Anantha Kumar Kondra, Smt. U. V. Ratna Kumari / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.1090-1096

An Improved (8, 8) Colour Visual Cryptography Scheme Using Floyd Error Diffusion

Anantha Kumar Kondra*, Smt. U. V. Ratna Kumari**
*(Department of Electronics and Communications, University College of Engineering, JNTUK, Kakinada)
** (Department of Electronics and Communications, University College of Engineering, JNTUK, Kakinada)

ABSTRACT

Visual cryptography (VC) is the simplest and a perfect way to provide the security to the confidential information. VC in color images encrypts a color secret message into n color halftone image shares. In earlier VC schemes in order to recover the secret image, one has to collect a set of qualified shares and print them onto transparencies. However this VC scheme shows good results for black and white or gray scale images, but not with the Color Images due to its color structure. Using the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. Now a days the biggest challenge is to provide the security in order to protect the confidential information from Security threats. In this paper we introduce a new solution which helps to identify the error in the shares and to verify the Authentication. Using CRC algorithm and Color VC scheme and error diffusion method generates the quality shares and diffuses the errors and provides the security from threats like Modification ,Fabrication ,Interception and shows the good results compared to the previous schemes and increases the security level.

Keywords - Colour Meaningful Shares, Cyclic Redundancy Check, Binary Information, Visual Cryptography Scheme, Error Diffusion, Secret Sharing.

I. INTRODUCTION

Visual Cryptography is a perfect way to provide the security for the confidential information. Initially it was introduced by Kafri and Keren in 1987 [1] where binary pictures were considered in the encryption of pictures by two random grids. The encryption of a secret picture or shape into two random grids which are printed on transparencies such that the areas containing the secret information in the two grids are inter-correlated. Similar idea that the decryption needs only human visual ability, Naor and Shamir initially used the terminology, visual cryptography[1], which is defined as the study of secret (crypto) writing (graphy) and the study of mathematical techniques related to aspects of information security. Visual cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. Visual cryptography is a very secure and unique way to protect secrets. Visual cryptography has two important features. The first feature is its perfect secrecy, and the second feature is its decryption method which requires neither complex decryption algorithms nor the aid of computers. Consider a binary secret image B and a set of *n* participants sharing B. A *k* out of *n* visual secret sharing scheme encrypts B into *n* transparencies (called shares) which are distributed to the *n* participants one by one in such a way that only when *k* or more shares are stacked together can the participants see B by their visual system; while any group of less than *k* shares obtains nothing about B.

Visual cryptography proposed by Naor and Shamir [1] discloses the possibility for using human visual ability to perform the decryption process. Neither computational devices nor cryptographic knowledge is required for the decryption process. With such an interesting characteristic that the decryption process is by the human visual system only, instead of any computational device, visual cryptography attracts much attention from researchers. In particular, it is much useful in situations where computing devices are not available or not possible to use. Naor and Shamir [1] first presented *k* out of *n* visual secret sharing schemes, which ensure that the secret is concealed from groups of less than *k* participants, while it can be seen by groups of at least *k* participants when they stack their shares altogether. Since this pioneer research, many theoretical results on the construction or contrast (the relative difference between the reconstructed white and black pixels in the superimposed image) of visual secret sharing schemes for binary images have been proposed in the literature [4, 5, 6, 7]. Some studies [8, 9, 10] focused on the practical realization of visual cryptographic schemes for gray-level or color images.

A new method called extended visual cryptography (EVC) was developed by Ateniese[2]. In which shares contains not only the secret information but are also some meaningful images. Hyper graph colorings are used in constructing

meaningful binary shares. Since hyper graph colorings are constructed by random distributed pixels, the resultant binary shares contain strong white noise leading to inadequate results. Wang generalized the Ateniese's scheme using concatenation of basis matrices and the extended matrices collection to achieve more simpler deviation of basis matrices[12]. Nakajima extended EVC to a scheme with natural grayscale images to improve the image quality[13]. Zhou *et al.* used half toning methods to produce good quality halftone shares in VC[14]. Fu generated halftone shares that carry visual information by using VC and watermarking methods[4]. Myodo proposed a method to generate meaningful halftone images using threshold arrays. Wang et. al. produced halftone shares showing meaningful images by using error diffusion techniques. This scheme generates more pleasing halftone shares owing to errors diffused to neighbor pixels.

Visual secret sharing for color images was introduced by Naor and Shamir[1] based upon cover semi groups. Rijimen presented a 2-out-of-2 VC scheme by applying the idea of color mixture. Stacking two transparencies with different colors rises a third mixed color. Hou shares by applying halftone methods and color decomposition. Hou decomposed the secret color image into three (Red, Green and Blue) halftone images. He then devised three colored 2-out-of-2 VC schemes which follow the subtractive model for color mixture by exploiting some of the existing binary VC schemes. All of the previously mentioned methods, however, discuss color schemes for 2-out-of-2 or 2-out-of-2 secret sharing where the reconstructed colors are interpreted by some mixing rules of colors. The general construction of a k-out-of-n VC scheme for the color shares was first introduced by Verheul[16]. He proposed a k-out-of-n VC scheme for a -colored image with pixel expansion q^{k-1}, where devised schemes for color q>=c Koga and Yamamoto used a lattice structure to define the mixing result of arbitrary two colors. All of these VC schemes for color images produce random pattern shares. Even though the decrypted messages show messages with various colors, it is more desirable to generate meaningful shares which are less suspicious of encryption. Other approaches to color VC attempting to generate meaningful color shares include. Ching-Nung Yand and Tse-Shih Chen proposed a VCS for color images based upon an additive color mixing method[18]. In this scheme, each pixel is expanded by a factor of three.

This scheme suffers from pixel expansion problem in the size of encrypted shares. In order to reduce the size of encrypted shares Inkoo Kang proposed the VC for color image using visual information pixel (VIP) synchronization with error diffusion technique[11]. This paper introduces a new color VC encryption method which leads to produce securable and meaningful shares and is free of the previously mentioned limitations. The method is simple and efficient. It relies on two fundamental principles used in the generation of shares, namely, error diffusion and VIP synchronization. Error diffusion is a simple and efficient algorithm for image halftone generation.

The quantization error at each pixel is filtered and fed to future inputs. The error filter is designed in a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision. Synchronization of the VIPs across the color channels improves visual contrast of shares. In color VC schemes, due to random matrix permutation the colors of encrypted pixels and the contrast can be degraded. In grayscale VC schemes, it does not affect the visual quality; however, in color schemes, independent execution of random matrix permutation for each color channel can cause color distortion by placing VIPs at random positions in sub pixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation.

The rest of this paper is organized as follows: Section II provides previous methods about standard VC, the extended VC scheme, and the fundamentals of halftone techniques for easy understanding of the proposed VC method. Section III describes the proposed encryption method including the VC matrix ,CRC bits and Binary value adding method and a halftone process to generate final shares. Section IV shows experimental results of the new method and comparisons with previous approaches to prove its effectiveness. In Section V, we discuss topics about image quality, security and advantages of our scheme, and concluded this paper .

II. PREVIOUS WORK

In this section, we give a brief description of VC, extended VC, color models in VC and an error diffusion quantization.

2.1 Basic Visual Cryptography

Generally (k, n)-VC scheme encrypts a secret message into shares to be distributed to n participants. Each share shows noise-like random black and white patterns and does not reveal any information of the secret image by itself. In a k -out-n of scheme, access to more than k shares allows one to recover the secret image by stacking them together, but access to less than k shares is not sufficient for decryption. A black and white (k,n)-VC scheme consists of two collections of nxm binary matrices S_0 and S_1 , having elements denoted by 1 for a black pixel and 0 for a white pixel. To encrypt a white (black) pixel, a dealer randomly chooses one of the matrices in $S_0(S_1)$ and distributes its rows to the n participants. More precisely, a

formal definition of the black and white (k, n) -VC scheme is given next.

The security condition ensures that any less than k shares cannot get any information of the secret image other than the size of the secret image. Based upon the principle of VC, extended VC has been proposed whose shares take meaningful images rather than random noise-like patterns to avoid suspicion.

2.2 Extended Color Visual Cryptography

Generally, a (n, n) –EVC scheme takes a secret image and n original images as input and produces n encrypted shares with approximation of original images that satisfy the following three conditions:

• all the shares are required to recover the secret image;
• any less than shares cannot obtain any information of the secret image;
• all the shares are meaningful images; encrypted shares and the recovered secret image are colored.

Denote $S_c^{c1,c2,....cn}$ as the collection of matrices from which the dealer chooses a matrix to encrypt, where $C,C_1,.....C_n \epsilon \{0,1\}$. for i=1,.....n, C_i is the bit of the pixel on the ith original image and is the bit of the secret message. For a black and c white(k ,n) -EVC scheme, we have to construct 2^n pairs of such collection ($S_0^{c1,c2,....cn}$, $S_1^{c1,c2,....cn}$) , one for each possible combination of white and black pixels in the n original images.

2.3 Color Models

There are two models namely *additive* and *subtractive* color models, which are widely used to describe the constitutions of colors. In the additive color model, the three primary colors are red, green, and blue (RGB), with desired colors being obtained by mixing different RGB channels. By controlling the intensity of red, green, blue channels, we can modulate the amount of red, green, blue in the compound light. The more the colors are mixed, the more the brightness of the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model. In the subtractive model, color is represented by applying the combination of colored lights reflected from the surface of an object. The more the pigments are added, the lower the intensity of the light is and, thus, the darker the light is. This is the reason it is called the subtractive model. Red, Green, and Blue are the three primitive colors of pigment which cannot be composed from other colors. The color printer is a typical application of the subtractive model and, hence, the VC model of Naor and Shamir is also of such kind. the color of the pixel $X_{(p,q)}$ can be expressed in a binary form as

$$X_{(p,q)} = \sum_{i=1}^{8} x_{(p,q)}^{i}\, 2^{8-i}$$

Where $x_{(p,q)}^{i} = [x_{(p,q)1,}^{i}\ x_{(p,q)2}^{i}, x_{(p,q)3}^{i}\ ] \epsilon \{0,1\}^3$ denotes the binary vector at the ith bit-level with i=1 denoting the most significant bit.

2.4 Error Diffusion

Error diffusion is a simple yet efficient way to halftone a grayscale image. The quantization error at each pixel is filtered and fed into a set of future inputs. Fig. 3 shows a binary error diffusion diagram where f(m, n) represents the pixel at (m, n) position of the input image. d(m, n) is the sum of the input pixel value and the diffused errors, g(m, n) is the output quantized pixel value. Error diffusion consists of two main components.

The first component is the thresholding block where the output g(m ,n) is given by

$$g(m,n) = \begin{cases} 1, & if\ d(m,n) \geq t(m,n) \\ 0, & otherwise \end{cases}$$

The threshold t(m, n) can be position dependant. The second component is the error filter h(k, l) where the input e(n, m) is the difference between d(m ,n) and g(n ,m). Finally, we compute d(m, n)

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l)e(m-k,n-l)$$

Where $h(k,l) \epsilon H$, H is a2-D filter. A widely used filter is the error weight originally proposed by Floyd and Steinberg

$$h(k,l) = \frac{1}{16} \times \begin{bmatrix} & * & 7 \\ 3 & 5 & 1 \end{bmatrix}$$

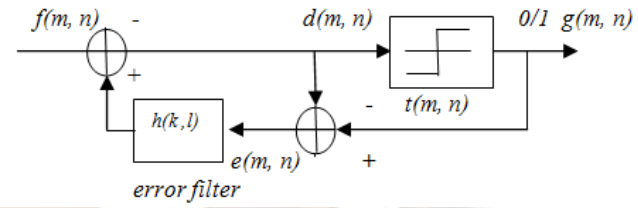


Fig 1 Block Diagram Of Floyd Error Diffusion Technique

where * is the current processing pixel. The recursive structure of the block diagram indicates that the quantization error e(m, n) depends upon not only the current input and output but also the entire past history. The error filter is designed in such a way that the low frequency difference between the input and output image is minimized. The error that is diffused away by the error filter is high frequency or "blue noise." These features of error diffusion produce halftone images that are pleasant to human eyes with high visual quality.

III. ENCRYPTION OF SECRET IMAGE WITH COLOR IMAGES USING VC MATRICES (S_0,S_1) AND ERROR DIFFUSION

In this section, we describe the encryption method for color meaningful shares with a VIP synchronization and error diffusion. First, we

describe the VC matrix derivation method for VIP synchronization from a set of standard VC matrices. We then introduce an error diffusion process to produce the final shares. The halftone process is independently applied to each Red (R), Green (G), and Blue (B) color channel so each has only one bit per pixel to reveal colors of original images. A secret message is half toned ahead of the encryption stage.

3.1 Visual Pixel Synchronization

VIPs are pixels on the encrypted shares that have color values of the original images, which make the encrypted shares meaningful. In each of the m sub pixels of the encrypted share, there are ƛ number of VIPs, denoted as C_i and the remaining (m-ƛ) pixels deliver the message information of the secret message image. Here each sub pixel m carries visual information as well as message information, while other methods extra pixels are needed in addition to the pixel expansion to produce meaningful shares. Since each VIP is placed at the same bit position in sub pixels across the three color channels, VIP represents accurate colors of the original image

3.2 Flow Chart For Encryption of Secret Image

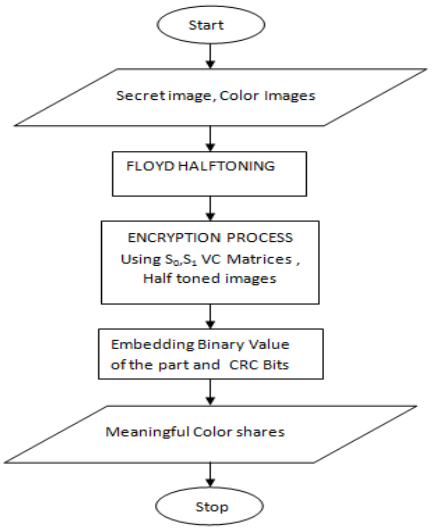


Fig 2 Flow Chart for Encryption of Secret Image

The Secret image and Color images are processed using half toning method and the leads to produce the half toned images.

$$X_{(p,q)}=\left[x^{R}_{(p,q)},x^{G}_{(p,q)},x^{B}_{(p,q)}\right] \in\{0,1\}^{3}$$

Here p, q lies in between ((1,k1),(1,k2)) respectively. here X that represents the pixel of the secrete image and p,q represents the location of the pixel. The 3 binary bits $x^{R}_{(p,q)}$, $x^{G}_{(p,q)}$, $x^{B}_{(p,q)}$ which represents the values for Red ,Green, Blue color channels respectively. each message pixel encrypted and expanded to sub pixel of length m and the encoded share i as

$X_{(p1\,,\,q1)}{}^{i}=[x^{R}_{(p1\,,\,q1)}, x^{G}_{(p1\,,\,q1)}, x^{B}_{(p1\,,q1)}]^{i}$ $\in \{S_0^{C1...Cn}[i], S_1^{C1...Cn}[i]\}^3$

where $1\le i\le n$; $p'= p.\, m_{-x}(m_x-1)$;

$q'= q.\, m_{-y}(m_y-1)$, $m= m_{-x}.\, m_{-y}$

m_{-x}, m_{-y} are non negative integers decide the aspect ratio encrypted color shares. the matrix $S_c^{c1...cn}[i]$ shows the i^{th} row of the matrix $S_c^{c1...cn}$. X is the image pixel and $X^{i}_{(p',q')}$ shows the corresponding pixel on the color channels position at (p', q') and the sub pixels takes one of the rows in $S_o^{c1...cn}$ or $S_1^{c1...cn}$ according to the bit value of corresponding message pixel color channel.

3.3 Share generation Via Error Diffusion

Using matrices S_0,S_1 processed across the all color channels after half toning algorithm is applied to generate the final encrypted shares.

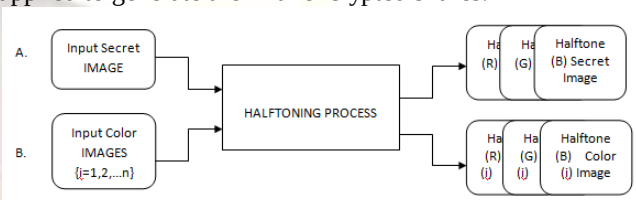


Fig. 3.3 Block Diagram to generate half toned Images

Fig. 3(a) shows a binary error diffusion diagram designed for our scheme. To produce the i^{th} halftone share, each of the three color layers are fed into the input. The process of generating halftone shares via error diffusion is similar to that shown in Fig.1 except that $F_{i,j}(m, n)$ is a (m, n) i^{th} pixel on the input channel $j(1\le i\le n, 1\le j\le 3)$ of i^{th} share.

Fig. 3(b) depicts this process. 1s and 0s in black are message information pixels that should not be modified and those are in red are VIPs that are already defined by the error diffusion. The C_i are also VIPs whose values are to be decided by referring the corresponding pixel values of original images and errors from neighboring pixels when the error filter window comes. Non C_i elements, however, still affect $d_{i,j}(m, n)$ and the quantization error $e_{i,j}(m, n)$ when they are calculated in the filter window. The non elements may increase quantization errors added to the shares, but in turn, these errors are diffused away to neighboring pixels. The visual quality of shares via error diffusion can be improved through edge enhancement methods. So the remedy for the apparent blurring of edges caused by the error diffusion algorithm is to apply an edge sharpening filter prior to half toning such that

$$X^{i}_{sharp}[n]=X[n]-\beta(\psi[n]*X[n])$$

Where X[n] stands for the original image, ψ[n] is a digital Laplacian filter, * denotes convolution and β is a scalar constant (β >0) regulating the amount of sharpening with larger β leading to a sharper image X^{i}_{sharp} Consequently, error diffusion produces high quality halftone

images.

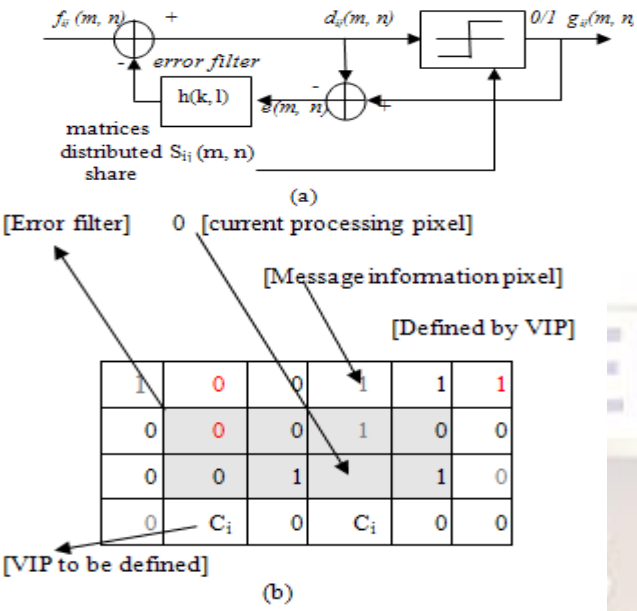


Fig. 3 (a) Block diagram of error diffusion with share encryption.
(b)Visualization of error diffusion with VIP

3.4 Adding binary information and CRC bits

The information will send from the source to destination via communication channel. in that process it might be chance of attack of the intruder whether he can change the information or misguide the people at the receivers side. so in order to protect from the security threats and detect the errors and to identify the shares to retransmit the shares from the source we added binary information which tells the secret information and to detect the error and for the authentication purpose we added CRC bits to the shares and transmitted to the destination through the communication channel.

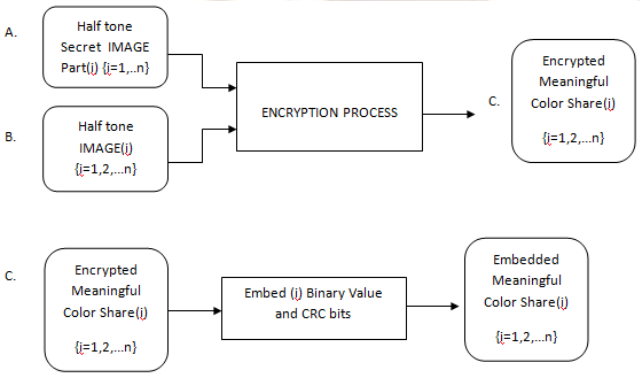


Fig. 3.4 Block Diagram for Encryption process and adding CRC bits

A represents the Secret image and B represents the Color Shares C shows the half toned Resultants. After generating the shares Binary Information and CRC bits added to the shares, which are extracted first and verified with key at receiver side.

3.5 CRC checking and Authentication Checking at the Receivers side

At the receivers side, all the shares are collected from the communication channel. through the secured channel the VC matrices S_0,S_1,key and the checker value will be received from the source. once the shares are collected at the receivers end it will processed in a reverse process of encryption . the binary information and crc bits were extracted first from the shares. using the key the crc bits were processed and the result which is equals to check value. if the result not equal to the check value that shows some error in the share and retransmission of the share is needed.

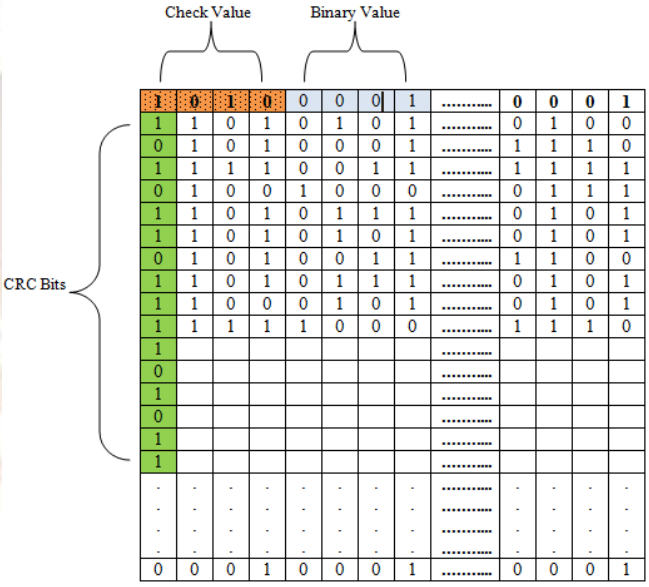


Fig 3.5 Color share values with binary information(0001) and CRC bits for R plane..similarly G and B.

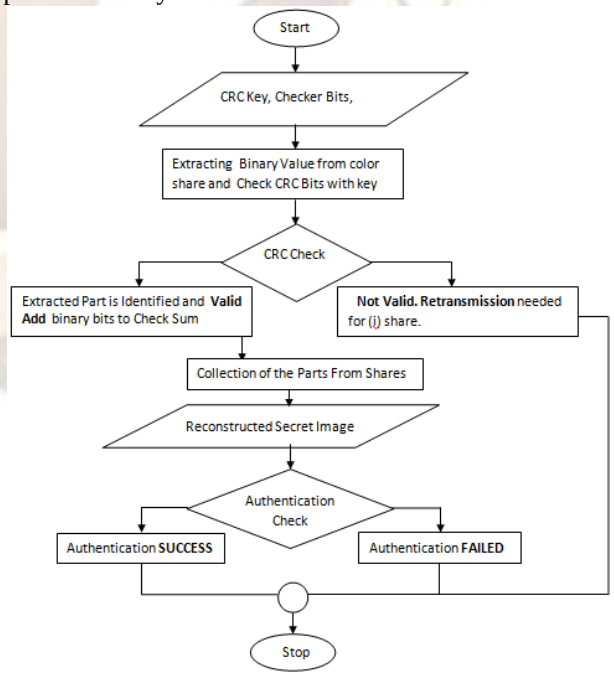


Fig 3.6 Flow Chart for CRC , Authentication checking at the receivers side.

If all the shares are verified with CRC checking key and then test for the Authentication checking. in each share the added binary information which represents by 8 bits, in that last 4 bits shows the part information that is order of the part of secret image. which helps to reconstruct the secret image from the shares at the destination side. And the first 4bits represents the authentication check bits. these check bits are collected from the shares according to the binary information in order and processed with the CRC key .if the result of the process and checker value is equal then Authentication Verified unless it shows that Authentication failed that means an attack of Intruder on the information.

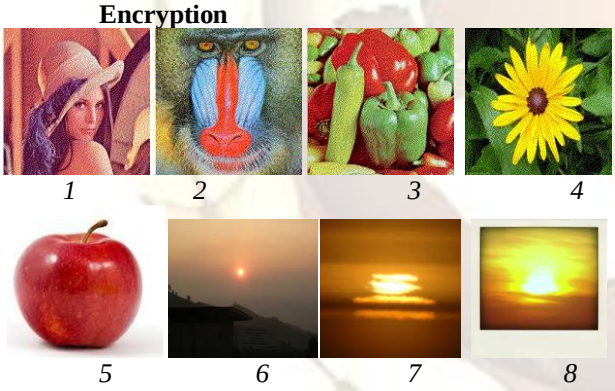
IV. SIMULATION RESULTS

This section presents the information regarding input secret image for encryption, meaningful shares or half toned shares used for encryption process and reconstructed image.

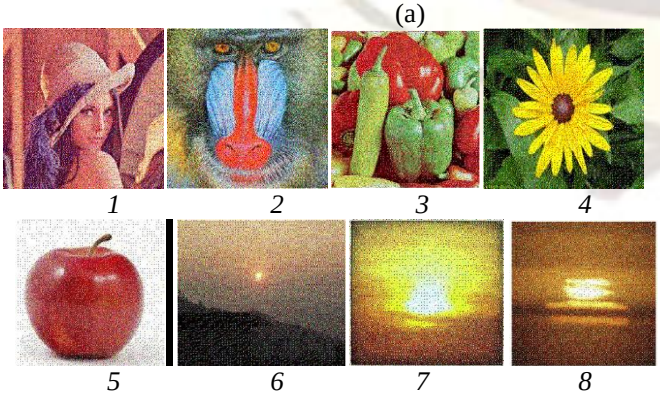
4.1 Original Secret Image for (n out of n) VCS

Fig:4.1 Secret Image

4.2 Colour Images for (n out of n) VCS for Encryption



(a)



(b)

Fig:4.2 (a) Actual Colour Images for Encryption Of SI
(b) After Encryption of SI the Meaningful Shares

4.3 Reconstructed Secret Image from meaning full Shares

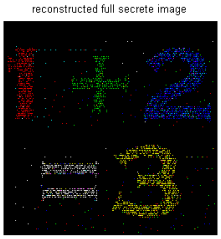


Fig:4.3 Reconstructed Secret image(8,8)VCS

TABLE I
COMPARISON OF (4,4) AND (8,8) COLOUR VC SCHEME

Images	(4,4)VCS	(8,8)VCS
1st Image(PSNR)	12.0650 dB	12.0650 dB
2nd Image(PSNR)	12.5358 dB	12.5358 dB
3rd Image(PSNR)	13.7786 dB	13.7786 dB
4th Image(PSNR)	15.7007 dB	15.7007 dB
5th Image(PSNR)	-	12.0378 dB
6th Image(PSNR)	-	12.5083 dB
7th Image(PSNR)	-	12.0778 dB
8th Image(PSNR)	-	12.5486 dB
Requirement for Encryption	Meaningful Shares	Meaningful Shares
No. of Shares Required for Decryption	All	All
Reconstructed Image PSNR	23.5705dB	25.4563dB
Mean Error	6.0383e+005	1.7202e+006
Quality & Clarity(by vision)	Good	High
Security	High	Very High
Computation Complexity	High	Very High
Hard ware Implementation	High	High

Fig: 4.1, The actual secret image which represents the confidential information that we want to send in secure way to the destination. Fig: 4.2 (a), The coloured images which plays the key role for the secure transmission of information. Fig: 4.3 (b), After applying to half toning the generated shares for the encryption of secret information .

Fig : 4.3, After the Half toning process the generated shares encrypted using VC matrices (S_0,S_1). that means the secret information is embedded into the shares which are called as meaning full shares. At the receiver side all the shares are collected and using the VC matrices S_0,S_1 the information is extracted from the meaning full shares. and thus forms the reconstructed secret image which showed in figure 4.3. from the figure 4 which shows that how binary values and crc bits embedded into color channels and at receiver side

the similar way the the information extracted first and checked with crc key. if the result checked successfully that means no error and identified the part of Secret image according the binary value. after that header bits (checker, from Fig:3.5) collected from the all shares and verify with CRC key ,if it shows that success Authentication proved unless need to retransmit the shares from the source.
The quality of the reconstructed image can be measured in different ways. Here the following table presents some quality measuring parameters using PSNR.

V. CONCLUSION

This paper develops an encryption method to construct color EVC scheme with VIP synchronization and error diffusion for visual quality improvement. VIPs synchronize the positions of pixels that carry visual information of original images across the color channels so as to retain the original pixel values the same before and after encryption. Error diffusion is used to construct the shares such that the noise introduced by the preset pixels is diffused away to neighbors when encrypted shares are generated. It is obvious that there is a tradeoff between contrast of encryption shares and the decryption share; however, we can recognize the colorful secret messages having even low contrast. Either VIP synchronization or error diffusion can be broadly used in many VC schemes for color images. In this paper has solved for the cryptanalysis which is helpful in security analysis of confidential information. As future work increase the no of share and range of CRC which leads to enhance the security level of the confidential information.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT , 1994, pp. 1–12.
[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.
[3] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography," in Proc. IEEE Int. Conf. Eng. Intell. Syst., 2006, pp. 1–5.
[4] M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in Proc. IEEE Int. Conf. Multimedia Expo, 2004, pp. 975–978.
[5] C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," Opt. Eng., vol. 44, p. 077003, 2005.
[6] M. Naor and B. Pinkas, "Visual authentication and identification," Adv. Cryptol., vol. 1294, pp. 322–336, 1997.
[7] W. Q. Y, J. Duo, and M. Kankanhalli, "Visual cryptography for print and scan applications," in Proc. IEEE Int. Symp. Circuits Syst., 2004, pp. 572–575.
[8] C. Blundo, P. D'Arco, A. D. S. , and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.
[9] L. A. MacPherson, "Gray level visual cryptography for general access structrue," M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000.
[10] C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett., vol. 75, no. 6, pp. 255–259, 2000.
[11] Inkoo Kang, Gonnzoalo R..Arce, Heun-Kyu Lee "Color Extened Visual Cryptography Using Error Diffusion" IEEE Trans, Image Process., vol. 20 No.1, pp.132-145,2011.
[12] D.s Wang, F.Yi, and X.Li,"On general construction for extended visual cryptography schemes" Pattern Recognit., pp.3071-3082,2009.
[13] M.Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images ," J WSCG vol. 10, no. 2, 2002.
[14] Z. Zhou, G. R Arce, and G. D. Crescenzo, " Halftone visual cryptography," IEEE Trans . Image Process., vol 18, no. 8,pp. 2441-2453,Aug.2006.
[15] C. N Yang, " A note on efficient color visual encryption," J. Inf. Sci.Eng., vol. 18, pp.367-372,2002.
[16] E. R.Verheul and H.C.A vanTilborg, "Construction and properties of k out of n visual secret sharing schemes, " Des. Codes Cryptogr., vol. 11, no. 2, pp. 179-196, May 1997.
[17] H. Koga and H. Yamamoto, " Proposal of a lattice based visual secret sharing scheme for color and gray –scale images, " IEICE Trans. Fundamentals, vol.E81-A, no. 06, pp. 1262-1269, Jun. 1998.
[18] C. N Yang and T.S . Chen, "Visual Cryptography .Scheme based on additive color mixing," Pattern Recognit., vol. 41, pp. 3114-3129,2008.