International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN : 2278-800X, www.ijerd.com
Volume 4, Issue 11 (November 2012), PP. 39-46

A Secure Visual Cryptography for Color Images

[1]K.Rashmitha, [2]Mr.G. Bhaskar, [3] Mr. Brahma Reddy,
[1]Assist. Professor, Dept of ECE, JNTUH, [2]PG Student, Dept of ECE, JNTUH
[3]Professor & HOD, JNTUH, ECE Dept, VBIT, Hyderabad

Abstract:-A visual cryptography scheme is a secret sharing scheme to encode a secret image SI in such a way that any qualified subset of participants can "visually" recover the secret image, while forbidden subsets have no information on SI. A "visual" recovery consists of xeroxing the shares, which are shadow images, onto transparencies and stacking them one on the top of the others. The participants in a qualified subset will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. Visual cryptography is a powerful tool for teaching cryptography to general audience. Applications have also been proposed to realize authentication, identification schemes and, recently, e voting schemes.

Index Terms:-Color meaningful shares, digital halftoning, error diffusion, secret sharing, visual cryptography (VC).

I. INTRODUCTION

Visual Cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir. In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into n shares of random binary patterns. The n shares are xeroxed onto n transparencies, respectively, and distributed amongst participants, one for each participant. No participant knows the share given to another participant. Any or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any k-1or fewer participants, even if infinite computational power is available to them.

VC scheme proposed by Naor and Shamir serves as a basic model and has been applied to many applications. Aside from the obvious applications to information hiding, there are many applications of VC, which include general access structures, copyright protection, watermarking, visual authentication and identification, print and scan applications, etc. 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 . Regardless of the value of the pixel, it is replaced by a set of four sub pixels, two of them black and two white. Thus, the subpixel set gives no clue as to the original value of p . When two subpixels originating from two white are superimposed, the decrypted subpixels have two white and two black pixels. On the other hand, a decrypted subpixel having four black pixels indicates that the subpixel came from two black pixels.

Several new methods for VC have been introduced recently in the literature. Blundo proposed an optimal contrast k-out-of-n scheme to alleviate the contrast loss problem in the reconstructed images. Ateniese proposed a more general method for VC scheme based upon general access structure. The access structure is a specification of qualified and forbidden subsets of shares. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The VC scheme concept has been extended to grayscale share images rather than binary image shares. Blundo proposed VC schemes with general access structures for grayscale share images. Hou transformed a gray-level image into halftone images and then applied binary VC schemes to generate grayscale shares. Although the secret image is grayscale, shares are still constructed by random binary patterns carrying visual information which may lead to suspicion of secret encryption.

Visual secret sharing for color images was introduced by Naor and Shamir based upon cover semigroups. 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 (yellow, magenta and cyan) 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.

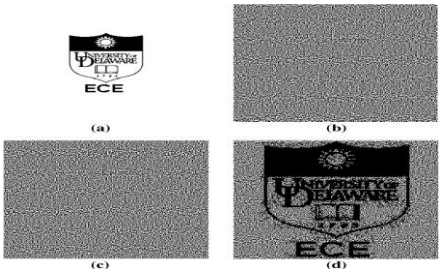


Figure :An Example of 2-out of-2 Scheme

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. Other approaches to color VC attempting to generate meaningful color shares include. These methods, however, produce shares with low visibility due to color inconsistency across color channels as discussed in the experiment section of this paper. Ching-Nung Yand and Tse-Shih Chen proposed a VCS for color images based upon an additive color mixing method . In this scheme, each pixel is expanded by a factor of three. We found that this scheme suffers from the problem of pixel expansion in the size of encrypted shares.

II. OUR APPROACH

In order to reduce the size of encrypted shares we propose the VC for color image using visual information pixel (VIP) synchronization with error diffusion technique. This VC for color image using visual information pixel (VIP) synchronization with error diffusion technique introduces a color VC encryption method which leads to 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 but 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, the colors of encrypted pixels and the contrast can be degraded due to random matrix permutation. Random matrix permutations are key security features in VC schemes. 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 subpixels which finally degrades the visual quality. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation.

III. VISUAL CRYPTOGRAPHY

Cryptography is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge — the art of encryption. In the past, cryptography helped ensure secrecy in important communications, such as those of spies, military leaders, and diplomats. In recent decades, the field of cryptography has expanded its remit in two ways. Firstly, it provides mechanisms for more than just keeping secrets: schemes like digital signatures and digital cash, for example. Secondly, cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications, and users are not aware of it.

The first visual cryptographic technique was pioneered by Moni Naor and Ad Shamir in1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares revealed no information about the original image. Visual Cryptography is a graphical form of information concealing. It can be seen as a cryptographic primitive, since it offers methods and technologies for building more complex information security systems.The techniques of visual cryptography are inspired from the general secret sharing schemes as presented by Adi Shamir and G.R. Blakley. The main difference between the visual and the general secret sharing schemes is that for the first ones the secret will be visually reconstructed in the decryption phase.

On special interest are the extended visual cryptography schemes for "natural images" – continuous tone gay images. In a two–out–of–two extended visual cryptography scheme, the two shares the secret image is split into are "innocent" images hiding the very intention of sending a secret message. Further contributions are made considering the applications of visual cryptography in e-commerce, especially for scenarios that involve the presence of a corrupt Post of Sale (POS).Being an one-time-pad method, visual cryptography is information-theoretically secure. That means, its security derives purely from the information theory. This aspect makes visual cryptography interesting since the security of the most actual cryptographic primitives is based on the difficulty of solving hard mathematical problems.

Steganography is the art and science of hiding the fact that communication is taking place. Using steganography, you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an "invisible" message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the Steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

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 random binary matrices S0 and S1 , 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 S0(S1) 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.

Definition 1*:* Let k, n and h be nonnegative integers satisfying 0<=k<=n and 0<=h<=m The two collections of n*m binary matrices S0 and S1 constitute a black and white (k, n)-VC scheme if there exists a value alpha(>0). satisfying the following.

Contrast: for any S belongs to S0 the OR operation k out of n of s is a vector v that satisfies w(v)<=h-alpha(m) where w(v) is the hamming weight of the vector v, m is the pixel expansion of the scheme and alpha is the contrast of the scheme.
Contrast: for any S belongs to S1 the OR operation of any k out of n of s is a vector v that satisfies w(v)>h.
The security of any i1<i2<……<in in {1,2,….,n} with t<k .The two collections of tRm matrices Di.j=0/1, obtained by restricting each n*m matrix in Si.j=0/1. To rows i1,i2,…,ii are indistinguishable in the sense that they contain the same matrices. In the previously mentioned definitions, the first two contrast conditions ensure that the stacking of k out of n shares can recovered the secret image. That means no matter what the secret message pixel is 0 or 1, the expected appearances of a restricted matrix Dj is same i.e, D0 and D1 are equal to a column permutation of the other in all possible ways.
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.

Extended VC:

Generally, a (k, 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:

- ❖ Any out of shares can 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 $c,c_1,c_2….c_n \in \{0,1\}$ for i=1,2,…..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.

IV. COLOR MODELS

The *additive* and *subtractive* color models 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. By mixing cyan, magenta and yellow pigments, we can produce a wide range of colors. 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. Cyan, magenta, and yellow 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 R(p,q) can be expressed in a binary form as

$R_{(p,q)} = R_{(p,q)}^{i}.2^{8-i}$ where {i=1,2,..,8}

denotes the binary vector at the ith bit-level with i=1 denoting the most significant bit.

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.

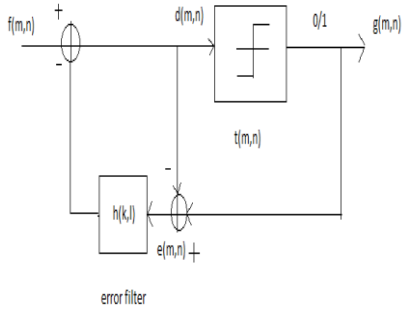


Figure : Error Diffusion Block Diagram

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

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

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)

$$d(m,n) = f(m,n) - \sum h(k,l)\, e(m-k,n-l)$$

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

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

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.

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 cyan (C), magenta (M), and yellow (Y) color channel so each has only one bit per pixel to reveal colors of original images. A secret message is halftoned ahead of the encryption stage.

Matrix Derivation With VIP Synchronization:

Our encryption method focuses on VIP synchronization across color channels. 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 subpixels of the encrypted share, there are λ number of VIPs, denoted as ci and the remaining (m-λ)pixels deliver the message information of the secret message image. Thus, in our method, each subpixel 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 subpixels across the three color channels, VIP represents accurate colors of the original image. First, we derive the basis matrices from a given set of matrices used in standard VC scheme. We first generates a set of basis matrices $S_c^{c1,c2,\ldots,cn}$ $(C,C_1,C_2,\ldots,C_n \in \{0,1\})$ where C is a bit pixel from the message image and $(C,C_1,C_2,\ldots,C_n)$ indicate the corresponding pixel bits from the original images. In each row of $S_c^{c1,c2,\ldots,cn}$ there are λ number of C_i and the values are unknown in the matrix derivation stage.

Halftoning then defines actual bit values of C_i by referring the pixel values of original images and errors diffused away. The $w(S_c[i])$ in the algorithem is a hamming weight of a "OR"-ed row vector up to th rows in $S_c^{c1,c2,\ldots,cn}$. It should be noted that the "OR"-ed row vector should not have any ci It should be noted that the "OR"-ed row vector should not have any cis are undefined values which can be defined as 0 or 1 in halftone stage, we cannot ensure the contrast difference between matrices $S_0^{c1,c2,\ldots,cn}$ and $S_1^{c1,c2,\ldots,cn}$

Distribution of Matrices Across Color Channels:

The encryption process starts with basis matrices distribution by referring secret message pixels. The encryption shares should be in a form of 3-b per pixel because they will be the results of the halftoned shares. Furthermore, the secret message of size K1*K2 should be halftoned ahead of the encryption stage as

$$R_{(p,q)} = [R_{(p,q)}^{C}, R_{(p,q)}^{M}, R_{(p,q)}^{Y}] \in \{0,1\}^3$$

Where $1 \le p \le K1$, $1 \le q \le K2$.$R_{(p,q)}$

is a pixel of the message image at location(p,q) composed of three binary bits $R_{(p,q)}^{C}$, $R_{(p,q)}^{M}$, $R_{(p,q)}^{Y}$ representing values for Cyan, Magenta and Yellow color channels, respectively. Each message pixel composed of 3 bits encoded and expanded to subpixels of length in the encrypted shares as

$$R_{(p,q)}^{i} = [R_{(p,q)}^{C}, R_{(p,q)}^{M}, R_{(p,q)}^{Y}] \in \{0,1\}^3$$

Where

$1 \le i \le n$

$P^1 = p.m_R - (m_R - 1)$

$q^1 = q.m_y - (m_y - 1)$

$m = m_R . m_y$

m_R and m_y are nonnegative integers and decide the aspect ratio of encryption shares. The $S_c^{c1,\,c2,\ldots.cn}[i]$ is the ith row of the matrix $S_c^{c1,\,c2,\ldots.cn}$ Each $R_{(p,q)}^{i}$ corresponds to subpixels on three channels starting at the position (p,q) and each subpixel takes one of the rows in $S_0^{c1,c2,\ldots,cn}$ or $S_1^{c1,c2,\ldots,cn}$ according to the bit value of the corresponding color channel of the message pixel.

This algorithm produces encryption shares Ri An example of the matrices distribution for (2, 2)-color EVC scheme is depicted in Fig.6. Fig. 6(a) shows the matrices distribution along with each message pixel. Each binary bit on three color channels of message pixel is expanded into four subpixels on corresponding color channels throughout the encryption shares by taking the matrix S_0 and S_1 according to its bit value. Since the VIPs are placed at the same spot on the ith row in matrices S_0 and S_1 each encrypted subpixels has the VIPs at the same positions throughout the color channels, where colored in gray in the figure.

This feature makes the shares carry accurate colors of the original image after encryption. Fig. 6(b) depicts a decryption mechanism by the unit of subpixels showing how they present the desired color of the original message pixel. Regardless of the VIP values which will be decided in the error diffusion stage, the decrypted subpixels reveal the color of the message pixel $R_{(p,q)}$ with 1/4 contrast loss. Since the matrices S_1 and S_0 with 1/4 contrast loss. Since the matrices are derived in a way that the contrast difference is alpha , the decrypted subpixels show the intended color of the message pixel with probability alpha .

Matrices Distribution:

The algorithm produces n matrix distributed Shares Ri The random permutation for S0 and S1 is done independently in standard VC schemes having one color channel. On the contrary, the random permutation of our scheme should be executed for $S_0^{c1,c2,\ldots,cn}$ and $S_1^{c1,c2,\ldots,cn}$ at the same time, denoted as $P(S_0^{c1,c2,\ldots,cn}, S_1^{c1,c2,\ldots,cn})$ since each row in the matrices has VIPs and their positions are correlated between $S_0^{c1,c2,\ldots,cn}$ and $S_1^{c1,c2,\ldots,cn}$ This feature should be reflected on the permutation process so as to preserve the VIP structure.

Procedure Matrices Distribution:

1.$(R, S_0^{c1,c2,\ldots,cn}, S_1^{c1,c2,\ldots,cn})$
2.For $1 \leq a \leq K1$, $1 \leq b \leq K2$ do
3. Find the starting pixel position on share R'
$A^1 = a.m_R - (m_a - 1)$
$B^1 = b.m_y - (m_b - 1)$
4.Conduct random column permutation,
$A(S_0^{c1,c2,\ldots,cn}, S_1^{c1,c2,\ldots,cn})$
5. For the color channel C $R_{(p,q)}^c$ do
6. If the bit $R_{(p,q)}^c$ then Place ith row of the $S_1^{c1,c2,\ldots,cn}$ to $[R_{(p,q)}^c]^i$ of the size m_R by m_y.
$[R_{(p,q)}^c]^i$ goes to the channel C of the ith share.
7. Else if the bit $R_{(p,q)}^c = 0$; then Place ith row of the $S_0^{c1,c2,\ldots,cn}$ to $[R_{(p,q)}^c]^i$ of the size m_R by m_y $[R_{(p,q)}^c]^i$ goes to the C channel of the ith share
8.End if
9. End for
10. Repeat 5 to 9 for the channel M and Y.
11. End for
12. End procedure

Share Generation via Error Diffusion:

Once the distribution of the basis matrices is completed, a halftoning algorithm is applied to produce the final encrypted shares. Error diffusion is used in our scheme as it is simple and effective. The quantization error at each pixel is filtered and fed back to future inputs. Fig 6.1 shows a binary error diffusion diagram designed for our scheme. To produce the ith 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.6.1 except that $f_{ij}(m,n)$ is a (m, n) th pixel on the input channel j($1 \leq i \leq n$, $1 \leq j \leq 3$) of ith share.

The other difference between our scheme from standard error diffusion is that the message information components, non , are predefined on the input shares such that they are not modified during the halftone process, i.e., the process is applied when the input is ci above Fig. 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 ci 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 ci elements, however, still affect $d_{ij}(m,n)$ and the quantization error $e_{ij}(m,n)$ 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 measure of a particular halftoning algorithm is its performance in DC regions and its performance near edges or in areas of high frequency image content can be manipulated through prefiltering the image prior to halftoning. So the remedy for the apparent blurring of edges caused by the error diffusion algorithm is to apply an edge sharpening filter prior to halftoning such that

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

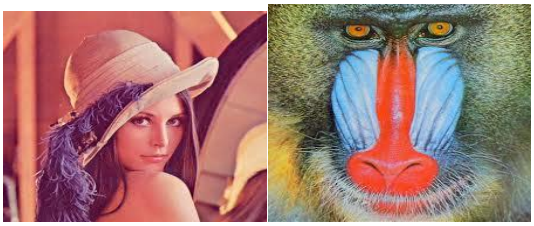
Where R[n] stands for the original image, ψ[n] is a digital Laplacian filter, * denotes convolution and β is a scalar constant ($\beta > 0$) regulating the amount of sharpening with larger β leading to a sharper image R_{sharp}^i Consequently, error diffusion produces high quality halftone images. The effectiveness of error diffusion can be confirmed in the simulation result section.

V. SIMULATION RESULTS

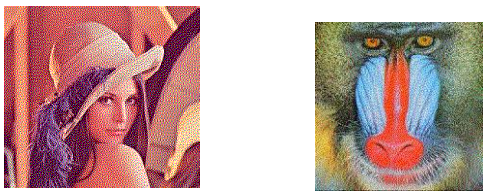
Results for 4 input -images:

Secret image :

4-Input Images:



4-Encrypted Shares:



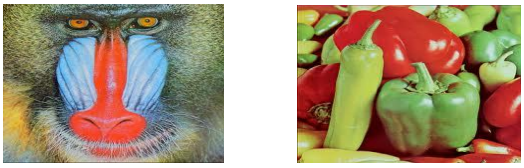
Decrypted Image:

PSNR for Resultant Image:
PSNR = 23.2748

Percieved ERROR for Resultant Image:
Perceived Error = $5.4527*10^5$

Results for 8-Input images:
Secret Image:

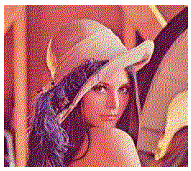
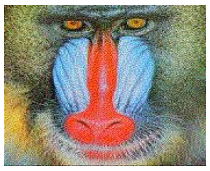
8-Input Images:



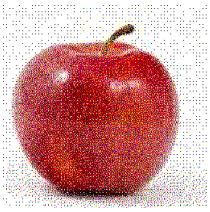
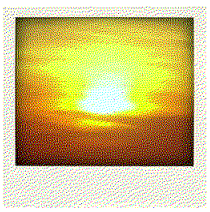




Encrypted shares:



Decrypted Image:

PSNR for Resultant Image:
PSNR= 20.6179
Percieved ERROR for Resultant Image:
Perceived Error = $6.1209*10^{5}$

VI. CONCLUSION AND FUTURE SCOPE

In this project we developed 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 where the noise introduced by the preset pixels are 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.

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 ERpo*, 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]. Y. T. Hsu and L. W. Chang, "A new construction algorithm of visual crytography for gray level images," in *Proc. IEEE Int. Symp. Circuit Syst.*, 2006, pp. 1430–1433.
[12]. C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, pp. 349–358,2003.
[13]. Y. C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, pp. 1619–1629, 2003.
[14]. G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *ACM Theor. Comput. Sci.*, vol. 250, pp. 143–161, 2001.
[15]. D. S.Wang, F. Yi, and R. Li, "On general consturction for extended visual cryptography schemes," *Pattern Recognit.*, pp. 3071–3082, 2009.