A New k out of n Secret Image Sharing Scheme in Visual Cryptography

K.Shankar
Ph.D - Research Scholar
Department of Computer Science and Engineering
Alagappa University, Karaikudi-630 003, Tamilnadu, India
shankarcrypto@gmail.com

Dr.P.Eswaran
Assistant Professor
Department of Computer Science and Engineering
Alagappa University, Karaikudi-630 003, Tamilnadu, India
eswaranperumal@gmail.com

***Abstract*—Visual cryptography (VC) is a method for shielding the secret image which encodes the image into many shares and allocates them to various participants. When all shares are aligned and stacked together, they expose the secret image. In k out of n (k, n) VC scheme, the secret image is shared into n shares such that when k or more participants by amassing their transparencies by means of an overhead projector to reveals the secret image. This paper proposed a brand new of simple and robust (k, n) visual cryptography technique which is used to effectively sharing the secret image with utmost confidentiality. In share creation process, specified new condition for random matrices and then XOR operations are performed to generate the 'n' transparencies. It is possible to decode the secret image visually by superimposing a k subset of transparencies. Nevertheless no secret data can be acquired from the superposition of an illegal subset. Experiments, statistical and security assessments are carried out on the shares to validate the strength of the proposed scheme by means of a sequence of investigations such as visual testing, encryption quality testing, security analysis and different attacks. The proposed (k, n) VC scheme offers a consistent protection for communicating images over the public channels.**

Keywords—Visual cryptography; (k, n) Visual cryptography scheme; Shares; XOR; attacks; Secret image sharing

I. INTRODUCTION

Initially Visual Cryptography was coined by Naor and Shamir, in which a secret image is encrypted into several shares by two matrices. A conventional (k, n) threshold Visual Cryptography encodes a secret image into n random-liked images in such a way that any k or more shares can visually decrypt the secret by stacking operation. XOR-based visual cryptography (VC) works for solving alignment problems and handling the images that possess low quality [1]. Another, secret sharing scheme is Visual Secret Sharing(VSS), based on the (k-n) threshold concept. This method, works out of n share with any k or more reconstructed shares, to retrieve the original image by superimposing the shares eliminates complex computations [2]. The (k, n) Threshold Visual Cryptography Scheme is found in literature, in which the size of generated shares as well as recovered image have same as the secret image differs it from other visual cryptography schemes where k is the threshold value [3]. There are many applications of VC that includes copyright protection, general access structure; watermarking and visual authentication etc. is in use. In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into shared images of its random binary patterns. In this technique, the shared images such as printed text, pictures, and the like are perceptible by k or more participants by gathering their transparencies by means of an overhead projector [4]. The VC, also known as the VSS, represents a confidential sharing model for images in which the decryption is carried out by superimposing the stacked shares through the human visual mechanism [5]. 2 out – of –2 visual cryptography scheme generates, 2 share pictures on the basis of an original image from shares present at the user end, need to superimpose on the generated shares to get back the original image [6]. In the case of augmenting the quality of the restored image, VCS-XOR frequently offers several merits on pixel development and contrast qualities when compared to the VCS-OR. It is crystal clear that the deciphering techniques have emerged as more intricate and challenging during the course of deciphering a large number of shares and in this connection, the XOR based VCS has established itself as the most realistic in respect of the (2; n) case [7]. The solution of the innovative technique for keeping dishonesty at bay is the acceptance of several secret images in such a way that each qualified subsets will expose the relative secret image only, leaving the other secret images unfamiliar to the prospective hawkers. [8]. In this paper, a new k out of n secret image sharing scheme is proposed. The proposed (k, n) visual cryptography method, split the image into n shares and distributed to the users. When all k or n shares are overlay, then only the secret image appear to the users.

II. RELATED WORKS

In 2014, Hao Luo et al [9] examined an innovative color transfer technique which could be blended into the (k, n) VC model. The author projected a color transfer scheme which can be incorporated into the (k, n) visual cryptography model. The concept is intended towards to building up a color image secret sharing for output devices like the fax machines or monochrome printers. When stacking a qualified set of shadows, the grey level version of secret content could be exposed by the human visual mechanism. However, the suggested model tends to be devious-resistant. The author describes their paper is very efficiency for that reason of their test outcomes and the linked examples.

In 2013, Pandey et al. [10] have capably advanced the visual cryptography schemes by method for compressed random shares. In the strategy, the visual cryptography plan had the accompanying n number of linear shares with consolidated measurement and backings differences of image outlines despite offering an incorporated methodology for binary, gray and shade image visual cryptography by defending the visual immensity and pixel development.

In 2013, Anupam Bhakta et al [11] discussed a innovative method which is done the encryption in several levels. In first level they use a variable length image key to encrypt the original image then bit sieve procedure is used on resultant image and finally k-n secret sharing scheme on the final encrypted image was performed. The author's take specific 'k' numbers of shares among 'n' number of shares thus provide a more secured system. The experimental results proceeds the superior computation speed compared between existing methods. The author justified their paper has multiple levels of encryptions, so the security is being increased in improved manner.

In 2013, Ching-Nung Yang et al. [12] have proposed an easy solution to construct visual cryptography scheme by image filtering and resizing. The author incorporated to design a mapping pattern that reduces the number of dummy sub pixels to minimum is a huge challenge, especially for some pixel expansions and secret image sizes. They try to keep the aspect ratio of a reconstructed image. In this paper the author proposed two ARIVCSs were arrange the sub pixels in VC. Besides, they also need a mapping pattern that reduces the number of dummy sub pixels to minimum for some pixel expansions and secret image sizes. The illustrated result shows another view to construct the ARIVCS by resizing the secret image to keep the aspect ratio invariant.

III. PROPOSED METHODLOGY

In enlarged size of the internet communication, visual cryptography is used to sharing a secret image with utmost confidentiality over unsecured public channels. The whole proposed scheme described is simply states as the block diagram is shown in Figure 1.

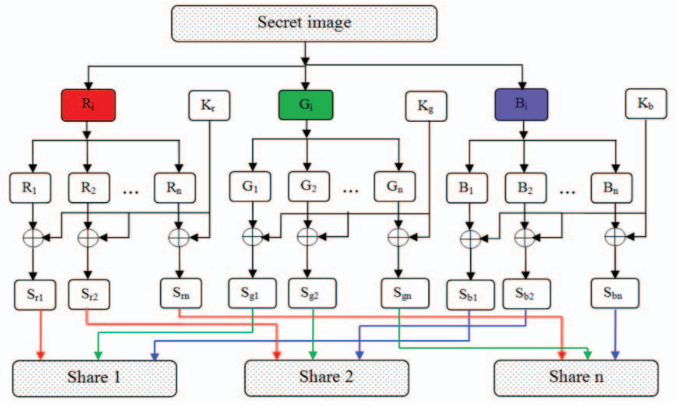

Fig. 1. Block diagram of proposed scheme

The proposed (k, n) visual cryptography scheme in which the secret image perceptible by k or more participants by amassing their transparencies by means of an overhead projector. The secret image is converted into three different grayscale images based on its color components (R_i, G_i, B_i). Generate distinct random matrices (based on R_i, G_i, B_i values) and these matrices are utilized to create the number of shares (share1, share2…share n). The size of the secret image and matrices are identical. In share creation process, specified new condition for random matrices and then XOR operations are performed. Finally visual testing, encryption quality testing, security analysis and various attacks analysis are used to evaluating the performance of the proposed scheme.

A. Shares Creation Scheme

Step 1: The secret image represents $I_{h\times w}$. Here I indicates the pixels values of the secret image, where h=height, w=width.

Step 2: Extracting the pixel values of each color components from the secret image.

$$I_{h\times w} = \sum R_i + G_i + B_i$$

Step 3: Let consider $2 \leq k \leq n$, where n = number of shares, k = number of reconstructed shares.

Step 4: Generate n-1 distinct random matrices of size h×w for individual color components. Suppose dealer wants 4 shares then generate 3 distinct random matrices such as $T_{r1,}$ $T_{r2,}$ $T_{r3,}$ $T_{g1,}$ $T_{g2,}$ $T_{g3,}$ $T_{b1,}$ $T_{b2,}$ T_{b3} for the color components of R_i, G_i, B_i.

Step 5: The proposed (k, n) visual cryptography specified new condition for random matrices. Get the pixel value and then generate 3 random numbers which are lesser than the pixel value for individual color component.

$R_i < \{ T_{r1} , T_{r2} , T_{r3} \}$, $G_i < \{ T_{g1} , T_{g2} , T_{g3}\}$, $B_i < \{ T_{b1} , T_{b2} , T_{b3}\}$

Ex: If $R_{(1,1)} = 150$ for red component, then generate 3 random numbers such as 40,100,10.

Step 6: Arrange the step 5 resultant matrices in ascending order.

$$R_i < T_{r1} < T_{r2} < T_{r3}$$
$$G_i < T_{g1} < T_{g2} < T_{g3}$$
$$B_i < T_{b1} < T_{b2} < T_{b3}.$$

Ex: $0 < 10 < 40 < 100$

Step 7: Create four basic matrices for individual color components as $S_{r1,}$ $S_{r2,}$ $S_{r3,}$ $S_{r4.}$ $S_{g1,}$ $S_{g2,}$ $S_{g3,}$ $S_{g4,}$ $S_{b1,}$ $S_{b2,}$ $S_{b3,}$ $S_{b4.}$ under following conditions:

$$\begin{array}{lll} S_{r1} = T_{r1} & S_{g1} = T_{g1} & S_{b1} = T_{b1} \\ S_{r2} = T_{r2} - T_{r1} & S_{g2} = T_{g2} - T_{g1} & S_{b2} = T_{b2} - T_{b1} \\ S_{r3} = T_{r3} - T_{r2} & S_{g3} = T_{g3} - T_{g2} & S_{b3} = T_{b3} - T_{b2} \\ S_{r4} = R_i - T_{r3} & S_{g4} = G_i - T_{g3} & S_{b4} = B_i - T_{b3} \end{array}$$

Ex:
$$\begin{array}{l} S_{r1} = 10 \\ S_{r2} = 40 - 10 = 30 \\ S_{r3} = 100 - 40 = 60 \\ S_{r4} = 150 - 100 = 50 \end{array}$$

Step 8: Now generate K_r, K_g, K_b key matrices for individual color components.

Step 9: XOR operations are performed between basic matrices and key matrices.

Share 1_R = $S_{r1} \oplus K_r$	Share 1_G = $S_{g1} \oplus K_g$	Share 1_B =$S_{b1} \oplus K_b$
Share 2_R = $S_{r2} \oplus K_r$	Share 2_G = $S_{g2} \oplus K_g$	Share 2_B= $S_{b2} \oplus K_b$
Share 3_R = $S_{r3} \oplus K_r$	Share 3_G = $S_{g3} \oplus K_g$	Share 3_B= $S_{b3} \oplus K_b$
Share 4_R = $S_{r4} \oplus K_r$	Share 4_G =$S_{g4} \oplus K_g$	Share 4_B =$S_{b4} \oplus K_b$

Step 10: Finally all RGB color components are combined to create shares.

Share1= (Share 1_R, Share 1_G, Share 1_B)
Share2= (Share 2_R, Share 2_G, Share 2_B)
Share3= (Share 3_R, Share 3_G, Share 3_B)
Share4= (Share 4_R, Share 4_G, Share 4_B)

B. *Shares Reconstruction Scheme*

Step 1: Extracting the pixel values of the each and every share along with color components.

Step 2: XOR operations are performed between the shares and key matrices for individual color components to retrieve basic matrices

S_{r1} = Share 1_R $\oplus K_r$	S_{g1} = Share 1_G $\oplus K_g$	S_{b1} = Share 1_B $\oplus K_b$
S_{r2} = Share 2_R $\oplus K_r$	S_{g2} = Share 2_G $\oplus K_g$	S_{b2} = Share 2_B $\oplus K_b$
S_{r3} = Share 3_R $\oplus K_r$	S_{g3} = Share 3_G $\oplus K_g$	S_{b3} = Share 3_B $\oplus K_b$
S_{r4} = Share 4_R $\oplus K_r$	S_{g4} = Share 4_G $\oplus K_g$	S_{b4} = Share 4_B $\oplus K_b$

Step 3: Shares are reconstruct under the following condition.

Condition 1 : If n=4 then k=3 shares are reconstructed.

$$I_3 = S_{r1} + S_{r2} + S_{r3} \text{ (or) } S_{r1} + S_{r2} + S_{r4} \text{ (or)}$$
$$S_{r1} + S_{r3} + S_{r4} \text{ (or) } S_{r2} + S_{r3} + S_{r4}$$

Condition 2 : If n=4 then k=2 shares are reconstructed.

$$I_2 = S_{r1} + S_{r2} \text{ (or) } S_{r1} + S_{r3} \text{ (or) } S_{r1} + S_{r4} \text{ (or)}$$
$$S_{r2} + S_{r3} \text{ (or) } S_{r2} + S_{r4} \text{ (or) } S_{r3} + S_{r4}$$

These conditions are repeated for other two pixel values of the G and B color components.

Step 4: All basic matrices combined together to retrive the secret image color components individually,

$$S_r = S_{r1} + S_{r2} + S_{r3} + S_{r4}$$
$$S_g = S_{g1} + S_{g2} + S_{g3} + S_{g4}$$
$$S_b = S_{b1} + S_{b2} + S_{b3} + S_{b4}$$

Finally retrive the secret image($I_{h\times w}$),

$$I_{h \times w} = \sum S_r + S_g + S_b$$

IV. Experimental Results and Analysis

The proposed scheme is implemented in Visual Studio 2010, C# language under the configuration of windows 7 operating system with Core-i3 and 3 GB RAM. The proposed k out of n visual cryptography evaluating its performance in various images such as the Lena, Jet, Sailboat, and Barbara. The experiments are conducted on a database comprising of 50 test images. The images were obtained from USC-SIPI Image Database [13] The overall performance of the proposed method is analysed by using the Peak Signal to Noise Ratio (PSNR), Correlation Coefficient (CC), Mean Square Error (MSE), Number of Pixels Changing Rate (NPCR), Unified Average Changing Intensity (UACI) values and Entropy analysis. Different attacks are also used to evaluating the efficiency of the proposed method such as Salt - Pepper noise attack, Gaussian Noise attack, Poission Noise attack and speckle noise attack.

A. *Experimental Results*

A (2(k), 4(n)) secret sharing assessment and Different test images are selected to expose the performance of the proposed scheme. The experimental results of the original image, share images, and reconstructed shares of the Lena, Jet, Sailboat and Barbara images are represented in the Figure 2,3,4,5 respectively.

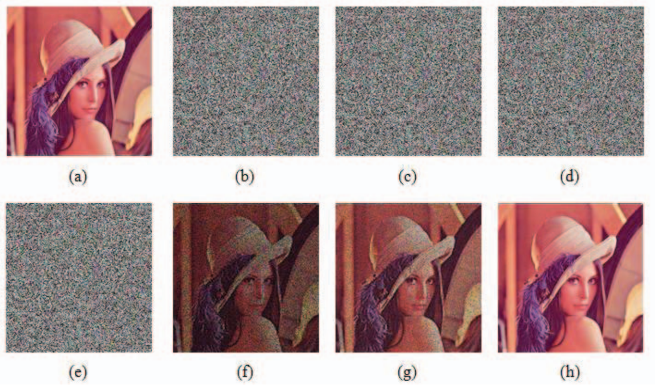

Fig. 2. Results of the Lena (a) Secret image (b, e) Shares (f, g) Images reconstructed from any 2 or more shares (h) Stacked Image;

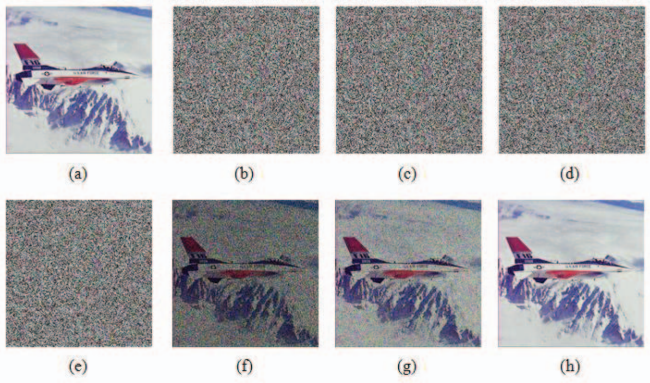

Fig. 3. Results of the Jet (a) Secret image (b, e) Shares (f, g) Images reconstructed from any 2 or more shares (h) Stacked Image;

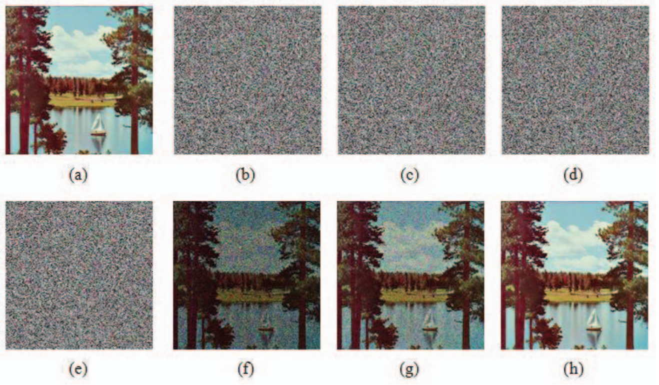

Fig. 4. Results of the Sailboat (a) Secret image (b, e) Shares (f, g) Images reconstructed from any 2 or more shares (h) Stacked Image;

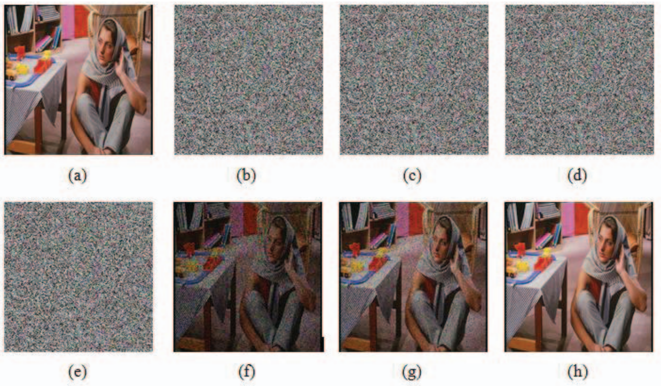

Fig. 5. Results of the Barbara (a) Secret image (b, e) Shares (f, g) Images reconstructed from any 2 or more shares (h) Stacked Image;

B. Performance Analysis

1) Visual Testing :

NPCR and UACI Analysis : NPCR is the change rate of the number of pixels in the share image. The unified average changing intensity (UACI) is the measurement of the average intensity of differences between the secret image and share images.

TABLE I. VALUES OF NPCR AND UACI TESTS OF SHARES

Image Name (Share 1)	NPCR (%)	UACI (%)
Lena	99.59	32.08
Jet	99.59	32.56
Sailboat	99.60	32.24
Barbara	99.62	33.46

The result of this experiments are evaluated by using sample images and their values are shown in Table 1. It shows that high NPCR values which represents the share image pixel indexes are completely changed compared to secret image. Table 1 shows that estimated expectations and variance of NPCR and UACI values are very close to the theoretical values which justify the validity of theoretical values. Hence, the proposed scheme is resistant against differential attacks [14]

2) Encryption Quality Testing :

Peak Signal to Noise Ratio (PSNR): The signal, here, represents the original data, and the noise relates to the flaw triggered by the compression. While analyzing and contrasting the compression codec's, the PSNR constitutes an approximation to human insight of modernization excellence. Even though a superior PSNR usually reveals the fact that the modernization is of superb quality, though there are exceptions to this trend. Therefore, it is highly essential to take utmost care regarding the extent of validity of this metric.

Mean Square Error (MSE): In statistics, the mean squared error (MSE) of an estimator evaluates the average of the squares of the "errors", in other words, the divergence between the estimator and the subject-matter of estimation. This tool represents a risk function, relating to the anticipated value of the squared error loss or quadratic loss.

In table 2, the proposed visual cryptography scheme with their PSNR values is employed for various sample test images. In general, the PSNR value of the original image and share image should be a low value, which yields better encryption quality. It is clear that the values between original image and any one share image (Share 1) , shares reconstructed from any 2 shares (I_2), shares reconstructed from any 3 shares (I_3) all are minimum 8.38 to maximum 17.46 which shows low PSNR value, it represents better encryption quality with high security of the secret image.

TABLE II. VALUES OF PSNR AND MSE TESTS OF SHARES

Image Name	PSNR			MSE		
	Share 1	*I_2*	*I_3*	*Share 1*	*I_2*	*I_3*
Lena	9.39	11.38	16.71	7.47	4.72	1.38
Jet	8.39	8.38	13.74	9.40	9.42	2.74
Sailboat	8.44	10.71	16.02	9.29	5.52	1.62
Barbara	9.04	12.15	17.46	8.09	3.95	1.16

3) Security Analysis :

The correlation coefficients and histogram estimations have made it crystal clear that the share creation scheme is performed on the secret image so as to preserve the confidentiality of the share image.

Histogram Analysis : The histogram image demonstrates the proposed shares creation scheme always generate a share images are different from that of the original image. The analyzed the histograms of the several share images as well as its secret images that have widely different content. Figure 6 shows that the histograms of share image is fairly similar and significantly unsimilar from the histogram of the original image.

Correlation Coefficient Analysis : Correlation is a measure of relationship involving a pair of variables. If two variables are the image and its encryption, then they are usually in great correlation and also the correlation coefficient equates to one, when they are remarkably reliant(identical). If the correlation coefficient equates to zero, then this original image and its encryption are usually different (good encryption), i.e. the particular encrypted image does not have any different characteristics and it's remarkably independent of the original image. The results of this experiment evaluated using different images and their values are shown in Table 3. It shows that the CC value is nearly zero, which means the original image information can be encrypted and its security maintained efficiently.

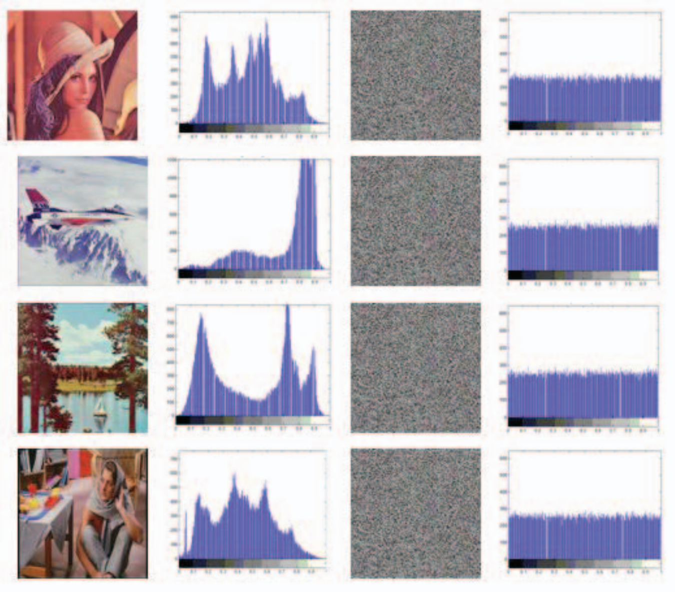

Fig. 6. Histogram Results of the different images such as the Lena, Jet, Sailboat, Barbara.

Entropy Analysis : Table 3 indicates the entropy values of the original and shares of the sample images(Lena, Jet, Sailboat and Barbara). The entropy values of the shares images are very close to the ideal value of 8 sh, which means that the shares are highly robust against entropy attacks[14].

TABLE III. VALUES OF ENTROPY AND CORRELATION COEFFICIENT TESTS

Image Name (Share 1)	Entropy		Correlation Coefficient
	Original Image	Share Image	
Lena	7.6554	7.9988	0.0012
Jet	6.7256	7.9989	0.0071
Sailboat	7.7751	7.9989	0.0050
Barbara	7.7719	7.9988	0.0026

4) Attacks :

The different types of attacks applied on the image for stealing the information of the image or blurring the image for reducing its quality of the image. The four different types of attacks applied on the images and they are Salt - Pepper Noise attack, Gaussian Noise attack, Poission Noise attack and Speckle Noise attack. These attacks are applied on the shares and the results are shown in table 4.

TABLE IV. PSNR AND MSE VALUES OF DIFFERENT ATTACKS AGAINST SHARES

Image Name (Share 1)	Salt and pepper Noise attack		Gaussion Noise attack		Poission Noise Attack		Speckle Noise attack	
	PSNR	MSE	PSNR	MSE	PSN R	MSE	PSNR	MSE
Lena	9.71	6.93	9.71	6.94	9.65	7.03	9.74	6.90
Jet	8.49	9.40	8.36	9.47	8.34	9.51	8.37	9.44
Sailboa t	8.45	9.28	8.42	9.33	8.41	9.37	8.46	9.26
Barbara	9.04	8.10	9.04	8.10	9.00	8.18	9.07	8.04

The attack is changed the image information but the proposed scheme retrieve the image with the minimum noise and its PSNR, MSE values are nearly 90-97% retrieved. So when attacks applied on the share images, the proposed scheme retrieves the maximum share image information with the minimum distortion.

Figure 7 and 8 shows that the comparison graph between the with attack and without attack of the sample images (Lena, Jet, Sailboat, Barbara) with the performance such as PSNR and MSE values. In this graph the X axis takes with attack and without attack, Y axis takes the different images and Z axis shows that the PSNR and MSE values. When the attacks are applied to the different images, the PSNR and MSE values of without attack on the shares are a best performance. The PSNR and MSE values of the without attack compared to with attack 90-97% retrieved the shares.

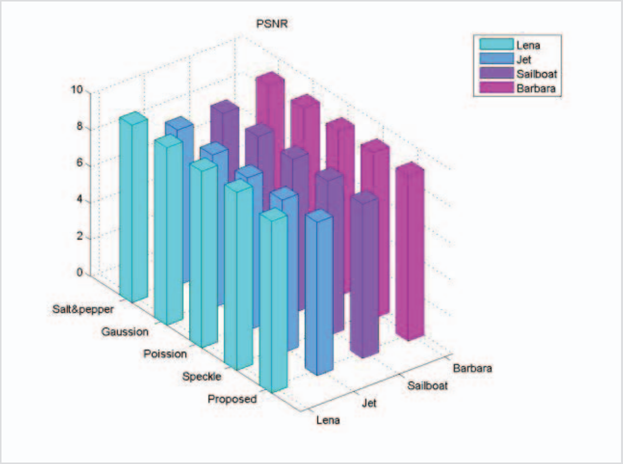

Fig. 7. Comparison between PSNR values of different attacks and proposed scheme

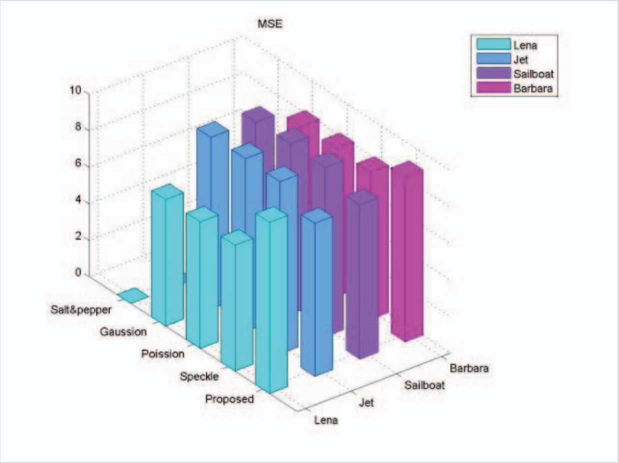

Fig. 8. Comparison between MSE values of different attacks and proposed scheme

C. *Comparative Analysis*

The proposed (k, n) visual cryptography is compared with many other existing schemes [2, 14–20] are listed in Table 5.

TABLE V. COMPARISON OF ENTROPY, NPCR, UACI MEASURES WITH EXISTING SCHEMES

Schemes	Entropy (sh)	NPCR (%)	UACI (%)
Propsoed Scheme	7.9988	99.60	32.58
Ref. [2]	-	99.56	25.63
Ref. [14]	7.9968	99.58	28.62
Ref. [15]	7.9970	99.58	33.45
Ref. [16]	-	99.52	33.14
Ref. [17]	-	70.10	32.80
Ref. [18]	7.9890	95.00	28.96
Ref. [19]	7.2470	98.75	37.68
Ref. [20]	6.7320	98.70	27.46

From the table 5, the Entropy, NPCR, UACI values of the proposed method is higher than the existing method. So the image security is improved by the proposed VC Scheme.

V. CONCLUSION

In this paper, a new k out of n secret image sharing scheme in visual cryptography is proposed. The performance of the proposed scheme was implemented and evaluated based on the standard test images such as Lena, Jet, Sailboat, Barbara. The experimental results and analysis for test images shows that the scheme has great performance in terms of visual testing, encryption quality testing and security analysis can satisfy the security and performance requirements. As an attack results, the proposed scheme has a superior ability to shares the secret image against any attacks such as salt and pepper noise attack, gaussion noise attack, poission noise attack and speckle noise attack.

REFERENCES

[1] Duanhao Ou, Wei Sun and Xiaotian Wu, “Non-expansible XOR-based visual cryptography scheme with meaningful shares”, Journal of Signal Processing, Vol.108, pp.604-621, 2015.

[2] A Nag, S Biswas, D Sarkar, PP Sarkar, “Secret Image Sharing Scheme Based on Boolean Operation. Cybernetics and Information Technologies”, 2014;14:98-113.

[3] Ram Krishna Jha and Abhijit Mustafi, “Boolean XOR Based (k, n) Threshold Visual Cryptography for Grayscale Images”, International Journal of Computer Science and Informatics ISSN: 2231 –5292, Volume-2, Issue-3, 2012.

[4] Savita Patil1, Jyoti Rao, “Extended Visual Cryptography for Color Shares using Random Number Generators”, International Journal of Advanced Research in Computer and Communication Engineering 2012:1.

[5] Xiaotian Wu and Wei Sun, “Improved tagged visual cryptography by random grids”, Signal Processing, Vol.97, pp.64-82, 2014.

[6] Vinita Sharma et al, “k-n Secrete Sharing Scheme of Visual Cryptography Using2X2 Blocks Replacement”, International Journal of Science, Engineering and Technology, 10.2348 /ijset06150553.

[7] Carlo Blundoa, Alfredo De Santis, and MoniNaor, “Visual cryptography for grey level images”, Journal of Information Processing Letters Vol.75, pp.255–259, 2000.

[8] S. Tsai, T.H. Chen, G. Horng, “ A cheating prevention scheme for binary visual cryptography with homogeneous secret images”, Pattern Recognition 2007; 40:2356–2366

[9] Hao Luo, Hua Chen, Yongheng Shang, Zhenfei Zhao and Yanhua Zhang, “Color transfer in visual cryptography”, Journal of Measurement, Vol.51, pp.81-90, 2014.

[10] Pandey and Neerajshukla, “Visual Cryptography Schemes using Compressed Random Shares”, Journal of Advance Research in Computer Science and Management Studies,Vol.1,No.4,pp.62-66,2013.

[11] Anupam Bhakta, Sandip Maity, Ramkrishna Das and Saurabh Dutta , “An Approach of Visual Cryptography Scheme by Cumulative Image Encryption Technique Using Image-key Encryption, Bit-Sieved Operation and K-N Secret Sharing Scheme”, International Journal of Innovative Technology and Exploring Engineering, Vol.3, Issue.1, pp.20-23,2013.

[12] Ching-Nung Yang et al, “Aspect ratio invariant visual cryptography by image filtering and resizing”, Pers Ubiquit Comput, DOI 10.1007/s00779-012-0535-0, pp. 843–850, 2013.

[13] http://www.hlevkin.com/TestImages/

[14] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, “A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle”, Journal of Electrical and Computer Engineering,Vol.2012,pp.1-14,2012.

[15] Musheer Ahmad, Hamed D. Alsharari, Munazza Nizam, “Security Improvement of an Image Encryption Based on mPixel-Chaotic-Shuffle and Pixel-Chaotic-Diffusion”, European Journal of Scientific Research, Vol. 98, No. 3, 2013.

[16] Khanzadi, H.; Omam, M.A.; Lotfifar, F.; Eshghi, M., “Image encryption based on gyrator transforms using chaotic maps”, In: Signal Processing (ICSP), 2010 IEEE 10th International Conference on 2608–2612 (2010)

[17] Chin-Chen Changa, Chia-Chen Linc, T. Hoang Ngan Led, Hoai Bac Led, “Sharing a Verifiable Secret Image Using Two Shadows”, Pattern Recognition, Vol. 42, November 2009, Issue 11, 3097-3114.

[18] N. Sethi, D. Sharma, Novel Method of Image Encryption Using Logistic Mapping, Int. J. Comput. Sci. Eng., 1(2) (2012) 115-119.

[19] R. Ye, “A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism”, Elsevier Optics Commun., 284(2011), 5290-5298.

[20] C.K. Huang, H. Nien, “Multi chaotic systems based pixel shuffle for image encryption”, Elsevier Optics Commun., 282(11) (2009) 2123-2127.