GVCS sharesimproves the visual quality. In [19], Srividhya et al. improved the TiOISSS image quality by applying adaptive halftoning. The dynamic threshold in the adaptive halftoning results in better contrast of the decoded image. In [20], TiOISSS with meaningful shares was proposed to secure a single secret image, but the secret image was not perfectly decoded. The existing model of TiOISSS are implemented for securing only one image and the decoding was done by direct stacking of shares.

In this proposed scheme, existing TiOISSS [20] is implemented forsharing multiple secret images. Further, in addition to applying PISS algorithm, the secret imagesareencrypted by permuting its pixels at the bit level, block level and pixel level to improve security. Thenoisy shares are generated for the secret images. Additionally, a textual secret message isencoded into the shares forvalidating the genuineness of the decoded image.

Experimental results of the proposed scheme show that the weaknesses of the existing TiOISSS schemes are attempted that the multiple secret images were perfectly reconstructed with the enhanced quality and improved security.

This paper is organized as follows. The VCS, halftoning technique, TiOISSS are detailed in section II. The proposed Multiple secret sharing in VCS is discussed in section III. The results are discussed in section IV. The Quality analysis and Security analysis are discussed in section V and section VI. The conclusion is presented in section VII.

II. RELATED WORKS

The proposed work is to share multiple secret images in TiOISSS, with better quality and perfectdecoding. The related works pertaining to the existing scheme is discussed in this section.

A. *Visual Cryptography Scheme*

Moni Noar and Adi Shamir implemented the visual secret sharing scheme in 1994 [1]. This VCS uses mathematical computations in the encoding stage only. The decoding of secret image is done by the human visual system (HVS).

In the threshold visual secret sharing scheme, *n*numbers of noise like shares are generated, out of which any *k* or more number of shares are used to decode the secret image. With shares fewer than *(k-1)*, the encoded secret image cannot be revealed.

In conventional VCS, the secret image pixel is expanded into 2x2 sub-pixel group to generatetwo noisy shares, based on the coding table shown in Fig. 1. For every white pixelof the secret image, any one of the six sub-pixels are randomly selected for both shares. Similarly, for every black pixel of the secret image, any one out of the six sub-pixels are randomly selected for share 1, and its compliment sub-pixels for the share 2. Now, when overlapping two noisy shares, the white pixels are reconstructed with 50% contrast. Further, the black pixels are reconstructed as such, but with pixel expansion. Every shares havean equal number of bothblack and white pixels in each sub-pixel groups, hence information about the secret image is always hidden. The share size and therefore the reconstructed image are doubled due to pixel expansion.

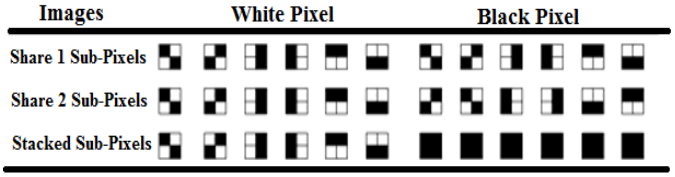
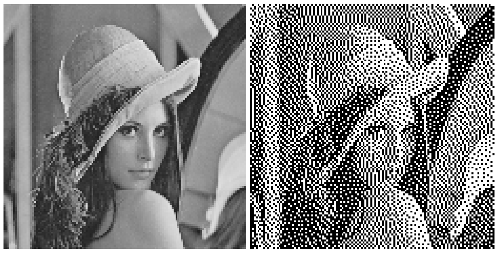


Fig. 1Coding table

B. *Adaptive Halftoning*

Halftoning technique is a process of converting the continuous tone image to the monochrome image or the binary image. The conventional VCS is based onbinary images. In order to use the grayscale image in VCS, it has to be converted to the binary image. Halftoning techniques like ordered dithering, Error diffusion are used to convert the grayscale image to the binary image. Many techniques like AM halftoning, FM halftoning, etc. are also available for converting the gray scale image to the binary image. In [16-18], Error diffusion based on FM halftoning with is implemented. But, this results in scattered white pixels in the place of darker areas of the gray image. The proposed work utilizes the Adaptive Halftoning [19] where in the dynamically determined threshold for halftoning, results in better contrast for both constantly varying images and sharp transition images. The human eye perceives the tiny dots as white and denser dots as black, in the halftoned image. A gray scale image and its halftoned image is shown in Fig. 2.



a) b)

Fia. 2 a) Continous tone b) Halftone

C. Polynomial Image Secret Sharing Scheme (PISSS)

The PISS scheme was first implemented [16] to hide the secret image. Though, it contradicts the advantage of VCS, by involving mathematical calculations in both encrypting and decrypting stages, it offers perfect retrieval of the secret image pixels.The PISS is implemented for TiOISSS with perfect reconstruction [20].

The polynomial in equation 1, encodes the image pixels to cipher data, which is then embedded in GVCS shares.

$$\boldsymbol{F(x)} = \left(\boldsymbol{a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}}\right) \boldsymbol{modulus\ P} \qquad (1)$$

in which$\boldsymbol{a_0, a_1, \ldots\ldots a_{k-1}}$ are the sequential *k* pixels of the image and *P* is the prime number.

In the decoding phase, the Lagrange interpolation formula in the equation (2) is used to derive the polynomial coefficients,

$$\boldsymbol{l_i} \equiv \prod_{\substack{1 \le j \le k \\ i \ne j}} \frac{\boldsymbol{x - x_j}}{\boldsymbol{x_i - x_j}} \qquad (2)$$

Bysubstituting the pixel position for$\boldsymbol{x_j}$(where, $\boldsymbol{j = 1, 2, \ldots, k}$), keeping $\boldsymbol{x}$as the variable, the polynomial coefficients$\boldsymbol{l_i}$ is derived,Further, the decoding polynomial equation can be derived by from the polynomial coefficient$\boldsymbol{l_i}$and the encoded image pixels $\boldsymbol{s_i}$ in the equation (3).

$$\boldsymbol{f(x)} = \sum_{i=1}^{k} (\boldsymbol{s_i} \times \boldsymbol{l_i})\ \boldsymbol{modulus\ P} \qquad (3)$$

The original secret pixel value can be retrievedfrom the equation (3), by substituting the image pixel position $\boldsymbol{x}$,. A large prime number of 251, which is within gray pixel range, can be considered for encrypting the grayscale image.

D. TiOISSS

Two in One Image Secret Sharing Scheme (TiOISSS)[18] combines the merits of both the PISS to achieve perfect reconstruction & VCS to decode the vague secret image by HVS. Hence, it involves two levels of encoding and decoding phases.

The encoding phase starts with generating *n* VCS shares and *n* PISS shares from the same secret image, followed by replacing the black pixels of VCS shares by the gray-valued pixels of PISS shares to generate GVCS shares, which are transmitted through n users. In the decoding phase, GVCS shares from the users are overlapped to reconstruct the vague secret image, in the 1st stage level with just HVS. This process does not require any mathematical computations. Further, Inverse PISS is applied to the gray pixels of GVCS shares to perfectly retrieve the secret image, in the 2nd stage level of decoding.

III. PROPOSED SCHEME

The existing TiOISSShides only one secret image. In [19], an extra authentication image was shared in addition to the secret image. Thus, limiting the number of images to be shared.In the proposed scheme, the existing TiOISSS is modified for sharing multiple secret images. The main secret image along with three extra secret images are shared in two GVCS shares.

The vague secret images can be decoded, in the first decoding phase, from the proper stacking of GVCS shares. Additionally, to provide the authenticity, a 2^{16} bits of textual message can be embedded in the two LSBs of white pixels of all GVCS shares, which are then decoded in the 2nddecoding phase.The multiple secret images are then retrieved by applying Inverse PISS. The stages involved in the proposed scheme are discussed in the following sections.

A. VCS Share generation

VCS shares are generated from the Main Secret image and the other three secret images. All the grayscale secret images are halftoned by using the adaptive halftoning technique discussed in section II-B, results in binary secret images. The VCS share generation process is illustrated in the block diagram shown in Fig. 3.

By considering the secret image 1, the 2^{nd} quadrant of the share 1 (S1_Q2) and the 90^{o} angular shifted version of the 1^{st} quadrant of the share 2 (S2_Q1_90) are generated using conventional VCS. This is to decode the secret image 1 in the 2^{nd} quadrant, when the share 1 and the 90^{o} angular shifted version of share 2 is stacked.

Now, from the secret image 2 (S2) and S2_Q1_180, the 4th quadrant of the share 1 (S1_Q4) is generated by VCS. Further, the 3rd quadrant of share 1 (S1_Q3) is generated from the secret image 3 and the 270° angular shifted version of the 1st quadrant of the share 2 (S2_Q1_270).

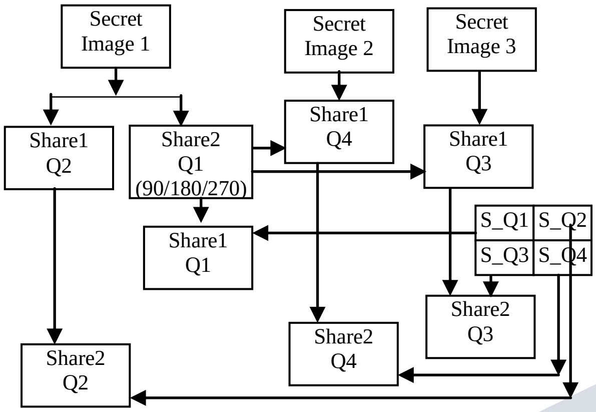


Fig. 3 Generation of VCS shares

The main secret image is divided into 4 quadrants (S_Q1, S_Q2, S_Q3 & S_Q4). By processing S1_Q2 and S_Q2, the 2nd quadrat of share 2 (S2_Q2) is generated. Further, S2_Q3 is generated from S1_Q3 and S_Q3. Similarly, S2_Q4 is generated from S1_Q4 and S_Q4. The remaining quadrant S1_Q1 is generated from S2_Q1 and S_Q1.

Finally, all the quadrants of the share 1 and share 2 are merged correspondingly, to frame the VCS share 1 and VCS share 2.

B. GVCS Share generation

All the secret images pixels are processed by PISS algorithm as discussed in section II-C, to generate two PISS shares. The PISS shares carries the encrypted version of all the secret images. To further improve the security of the proposed scheme, the pixels of both PISS shares are permuted in three levels namely,bit level, block level and pixel level.The 128-bit encryption key is shown as formatted in Fig. 4.

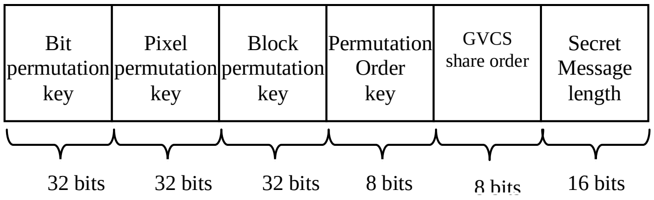


Fig.4 Encryption key format

The bit level, block level and pixel level permutations are performed with the respective 32-bit keys. The permutation order key defines the order of permutation performed which is required in reverse permutation operation for the proper reconstruction of PISS shares. The GVCS share order defines the share order to be processed to retrieve the embedded key from the GVCS shares. The size of the textual secret message embedded in the GVCS shares is defined in the 16-bit Secret Message length.

In order to generate the GVCS shares, the PISS shares pixels are embedded in each black pixel are VCS shares. Prior to embedding these PISS values, it is truncated by a factor α, (α = 1, 2, … 16). This truncated value along with its remainder will be darker near to black, providing better visual quality. The textual secret message will be embedded into the two LSBs of each white pixel of the VCS shares. Thus, the resultant shares will contain gray pixels from truncated PISS values and thus termed as GVCS shares. The generation of the GVCS shares is illustrated in the block diagram shown in the Fig.5.

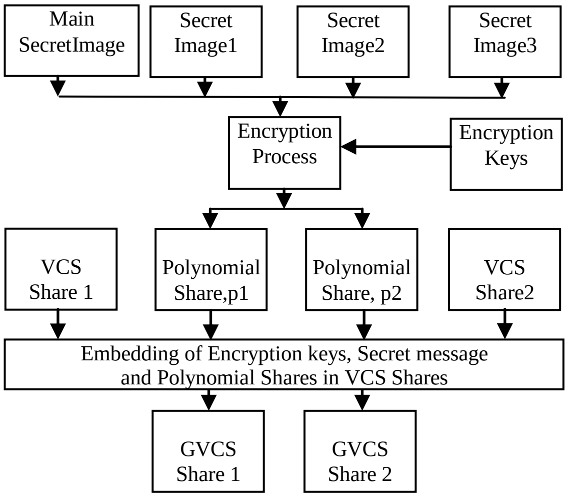


Fig. 5. Generation of GVCS shares

C. *Decryption of the Secret image*

The decryption of the secret images is done in two phases. In the 1st phase, the two GVCS shares are overlapped to decode the main secret image. By overlapping the GVCS share 1 and the 90° angular shifted version of GVCS share 2, the secret image 1 will be visually decrypted in 2nd quadrant. By overlapping the GVCS share 1 and the 180° angular shifted version of GVCS share 2, the secret image 2 will be visually decrypted in the 4th quadrant. Similarly, by overlapping the GVCS share 1 and the 270° angular shifted version of the GVCS share 2, the secret image 3 will be visually decrypted in the 3rd quadrant.

In the 2nd phase of decoding, the encryption keys and the secret messages are extracted from the white pixels of each GVCS shares. PISS values are extracted from the black pixels of GVCS shares. Inverse PISS algorithm and the reverse permutation are applied to PISS shares with the extracted 128-bit encryption key to reconstruct the main secret image and all the three secret images, perfectly. The decoding process is illustrated in the block diagram shown in Fig.6.

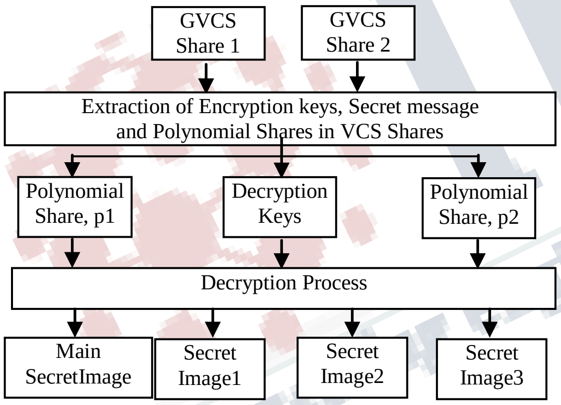


Fig. 6 Extraction of PISS Shares and Secret Images

IV. EXPERIMENTAL RESULTS

The experimental result of the proposed scheme is discussed in this section. The scheme is implementsadaptive halftone technique and with PISS reduction factor, α = 7.

The 512x512 sized Mainsecret image and the three numbers of 256x256 sized additional secret images are considered as shown in Fig. 7(a) to7(d).

The halftoned secret images are shown in Fig. 7 (e) to 7 (h).

The PISS shares are generated from the secret images and are shown in Fig. 7 (i) & 7 (j). Further, from the secret images, by applying VCS with pixel expansion, m = 4, two VCS shares of 1024x1024 are generated. The GVCS shares generated from VCS shares by embedding PISS values as detailed in section III-B are shown in Fig. 7 (k) & 7 (l).

In the decoding phase, the two GVCS shares are stacked to decode the vague main secret image as shown in Fig. (m). The secret image 1 decoded from the stacked version of the GVCS share 1 with 90° rotated GVCS share 2 is shown in Fig. 7 (n). Similarly, the remaining secret images decoded in the 1st phase are shown in Fig. 7 (o) & 7 (p).
In the 2nd decoding phase, by applying Inverse PISS and reverse permutation over the extracted grayscale pixels of the GVCS shares, the perfect reconstruction of the Main secret image and the other secret images are decoded and is shown in Fig. 7 (q) & 7 (t).

V. QUALITYANALYSIS

The parameters like Contrast, Structural Similarity Index Measure (SSIM) & Peak Signal to Noise Ratio (PSNR) of the proposed scheme are analysed.

A. *Contrast*

Contrast which represents the visual quality of the image, is given by the normalized difference between the mean grayness of the white secret pixels and the mean grayness of black secret pixels in the decoded image. In this scheme, contrast [20] is calculated among the group of decoded pixels valued more than the threshold, (C_0) and the group of decoded pixels valued lesser than the threshold, (C_1) and is given by,

$$\alpha = \frac{C_0 - C_1}{255} \quad (4)$$

Contrast between the secret images and its 1st phase decoded secret images for adaptive halftoning has been tabled in the Table I for the different truncation factor, α = 7. The contrast has been improved for adaptive halftoning, for all the decoded secret images.

B. *SSIM*

It is a measure of resemblance between two images and it is calculated for two common sized ($N\times N$) windows x and yof the two images. SSIM is given by

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (5)$$

where
▯$_y$ and ▯$_x$ are the average of y and x.
σ_x^2 and σ_y^2 are the variance of x and y, σ_{xy} is the covariance of x and y
$c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are two variables to stabilize the division, L is the dynamic range of the pixel values and $k_1 = 0.01$ and $k_2 = 0.03$ by default.
The SSIM between the secret images and its 1stphase decoded secret images for the adaptive halftoning technique has been tabled in the Table I for various truncation factor, α = 7. The SSIM is improved resulting in increased similarity between the secret image and the decoded secret image.

C. PSNR

The Peak Signal to Noise Ratio (PSNR) is a measure to estimate the image quality between two images. Based on the pixel difference between the reconstructed image and the original image, PSNR is defined as

$$PSNR = 10\,log\,\frac{s^2}{MSE} \qquad (6)$$

where *MSE* denotes Mean Squared Error and *s* = 255, the maximum pixel value of the image.
The PSNR between the secret image and its 1stphase decoded secret image for the adaptive halftoning technique has been tabled in the Table I for various truncation factor, α = 7.The PSNR is higher for the adaptive halftoning technique.

Table I
Comparisonofsecret imagesv and 1stphase decodedsecret images (for α = 7)

Parameters	Original Secret image vs Decoded Secret image (1st phase)			
Secret Images	Main Secret Image	Secret Image 1	Secret Image 2	Secret Image 3
PSNR (dB)	7.1587	6.8655	6.2468	6.54605
Contrast	0.3211	0.2525	0.1933	0.2045
SSIM	0.4001	0.36402	0.4056	0.3709

Table II shows the comparison of GVCS shares with Main secret images. It shows that the GVCS shares are highly uncorrelated to the Main secret images, due to lower contrast value. Thus, the security of the proposed scheme is enhanced.

TABLE II
ContrastComparison for Main Secret image vs GVCSShares, for α = 7

Proposed Scheme	GVCS 1	GVCS 2
Contrast	0.00010	-0.000038

Table III shows the comparison of different halftoning techniques, which shows that the adaptive halftoning offers better visual quality.

TABLE III
Parameter Comparison between the Main Secret Image and 1st decoded Main Secret Image, for Different Halftoning, for α = 7

Halftoning Technique	AM Halftoning	FM Halftoning	Adaptive Halftoning	% Improvement FM vs Adaptive
PSNR (dB)	6.6704	6.6869	7.1587	7.06
Contrast	0.2018	0.1976	0.3211	62.5
SSIM	0.1715	0.3041	0.4001	31.57

VI. SECURITY ANALYSIS

The security aspects of the proposed schemeareanalysed based on the following aspects.

A. Encryption key size

The proposed scheme encrypts the secret images with 128-bit permutation key. Thus, the key space of $2^{128} = 3.4 \times 10^{38}$ is sufficient to defence all kinds of Brute Force attacks. Furthermore, the three stages of permutations viz. bit level, pixel level and block level is also implemented, to provide sufficient level of confusion.

B. Textual Authentication for additional security

The hackers may create any bogus share, from any one of the legitimate GVCS, due to which the genuine receiver may get thefake secret imagesas against the original secret images. To prevent this weakness, a secret textual message is embedded in the white pixels of GVCS shares. In the second decoding phase, the textual message can be retrieved from the GVCS shares and thereby the validity of the secret image is ensured.Thus, the security of the scheme is enhanced.

C. Histogram of GVCS Shares

The histogram pattern of the GVCS share 1 is shown in Fig. 8. The share pixels are valued up to 36 (i.e. $2^8/\alpha$) and at 255. The pixel values can be limited by choosing different values for the truncation factor, α.Though, the pixels of all the original secret images are distributed over the entire range, the pixels of GVCS shares are secured with limited distribution.Thus, the security of the proposed scheme is enhanced.

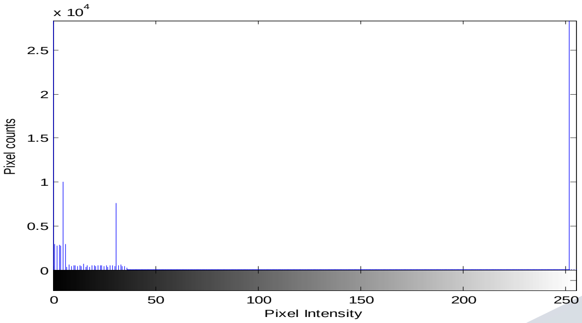


Fig 8. The Histogram pattern of GVCS shares1, (α =7)

D. Noise Attacks

To test the ability of the proposed scheme for noises, the GVCS shares were subjected to the different noise attacks before decoding the secret images.In the 1st phase decoding phase, secret images were retrieved with better quality. PSNR values are computed for each attack and are listed in Table IV.

TABLE IV
PARAMETER COMPARISON FOR DIFFERENT ATTACKS

Attacks	PSNR (dB)	Contrast	SSIM
Salt and Pepper	7.0796	0.3083	0.3607
Gaussian	7.5200	0.2830	0.3877
Speckle	7.5409	0.2974	0.3960
Sharpened	6.9007	0.3430	0.2695

VII. CONCLUSION

The proposed Multiple Secret Sharing in the Visual Cryptographyhides multiple secret image in the shares.The Polynomial Secret Sharing encrypts all the secret images in PISS shares, which are embedded into VCS shares to generate GVCS shares. The secret image is permuted in three stages viz. bit level, pixel level and block level, and PISS algorithm is implemented for perfect decoding of the secret image.Further, a textual secret message is embedded in GVCS shares to validate the authenticity of the decoded secret images. The contrast and the quality of thedecoded secret image is improved by using the Adaptive halftoning technique. The 128-bit Encryption key for the generation of GVCS shares improves the security of the scheme. SSIM, PSNR and Contrast parameters have been improved. In the 1st phase, the vague secret images have been decoded, and in 2nd phase, all the secret images are perfectly reconstructed.

REFERENCES

[1] M. Naor and A. Shamir, “Visual Cryptography”, Alfredo De Santis (Ed.), *Advances in Cryptology Proceedings of Eurocypto 94*, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1994.

[2] M. Naor, A. Shamir, in: M. Lomas (Ed.), VisualCryptography, II: “Improving the Contrast via the Cover Base”Presented at *Security in Communication Networks*, Amalfi,Italy, September 16–17, 1996.

[3] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, “Visualcryptography for general access structures”, *Inform. Comput*.129 (1996) 86–106.

[4] S. Arumugam, R. Lakshmanan and Atulya K. Nagar, “On (k,n) visual cryptography scheme”, *Journal of Designs, Codes and Cryptography*, vol. 71, no. 1, pp. 153-162, July 2014

[5] R.W. Floyd and L. Steinberg, “An adaptive algorithm for spatialgrayscale”, *Proc.SID*, 17/2:75–77, 1975

[6] C. Blundo, A. De Santis, M. Naor, “Visual cryptography for greylevel images”, *Inf. Process. Lett*. 75 (2000) 255–259.

[7] C.C. Lin, W.-H. Tsai, “Visual cryptography for grey-level images bydithering techniques”, *Pattern Recognition* Lett. 24 (2003) 349–358.

[8] Nakajima, M. and Yamaguchi, Y., “Extended visual cryptography fornatural images”, *Journal of WSCG*, v10 i2. 303-310.

[9] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, “Extendedcapabilities for visual cryptography”, *Theor. Comput. Sci. 250* (2001)143–161

[10] V. Rijmen, B. Preneel, “Efficient colour visual encryption forshared colors of Benetton”, *Eurocrypto’96*, Rump Session,Berlin, 1996.

[11] Wu, C.C. & Chen, L.H., “A study on visual cryptography”. *Master thesis. Institute of Computer and Information Science*, National Chaio Tung University, Taiwan, R.O.C., 1998.

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

[13] Shyu, S. J., Huang, S. Y., Lee, Y. K., Wang, R. Z., & Chen, K., “Sharing multiple secrets in visual cryptography”. *Pattern Recognition*, 40, 3633–3651, 2007.

[14] Feng, J. B., Wu, H. C., Tsai, C. S., Chang, Y. F., & Chu, Y. P., “Visual secret sharing for multiple secrets”. *Pattern Recognition*, 41, 3572–3581, 2008.

[15] H.Y. Chien, J.K. Jan, Y.M. Tseng, “A practical ðt; nÞ multi-secret sharing scheme”, *IEICE Transactions on Fundamentals E83-A* (12), 2762–2765, 2000.

[16] Chih-Ching Thien and Ja-Chen Lin, “Secret image sharing”, *Journal of Computers & Graphics*, vol. 26, no. 5, pp. 765-770, October 2002.

[17] Sian-Jheng Lin and Ja-Chen Lin, “VCPSS:A two-in-one two-decoding options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches”, *Journal of Pattern Recognition Letters*, vol. 40, no. 12, pp. 3652-3666, April 2007.

[18] Peng Lia, Pei-Jun Maa, Xiao-Hong Sua and Ching-Nung Yang, “Improvements of a two-in-one image secret sharing scheme based on gray mixing model”, *Journal of Visual Communication and Image Representation*, vol. 23, no. 3, pp. 441-453, January 2012.

[19] Srividhya Sridhar, R. Sathishkumar, Gnanou Florence Sudha, “Adaptive halftoned visual cryptography with improved quality and security”, *Journal of Multimedia Tools and Applications*, pp.1-20, November 2015.

[20] S.Srividhya, R. Sathishkumar, Gnanou Florence Sudha, “Implementation of TiOISSS with meaningful shadows and with an additional authentication Image”, *Journal of Visual Communication and Image Representation*, vol.38, pp.284-296, July 2016.