I.J.Computer Network and Information Security, **2014, 2, 54-60**
Published Online January 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.02.08

An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding

Aarti, Pushpendra K Rajput
Computer Science & Engineering Department, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India
Computer Science & Engineering Department, Sharda University, Greater Noida, India
aarti.1208@gmail.com, pushpendrakumar.rajput@sharda.ac.in

***Abstract*—**Conventional visual secret sharing schemes generate noise-like random pixels on shares to hide secret images. It suffers a management problem, because of which dealers cannot visually identify each share. This problem is solved by the Extended Visual Cryptography scheme (EVCS). However, the previous approaches involving the EVCS for general access structures suffer from a low contrast problem. This paper proposes a new *(k,n)*-threshold image sharing scheme using extended visual cryptography scheme for color images based on bit plane encoding that encrypts a color image in such a way that results of encryption is in the form of shares. Shares do not reflect any information directly, information is scrambled instead. The traditional binary EVCS is used to get the sharing images at every bit level of each principle component of a color image. This scheme provides a more efficient way to hide natural images in different shares. Furthermore, the size of the hidden secret can be recovered by inspecting the blocks in the shares. This new scheme for color images gives the ideal contrast in the recovered image.

***Index Terms*—**Extended visual cryptography scheme, bit plane encoding, pixel expansion, contrast, and histogram.

I. INTRODUCTION

Visual Cryptography is kind of secret sharing scheme which focuses on sharing secret images [1], [2]. Visual Cryptography split secret image into random looking share which does not reveal any information about secret message. But secret message can be reconstructed by stacking the transparencies. In *(k, n) VCS*, one secret message is encoded into *n* random looking shares. When k or more shares are printed on transparences or when these are stacked together, secret image is revealed. But *(k-1)* or fewer shares cannot reveal information about secret image.

The shares generated by the traditional visual cryptography schemes are nearly all disorganized images. The Hacker may break the shares, although he may not know the secret.

Nair et al. [1] and Blonde et al. [3] showed constructions of threshold VCS with perfect reconstruction of the black pixels. Ateniese et al.[4] gave constructions of VCS for the general access structure which proposed a cryptography scheme called Extended Visual Cryptography Scheme (EVCS). The security feature is greatly strengthened by transferring meaningful shares than disorganized shares. Based on the halftone technique and color decomposition [5], the concepts of EVCS have been extended to such a level that the secret image is allowed to be a gray scale or a color image rather than merely a black-white binary image [6], [7]. Dorset [8] proposed a method for an arbitrary access structure to construct an extended visual cryptography scheme, which is not necessarily monotonic.

In 2005, Lukac and Plataniotis [9] proposed an image encryption scheme using VCS. The encryption scheme decomposed the gray scale image into 8 bit planes and applied the VCS to each bit plane in order to get n random looking binary images. By stacking the corresponding binary images in bit level, the gray-scale noisy shares can be generated.

In this paper, we discuss the properties of the extended matrix collection for EVCS. Then we propose a EVCS for single color images with optimal extended matrix collection. The previous schemes (originally proposed for binary or grayscale or color images) using random-looking shares can be directly extended to generate innocent-looking shares using EVCS with bit-plane encoding scheme which provide the more security over network.

The rest of this paper is organized as follows. Section II briefly describes the Visual Cryptography Scheme and Lukas and Plataniotis's image encryption algorithm. Then, the proposed scheme is demonstrated in Section III. Section IV illustrates several experiment results. Section V. illustrates the performances of the proposed scheme. Finally, concluding remarks are given in Section VI.

II. RELATED WORKS

A. Fundamentals of Visual Cryptography

Visual cryptography is introduced by Normand Shamir [1].They developed a black and white *(k, n)*-VC scheme for secret sharing. It consists of two collections of $n \times m$ bbinary matrices S_0 and S_1 and, having elements denotedby*1*forablackpixeland*0*forawhite pixel. To encrypt white (black) pixel, a dealer randomly chooses one of the matrices in $S_0(S_1)$ and distributes its rows to the participants.

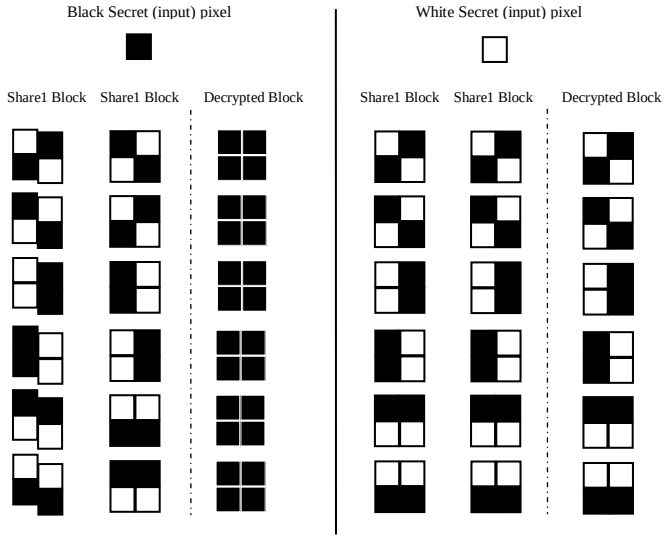


Figure 1: Conventioanl VC scheme: a secret pixel can be encoded into two sub pixels in each of the two shares.

Each pixel$p$ from a secret binary image is encoded into *m* black and white sub-pixels in each share. If *p* is a white (black) pixel, one of the six columns is selected randomly with equal probability, replacing *p*.

***Definition 1*:** Let k, n, m and d be non-negative integers satisfying $2 \leq k \leq n$ and $0 \leq d \leq m$. The two collections of $n \times m$ binary matrices (S_0, S_1)constitute a black and white *(k, n)*–VC scheme if there exists α (> 0) value satisfying the following.

1) Contrast: for any s in S_0, the "OR" operation of any *k* out *n* of rows of *s* is a vector *v* that satisfies $w(v) \leq d - \alpha(m)$ where $w(v)$is the Hamming weight of the vector $v, m$is the pixel expansion of the scheme and α is the contrast of the scheme.

2) Contrast: for any s in S_1, the "OR" operation of any $k$out $n$of rows of is a vector *v* that satisfies $w(v) \geq d$.

3) Security: for any $i_1 < i_2 < \ldots\ldots i_t$ in $\{1,2\ldots.n\}$ with $t < k$, the two collections of $t \times m$ matrices $D_j, j = 0,1$, obtained by restricting each $n \times m$ matrix in $S_j, j = 0,1$, to rows $i_1, i_2 \ldots i_t$, are indistinguishable in the sense that they contain the same matrices.

The first property is related to contrast of the image which states that when qualified sets of users stacked their transparencies, image is revealed. The value $\alpha(m)$is called relative difference and $\alpha(m).\ m$is called contrast of the image. The set$\{(X, t_x)\}_{x\epsilon\ \Gamma Qual}$is called set of threshold. Third property related to the security of the images which states that fewer shares *(k-1)* cannot reveal information about secret image.

Wang et al. [20] proposed the shift visual cryptography. Two secret images are encoded into two share images and all the secrets can be revealed by keeping one of two shares and shifting the other share several columns and rows in stacking phase. Wang et al. [10] proposed scheme which can encode three secrets into four shares, and decoding can be done by superimposing the transparency of shares with different level of contrast. To overcome the angle restriction of Wu and Chen's scheme [11]. Wu and Chang [12] refined the idea of Wu and Chen [11] by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90◦, 180◦ or 270◦) can be removed.

B. Extended Visual Cryptography

The term of extended visual cryptography scheme was first introduced by Nonretail in [2], where a simple example of *(2, 2)*-EVCS was presented. In this paper, when we refer to a corresponding VCS of an EVCS, we mean a traditional VCS that have the same access structure with the EVCS. Generally, an EVCS takes a secret image and original share images as input, and outputs shares that satisfy the following three conditions:

1) Any qualified subset of shares can recover the secret image;
2) Any forbidden subset of shares cannot obtain any in formation of the secret image other than the size of the secret image;
3) All the shares are meaningful images.

Definition 2: A *(k, n)*-threshold EVCS can be constructed by the values *αF (m), αS (m),* d and a family of *2n*pairsof collections $\{(B_W^{C_1 \ldots\ldots C_n})\}_{C_1 \ldots\ldots C_n} \epsilon \{b, w\}$ which satisfy the following three conditions:

1) For each $C_1 \ldots\ldots C_n \epsilon \{b, w\}$, the relative difference $\alpha_F(m)$, the threshold d satisfy that for each $S \epsilon B_W^{C_1 \ldots\ldots C_n}$the OR V of any k of the n rows meets $H(V) \leq d - \alpha_F \times m$; whereas, for any $S \epsilon B_b^{C_1 \ldots\ldots C_n}$ it results that $H(V) \geq d$

2) For each $C_1 \ldots\ldots C_n \in \{b, w\}$ and for any subsets $\{i_1 \ldots\ldots i_q\}$ of $\{1, \ldots\ldots, n\}$ with $q < k$, the two collection of $q \times m$ matrices $D_t^{C_1 \ldots\ldots C_n}$with$t \in \{b, w\}$ obtained by restricting each n ×m matrix in $B_t^{C_1 \ldots\ldots C_n}$to rows $i_1, \ldots, i_n$are distinguish in the sense that they contain the same matrices with the same frequencies.

3) For any $i \in \{1, \ldots, n\}$ and any $c_{1,\ldots\ldots\ldots, c_{i-1}, c_{i+1}, \ldots\ldots, c_n} \epsilon \{b, w\}$ it results that

$$min_{S \epsilon \mu_b} \left(H(S_i) - max_{S \epsilon \mu_w} \left(H(S_i) \right) \right) \geq \alpha_s(m).m$$

Where,

$$\mu_b = \cup\ B_W^{C_1 \ldots\ldots C_{i-1}} b_{C_{i+1} \ldots\ldots C_n}$$

$$c_1 .., \ldots .., c_{i-1}, c_{i+1}, \ldots, c_n \in \{b, w\}$$

and,

$$\mu_w = \bigcup\ B_b^{C_1 \ldots\ldots C_{i-1}} b_{C_{i+1} \ldots\ldots C_n}$$

$$c_1 .., \ldots .., c_{i-1}, c_{i+1}, \ldots, c_n \in \{b, w\}$$

The first condition states that q qualified set of users; stacking their shares (or transparencies) can correctly recover the secret image. The second condition is related to the security of the scheme, it implies that by inspecting the shares one cannot gain any secret information on the shared image even though he knows the original images of all n shares we started with. Finally, the third condition implies that the original images are not "modified".

Zhou et al. [5] presented an EVCS by using half toning techniques, and hence can treat gray-scale input share images. Wan get al. proposed three EVCSs by using an error diffusion half toning technique [13] to obtain nice looking shares. Fang [14] and Chen et al. [15] proposed VC-based and random - grid -based techniques respectively, for (k, k) -EVCS with a progressive decryption effect. Wang et al. developed a matrix extension algorithm for $(k,)$ -EVCS by modifying any existing VCS with random-looking shares, which were then, utilized as meaningful shares [13].

EVCS can also be treated as a technique of staging reply, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected.

C. Visual Cryptograhy for Color Images

Basic principles of color the additive (RGB model) and subtractive models (CMY model) are commonly used to describe the constitutions of colors [17]. In color images, encryption and decryption is based on half toning and inverse half toning. In color images, image is divided into Red, Green, Blue components and shares are generated by applying simple VCS scheme on this components. Then at receiver side shares are superimposed to reveal secret image.

Verheul and Tilburg [16] are first to present a secret sharing scheme for images with c colors in 1997. The principle of this scheme is to transform one pixel of image to b sub-pixels, and each sub pixel is divided into c color regions. Young-Chang Hou [17] introduced the visual cryptography for color images with the use of color model.

III. THE PROPOSED SCHEME

The proposed scheme is based on bit plane share gene ration using EVCS which provide better contrast in recovered image. Meaning flu share sari gene rated using EVCS which provide better security. This scheme divides true color image into R, G, B component. Each component is represented in bit planes. Two cover image sari used to hide the bit planes using EVCS. Using EVC Son each bit level representation of cover image sand secret images, mean ingful shares are gene rated by combining corresponding hare for each component. The flowchart of proposed scheme is represented in the Fig.3 and Fig.4 (encryption and decryption phase). Detailed description of proposed scheme is formulated in the following phase.

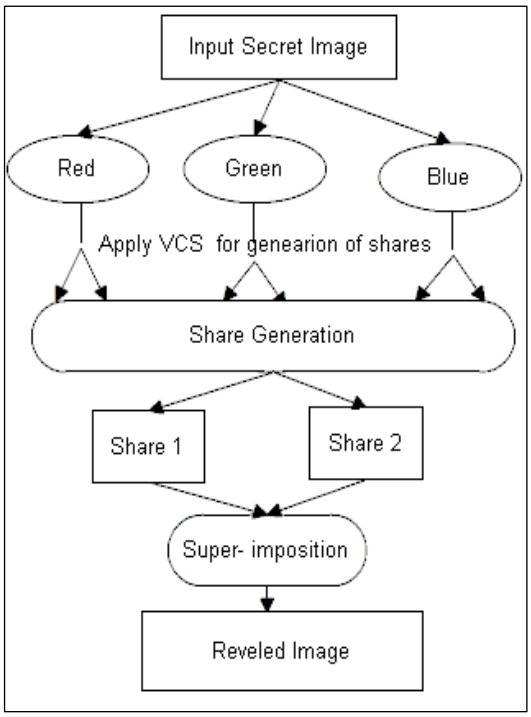


Figure 2: Visual Cryptography Scheme for color images

The idea of Orem bedded EVCS contains two main steps:

1) Generate *n* covering shares, denoted as

$$\{s_0, s_1, \ldots, s_{n-1}\}$$

2) Generate the embedded shares by embedding the corresponding VCS into the *n* covering shares, denoted as $\{e_0, e_1, \ldots . e_{n-1}\}$.

A. Algorithm for Share Generation

True color secret image of size $w \times h$ is taken. In this scheme secret image is divided into R, G, and Components. Each single value of pixel $R(i,j)$ $(G(i,j) or B(i,j))$ ofred (green or blue) components is represented in binary form, 0 to represent Tran's parent and 255 to represent red pixel (green or blue). Each component is represented to *N*1- bit planes. Colorful cover images are used to hidethe*N*1-bit planes using EVCS for generation of meaningful shares. Cover images are also de composed in to three components (R, G, B) and *N* 1-bit planes are gene rated. Then *n* bit planes of secret image scream bedded in to cover images for generating mean ingful images. Then, every pixel of all the binary image scene rated from the bit planeisexpandedintoa*2*×*2*blocktowhicha

Black or white color is assigned according to the model presented in Fig1.

***Algorithm of share generation*:**

1. Transform the color image S into three channels: *R, G,* and *B.*
2. Each component is divided into *N* 1-bit planes. Each bit plane is the binary image contacting level of information.
3. Apply EVCS to each bit planes of secret color image using corresponding bit planes of respective component (R, G or B) of public color images.

$$F_{EVCS}\left(R_{b1}(i,j), CV_1(i,j) \dots \dots CV_n(i,j)\right) =$$
$$\begin{cases} [S_i^1, S_i^2 \dots \dots, S_i^n]^T \epsilon\, C_w^{c_1 \dots \dots c_n}, R_{bi}(i,j) = 0 \\ [S_i^1, S_i^2 \dots \dots, S_i^n]^T \epsilon\, C_b^{c_1 \dots \dots c_n}, R_{bi}(i,j) = 1 \end{cases}$$

Where $C_w^{c_1 \dots \dots c_n}$ ={all the matrices obtained by permuting the columns of basis matrix$[S_i^1, S_i^2 \dots \dots, S_i^n]$
and,

$C_b^{c_1 \dots \dots c_n}$ = {all the matrices obtained by permuting the columns of basis matrix $[S_i^1, S_i^2 \dots \dots, S_i^n]$

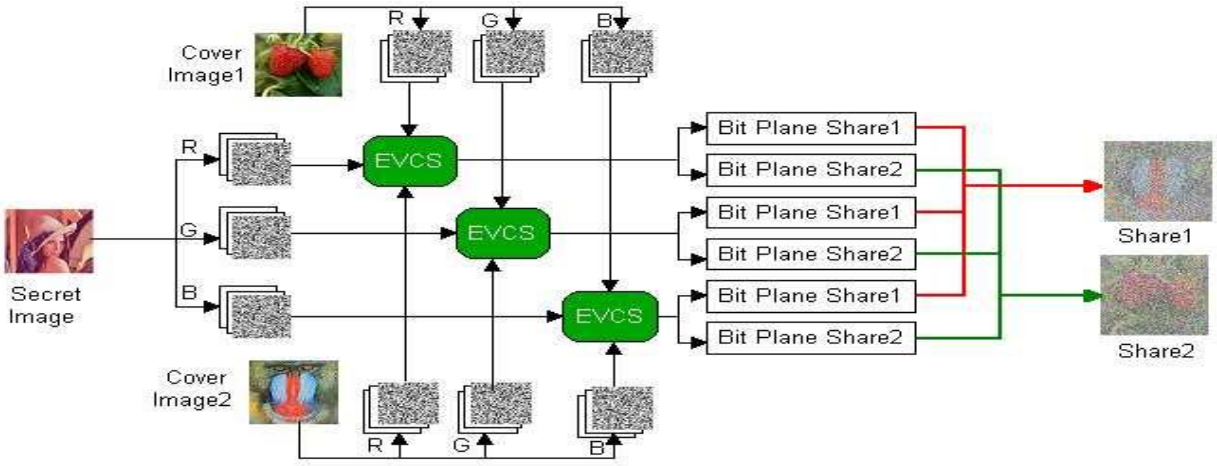


Figure 3: Encryption process for generating shares of color image with proposed scheme

$$R(i,j) = R_{b1}(i,j)2^{N-1} + \ R_{b2}(i,j)2^{N-2} + \ \dots$$
$$+ \ R_{bn-1}(i,j)2 + \ R_{bn}(i,j)(1)$$

Here, $R_{b1}(i,j)$ represents the pixel value in location *(i, j)* in *i-th*bit plane of each channel, and $R_{b1}(i,j)$ is the most significant bit plane. Therefore, a channel can be divided into *N* binary images using (l).

4. Stack the corresponding binary shares in bit level to achieve *n* shares.

$$CSH^{\,j}(x,y) = BSH^{\,j_1}(x,y).2^{N-1} + \dots\dots + BSH^{\,j_{N-1}}(x,y).2\ BSH^{\,j_N}(x,y)$$

5. Generate the *n* color shares by combining the corresponding shares of R, G and B channels.

B. Secret Revealing Phase

In the secret revealing stage, when any *q*, *k* of *n* color shares are achieved, they are broke into their RG and B channels.

***Algorithm of secret revealing phase*:**

1. Decompose the color shares into its component R, G and B channel.
2. Create bit planes of each channel.
3. Apply "OR" to the corresponding bit planes of every share.

$$RS_{bi} = \begin{cases} 0, \ BSH_j^i(x,y) = 0 (1 \le j \le q) \\ 2) \\ 1, \text{otherwise} \end{cases}$$

Then, all the binary shares at the same bit plane conduct the OR operation using (2) to get revealed binary secret image RS_{bi}

4. Stack the corresponding binary shares in bit level to achieve three channels of the secret image.

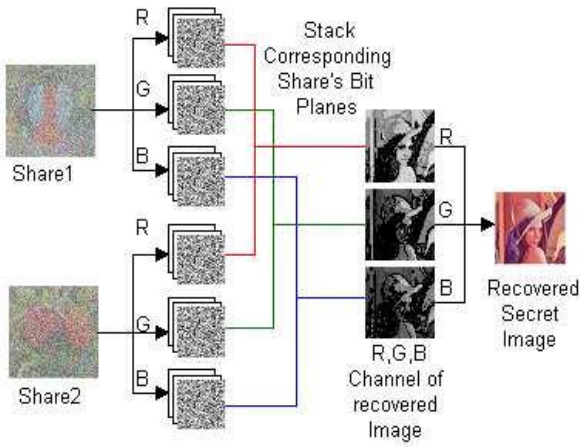


Figure 4:Decryptionprocess of proposed scheme

Revealed binary secret image $R\ S_{bi}$ are segmented into blocks with the same size as $s_i^j (l \le i \le N, l \le j \le q)$ in the sharing phase. The i^{th} original secret bit plane S_{bi} can be recovered by inspecting the corresponding blocks in RS_{bi}. The inspecting function is formulated in (3).

$$S_{bi} = \begin{cases} 1, HB \ge d \\ 0, otherwise \end{cases} \quad (3)$$

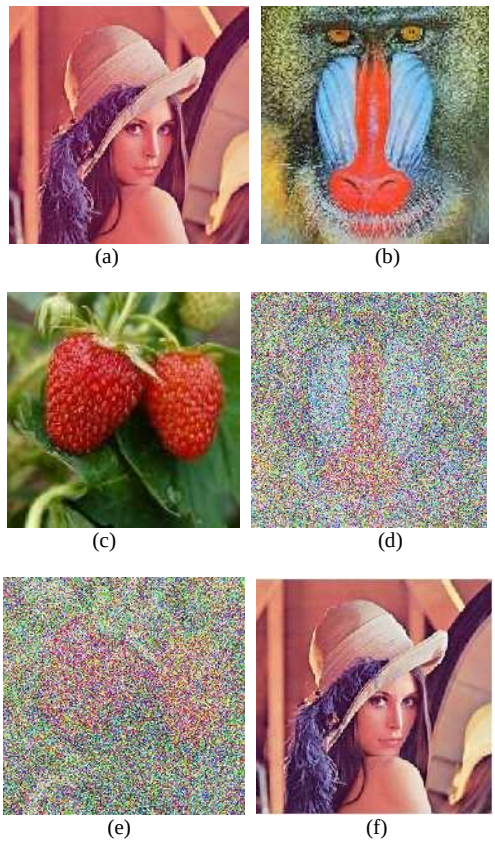
Where *HB* is the hamming weight of the blocks in RS_{bi} associated to location *(x,y).*

5. Combine the all three recovered component and get final secret image.

IV. EXPERIMENTAL RESULT

In this section, experimental results of the proposed sharing scheme are demonstrated.

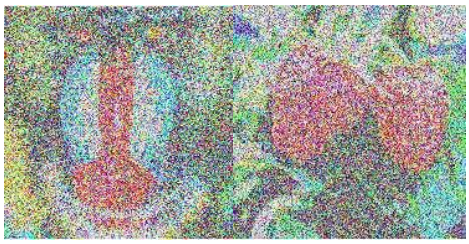
A *256 × 256* pixels true color secret image is used which is shown in Fig.5 (a). A *(2, 2)*-threshold EVCS is implemented using MATLAB R2009b in this experiment. Fig.*5 (b)* and *5(c)* show the cover images. Output shares of the proposed sharing scheme are represented in Fig.*5 (d)* and *5(e*).When the two shares are collected, the secret image can be perfectly recovered shown in Fig. 5*(f).*



(a) (b) (c) (d) (e) (f)

Figure 5: The proposed scheme using (2, 2)-threshold EVCS. (a) Secret Image, (b) Cover Image1, (c) Cover Image2, (d) Share1,(e) Share2,(f)Recovered Image

Experiments how that the mean ingful shares can be further improved if we apply the proposed EVCS with halftones component of cover images with each bit plane instead of taking the bit plane of cover images as shown in figure*6 (a)* and*6(b).*



(a) (b)

Figure 6: Further improvement in meaning flusher's using halftones component of cover images. (a) Share1, (b) Share2

Table I shows a brief comparison of proposed scheme with some other previously developed techniques based on some important parameters mostly accepted for VCS. Meaningful shares reduce the interest of hackers and can easily manage.

TABLE 1.COMPARISON OF VISUAL CRYPTOGRAPHY SCHEME ON THE BASIS OF PIXEL EXPANSION, TYPE OF SHARE GENERATED, IMAGE DIMENSION.

S.N.	Authors		Pixel Expansion	Type of share images	Image dimension
1	Naor and Shamir [1]		4	Random	Increasing
2	Du-Shiau Tsai *et al* [22]		9	Meaningful	Increasing
3	Chin-Chen Chang *et al* [12]		4	Meaningful	Increasing
4	Hegde*et al*. [21]		4	Meaningful	Increasing
5	Jena and jena [9]		2 or 4	Meaningful	Increasing
6	**Proposed Scheme**	**Stacking**	**4**	**Meaningful**	**Increasing**
		Inspection	**0**	**Meaningful**	**Constant**

A. MSE and PSNR based Comparison with Various Techniques

A descriptive comparison with previous techniques based on widely used quality parameters PSNR and MSE is presented in Table II. The results show that the proposed scheme has a better quality of recovered image. Fig. 7 illustrates that the proposed two approaches have a lower value of MSE and a significant improvement over PSNR values compared to the schemes of Kang [6] and Droste [8].

TABLE II.COMPARISON OF PSNR AND MSE VALUES OF PROPOSED SCHEME WITH PREVIOUS SCHEMES

Sr. No.	Scheme	MSE
1	Proposed Scheme	**33.14**
2	Kang [6]	5896.9
3	Droste [8]	5846.5

B. Robust Against Attacks

Table III shows the impact of various attacks on shares during transmission. The two most widely criteria MSE and PSNR for image quality are used to define the impact of various attacks. These attacks are considered on Shares during transmission. These results of proposed scheme with a number of image attacks demonstrate that the scheme is more robust. Results shows that altered share can recover an image with a significant level of quality

TABLE III.IMPACTS OF DIFFERENT NOISE ON SHARES AND RECOVERED IMAGES GENERATED USING EVCS

Noise Type	MSE			PSNR		
	RED	GREEN	BLUE	RED	GREEN	BLUE
Original image	275.675	80.863	61.413	23.726	29.053	30.248
Gaussian	13734	10754	11349	7	8	8
Gaussian (m=0,v=0.01)	15316	12044	12179	6	7	7
Gaussian (m=0,v=0.05)	17503	14184	13752	6	7	7
Salt and Pepper	6718.1	8970.1	10164	9.9	8.6	8
Salt and Pepper (v=0.09)	6718.1	8970.1	10164	9.9	8.6	8
Poison	5062.9	7318.7	9083.7	11.1	9.5	8.5
Speckle	16242	10897	11419	6	8	8

Gaussian Salt and Pepper Poison Speckle

Figure 7: Impact of different noises on recovered images using EVCS

V. CONCLUSION

This paper provides as asana annex tended visual cryptography scheme using bit plane encoding for different channel for improvement of visual quality. A bit plane of an image is binary image that carry visual information of original images across the color channels so store taint heroic in al pixel values the same before and after encryption. The proposed schemed crypt a true color secret image into *n* shares which are some meaningful images where any of the *k* or more shares can lossless recover the secret image. The size and contrast of the decrypted image using the propose scheme are real. Meaningful shares can be easily recognized and managed.

REFERENCES

[1] M.Naor, A.Shamir, “Visual crypto graphy”, in: A. De Santos (Ed.), Advances in Cryptology: Eurpocrypt’94, Lecture Notes inComputer Science, vol. 950, pp.1–12, 1995.

[2] M.NaorandA. Shamir "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary version appears in “Security Protocols", M. Lomased.Vol.1189ofLecture Notes in Computer Sciences, Springer-Verlag, Berlin, pp.197-202, 1997.

[3] C.Blundo, A.DeSantis, D.R.Stinson, “On the contrast in visual Crypto graphy schemes”. J. Cryptology12-261–289, 1999.

[4] G. Ateniese, C.Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography"in23rdInternationalColloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F.M. aufder Heide and B.Monien, Eds.,vol.1099. Berlin: Springer-Verlag, pp. 416-428, 1996.

[5] Z. Zhou, G. R.Arce, and G. D. Crescendo, “Halftone visual cryptography”, IEEE Transaction on Image Processing ,vol.15,no. 8, pp. 2441–2453, 2006.

[6] In Koo Kang, Gonzalo R.Arce, Heung-KyuLee, “Color extended visual cryptography using error diffusion”, icassp, pp.1473-1476, 2009.

[7] H.C. Wu, H.C. Wang, and R.W.Yu, “Color Visual Cryptography Scheme Using Meaningful Images”, IEEE Computer Society, vol. 03, pp.173-178, 2008.

[8] S.Droste, “New result son visual cryptography,” inProc.CRYPTO’96, vol.1109, pp.401–415,

Springer-Overflag Berlin LNCS, 1996.

[9] D. Jena and S.K. Jena, *"A Novel Visual Cryptography Scheme"*, In Proceeding of International Conference on Advance Computer Control, pp 207-211(2009).

[10] R.Z.Wang, Y.K.Lee, S.Y.Huang, andT.L. Chia, *"Multilevel visual secret sharin,"*, Proceedings of the Second International Conference on Innovative Computing, Information and Control, Kumamoto, Japan, pp. 283-283, 2007.

[11] C.C. Wu, L.H. Chen, "A study on visual cryptography, Master Thesis, Institute of Computer and Information Science", National Chiao Tung University, Taiwan, R.O.C., 1998.

[12] H.-C.Wu, C.-C.Chang, "Sharing visual multi-secrets using circle shares", Computer Standards & Interfaces 134 (28):123–135, 2005.

[13] D.Wang, F.Yi, and X.Li, "On general construction for extended visual cryptography schemes," Pattern Recognition, vol.42, pp. 3071-3082, Nov. 2009.

[14] W.P.Fang, "Friendly progressive visual secret sharing," Pattern Recognition, vol.41, pp. 1410 - 1414, Apr2008.

[15] T.H.Chen and Y.S.Lee, *"Yet another friendly progressive visual secret sharing scheme", in Proc.*5thInt. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, pp. 353-356, 2009.

[16] E.R. Verheul, H.C.A.Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes", Des. Codes Crypto gr. 11-179–196, 1997.

[17] Y.C. Hou, "Visual cryptography for color images", Pattern Recognition, vol. 36, pp. 1619–1629, 2003.

[18] D.R. Stinson, "An introduction to visual cryptography", presented at Public Key Solutions'97, Toronto, Canada, and April 28–30, 1997.

[19] R.Lukac and K.Plataniotis," Bit-level based secret sharing for image encryption," Pattern Recognition, vol. 38, no. 5, pp. 767-772, 2005.

[20] C. Hegdeet. Al., *"Secure Authentication using Image processing and Visual Cryptography for Banking Application", In Proceeding* of 16th International Conference on Advanced Computing and Communication(ADCOM 2008), MIT Campus, Anna University Chennai, India, pp.433-439, 2008.

[21] D.Wang, P.Luo, L.Yang, D.Qi, and Y.Dai, "Shift visual cryptography scheme of two secret images," Progress in Natural Science, Vol.13, No. 6, pp. 457-463, 2003.

[22] D.S. Tsai, G. Horng, T.H. Chen and Y.T. Huang, "A Novel Secret Image Sharing Scheme for True-Color Images with Size Constraint", Information Sciences vol.179, issue 19, pp. 3247–3254 Elsevier, 2009.

[23] I. Kang, G. R. Arce and H. K. Lee, "Color Extended Visual Cryptography using Error Diffusion", IEEE Transaction on Image Processing. vol. 20.No. 1, 1057-7149, pp. 132-145, 2010.

[24] J.K. Mandal and S. Ghatak, *"Secret Image/ Message Transmission through Meaningful Shares using (2,2) Visual Cryptography(SITMSVC)", In Proceeding* of International Conference on Recent Trends in Information Technology, ICRTIT, MIT, Anna University, Chennai, IEEE 978-1-4577-0590-8/11, 2011.

Aarti received the B. Tech. degree in Computer Science & Engineering from Punjab Technical University, Punjab in 2010 and M.Tech. degree in Computer Science & Engineering from Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, in 2012. She is assistant professor at the Department of Computer Science and Engineering, Guru Nanak Dev University, Punjab. These days she is pursuing her doctoral degree at Dr. B. R. Ambedkar National Institute of Technology. Her research areas lie in the area of visual cryptography and software engineering.

Pushpendra K Rajpiyt received the B. Tech. degree in Information Technology from Uttar Pradesh Technical University, UP in 2008 and M.Tech. degree in Computer Science & Engineering from Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, in 2012. He is assistant professor at the Department of Computer Science and Engineering, Shard University, Uttar Pradesh. His research areas lie in the area of cryptography, software Engineering and computational Intelligence.

How to cite this paper: Aarti,Pushpendra K Rajput,"An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding", IJCNIS, vol.6, no.2, pp.54-60, 2014. DOI: 10.5815/ijcnis.2014.02.08

