ISSN:0975-9646

A Novel Secured Transmission Of Color Extended Visual Images Using Error Diffusion

Srujan pentakota
M.Tech Student,
Dept of CSE, AIET

Maher Prasad
Asst. Professor,
Dept of CSE, AIET

Y.Ramesh kumar
Asst. Professor,
Dept of CSE, AIET

Abstract: Cryptography is the science of writing in secret code and is an ancient art. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.visual cryptography is a technique which allows visual information to be encrypted in such a way that the decryption can be performed by the human visual system. This paper introduces the concept of visual information pixel (VIP) synchronization and error diffusion with which high visual quality of images can be obtained. VIP synchronization retains the positions of pixels and error diffusion generates shares pleasant to human eyes. Basic visual cryptography is expansion of pixels. It uses two transparent images out of which one contains random pixels and the other contains secret information. Colour visual cryptography encrypts a colour secret message into n halftone image shares. It uses the additive and subtractive color models. Unlike the present system, it uses k-out of- n scheme in which any n shares can be present for the decryption. This system enhances the color quality of an image along with maintaining the security in the scheme. Presently a technique called watermarking is being used which means to make the data as small as possible. Now visual cryptography has been introduced as an extension to watermarking.

Keywords: watermarking, cryptography, visual cryption, VIP, encryption, decryption.

1. INTRODUCTION

Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir. In a k-outof- 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 n participants, one for each participant. No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any k - 1 or fewer participants, even if infinite computational power is available to them. Visual cryptography 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 visual cryptography, which include general access structures, copyright protection, watermarking, visual authentication and identification, print and scan applications, etc.

To illustrate basic principles of VC scheme, consider a simple (2,2)-VC scheme in which 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. Regardless of the value of the pixel p, it is replaced by a set of four sub pixels, two of them black and two white. When two sub pixels originating from two white p are superimposed, the decrypted sub pixels have two white and two black pixels. On the other hand, a decrypted sub pixel having four black pixels indicates that the sub pixel came from two black p pixels. Figure 2 shows an example of a simple (2; 2)-VC scheme with a set of sub pixels shown in Fig. 1. Figure 2(a) shows a secret binary message and Figure 2(b) depicts encrypted shares for two participants. Superimposing these two shares leads to the output secret message as the decoded image is clearly identified, although some contrast loss is observed.

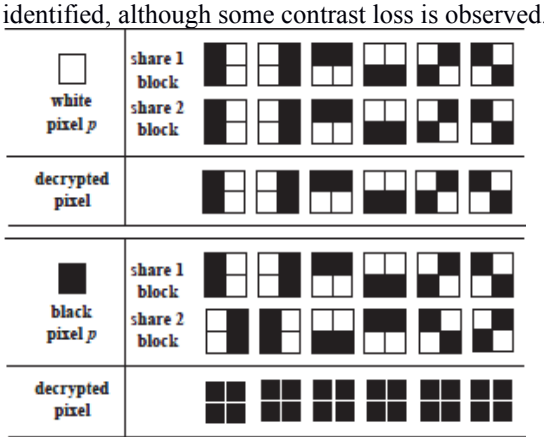


Fig 1: Construction of (2, 2) VC Scheme: A secret pixel is encoded into four sub pixels in each of two shares. The decrypted pixel is obtained by superimposing the blocks in shares one and two.

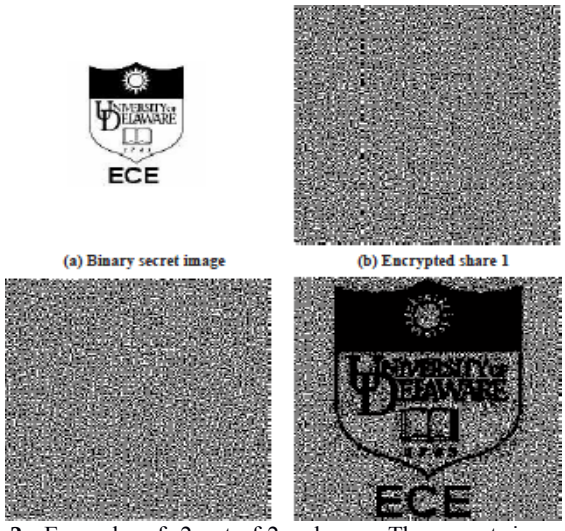


Fig 2: Example of 2-out-of-2 scheme. The secret image is encoded into two shares showing random patterns. The decoded image shows the secret image with 50% contrast less

Image cryptography contains two mechanisms those are **Encryption and Decryption of image**

In cryptography, **Encryption** is the process of encoding messages or information in such a way that only authorized parties can read it. In an encryption scheme, the message or information, referred to as plain-text, is encrypted using an encryption algorithm, turning it into an unreadable cipher text.

Decryption: It is the process of decoding the data which has been encrypted into a secret format. An authorized user can only decrypt data because decryption requires a secret key or password. In simple terms it is the conversion of cipher text into plain text .

The existing system makes use of only the black and white images i.e., the gray scale images. Presently, WATERMARKING technique is being used which makes use of the concept of STENOGRAPHY. Thus, it can be said that Visual cryptography is the extension of watermarking. Both Watermarking and Stegnography are related to HIDING of data where Stegnagraphy deals with completely hiding the information and watermarking deals with making the data as small as possible. The existing system makes use of k-out of- k scheme which means that the secret cannot be decoded by any *k* - 1 or fewer participants, even if infinite computational power is available to them. All the k participants or shares are needed to decode an image.

2. METHODOLOGY

The Proposed system 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 and the encryption method for color meaningful shares with a Visual Information Pixel (VIP) synchronization and error diffusion is well described here. It uses the additive and subtractive color models unlike the previous system. It mainly focuses on Cyan , Magenta and Yellow colors. An error diffusion process to produce the final shares is introduced at a later stage. This system enhances the color quality of an image along with maintaining the security in the scheme.

Algorithm 1:-which is used to concruct matrix with vip synchronization.

Procedure **MATRICES CONSTRUCTION** (S_0, S_1, λ)
Step 1: for i = 1, ..., n do
Step 2: for j = 1, ..., m do
Step 3: (a): set count = 0
Step 4: (b) : if $S_0[\ i_j\ ] = S_1[\ i_j\ ] = 0$ is found, then $S_0[\ i_j\ ]$ □ c_i and $S_1[\ i_j\ ]$ □ c_i and count = count + 1.
Step 5: goto (d) if i < k or goto (e) if i ≥ k.
Step 6: (c) : if $S_0[\ i_j\ ] = S_1[\ i_j\ ] = 0$ is not found, then switch element $S_0[\ i_{j1}\ ]$ and $S_0[\ i_{j2}\ ]$) ($j_1 \neq j_2$) or
Step 7: switch element $S_1[\ i_{j1}\ ]$ and $S_1[\ i_{j2}\ ]$) ($j_1 \neq j_2$), and goto (b).
Step 8: (d): if count = λ and i < k, then goto (a) with i increased by 1.
Step 9: (e): if count = λ and i ≥ k, then check if there exists α satisfying:

$$W(S_1[i]) - W(S_0[i]) \geq \alpha . M$$

if α exists, goto (a) with i increased by 1 until i reaches at n.

if α doesn't exist, undo all changes of i^{th} row and goto (c).
Step 10: end for
Step 11: end for
Step 12: end procedure

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 k out of n shares can recover the secret image.
- Any less than k shares cannot obtain any information of the secret image.

Algorithm 2:- which is used to matrix distrubution .

Step 1: Procedure **MATRICES DISTRIBUTION** (X, $S_0^{c1,...,cn}$, $S_1^{c1,...,cn}$)
Step 2: for p=1,...,k_1 and q=1,...,k_2 do
Step 3: find the starting pixel position on share X^i, $p`=p.m_x-(m_x-1)$, $q`=q-m_y-(m_y-1)$
Step 4: conduct random column permutation, P ($S_0^{c1,...,cn}$, $S_1^{c1,...,cn}$)
Step 5: for the color channel C of the secret message, $x^c_{(p,q)}$ do
Step 6: if the bit $x^c_{(p,q)}=1$, then place i^{th} row of $S_1^{c1,...,cn}$ to $[x^c_{(p`,q`)}]^i$ of size $m_x \times m_y$ and $[x^c_{(p`,q`)}]^i$ goes to the channel c of the i^{th} share
Step 7: else if the bit $x^c_{(p,q)}=0$, then place i^{th} row of $S_0^{c1,...,cn}$ to $[x^c_{(p`,q`)}]^i$ of size $m_x \times m_y$ and $[x^c_{(p`,q`)}]^i$ goes to the channel c of the i^{th} share
Step 8: end if
Step 9: end for
Step 10: Repeat steps 5 to 9 for the channel M and Y.
Step 11: end for
Step 12: end procedure

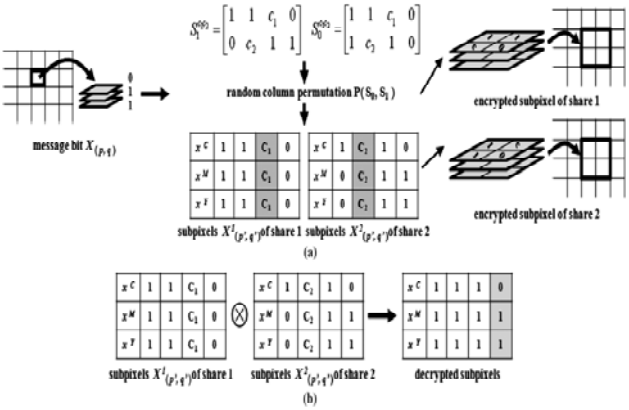


Figure3:matrix distribution.

General illustration of matrices distribution of (2, 2)-color EVC. (a) Matrices distribution along with a message pixel. Every message pixel composed of 3 bits encoded into four sub pixels for each color channel by referring the bit value on each channel of message bit. The positions of VIPs across color channels where colored in gray are preserved after encryption. (b) Decryption example of sub

pixels. Regardless of VIP values, the decrypted sub pixels represent the intended color, the same as that of the original message pixel, where colored in gray. The ⊗ represents the logical "OR" operation.

Error Diffusion:

Error diffusion is a simple yet efficient way to halftone a gray scale image. The quantization error at each pixel is filtered and fed into a set of future inputs. The following figure 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 is the output quantized pixel value. The output is given by:

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

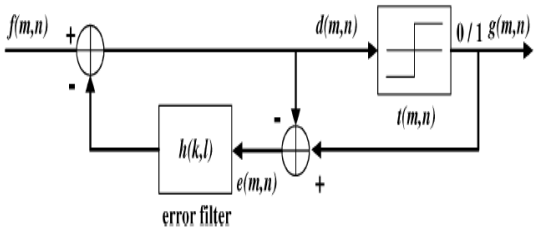


Figure4:Error diffusion block

Figure 4 shows Error diffusion block diagram. The pixel f (m, n) is passed through a quantizer to obtain the corresponding pixel g (m, n). The difference between these two,
e (m, n), is diffused away to the neighbouring pixels by the filter h (k, l). The threshold value t (m, n) determines g(m, n).

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.

Our paper contains three steps those are

- Initiates the process
- Algorithm generates shares and overlap with each other
- Show selected image

Initiates the process:

The process initiates by loading an image from the personal computer for the encryption and decryption process.. The image gets divided into shares called encryption . After overlying of shares we will get a decrypted image.

Algorithm generate shares and overlap with each other:

The matrix distribution algorithm generates shares and overlap with each other.

Color EVC Matrices Derivation:

Consider the basic matrices S_0 and S_1 of (2, 2) VC scheme with m = 4, λ = 1 such that:

$$S_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad S_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Let us assume λ be 1, and then the example given below generates the EVCS matrices VIP synchronized. The first row in each of the matrices S_1 and S_0 are (1100) and (1100). We begin by inserting the c_1s in the first row of each matrix as ($11c_10$) and ($11c_10$); the 0s at 3rd position in each row are replaced with c_1. with i = 2. For the second rows, the condition of $S_0[\ i_j\ ] = S_1[\ i_j\ ] = 0$ is not found. Switch the 2nd and the 3rd bits of S_1 by step leading (0101) for S_1. The condition $S_0[\ i_j\ ] = S_1[\ i_j\ ] = 0$ is found at 3rd position so replace them with c_2 resulting in ($01c_21$) for S_1 and ($11c_20$) for S_0). So far, we have matrices S_1^{c1c2} and S_0^{c1c2} as:

$$S_1^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 0 & 1 & c_2 & 1 \end{bmatrix}, \quad S_0^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 1 & 1 & c_2 & 0 \end{bmatrix}$$

Replace them with c_2 in both the matrices by (b), and then we have matrices s_1^{c1c2} and s_0^{c1c2} as:

$$S_1^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 0 & c_2 & 1 & 1 \end{bmatrix}, \quad S_0^{c_1c_2} = \begin{bmatrix} 1 & 1 & c_1 & 0 \\ 1 & c_2 & 1 & 0 \end{bmatrix}$$

'OR'- ed vectors are (1111) for s_1^{c1c2}, (1110) for s_0^{c1c2} and there exists the α =1/4 satisfying the contrast difference. The algorithm guarantees the placement of c_i at the same positions in i^{th} row of S_c^{c1c2} and the corresponding i^{th} rows of S_c^{c1c2} are used to encrypt an i^{th} share. Furthermore, each i^{th} row in S_0^{c1c2} and S_1^{c1c2} are used to encrypt bit 0 and 1 on each color channel of original images, respectively. Thus each encrypted sub pixel has the same VIP positions across three channels, which means that these sub pixels carry accurate visual information of the original images. In the example, sub pixels on three color channels of the first share have VIPs at the 3rd pixel and those of the second share have VIPs at the 2nd pixel throughout all channels. Consequently, VIP positions are synchronized across channels regardless of pixel colors and these results in high visual quality of the encrypted shares.

General illustration of matrices distribution of (2, 2)-color EVC. 3(a) Matrices distribution along with a message pixel. Every message pixel composed of 3 bits encoded into four sub pixels for each color channel by referring the bit value on each channel of message bit.The positions of VIPs across color channels where colored in gray are preserved after encryption. 3(b) Decryption example of sub pixels. Regardless of VIP values, the decrypted sub pixels represent the intended color, the same as that of the original message pixel, where colored in gray. The ⊗ represents the logical "OR" operation.

Show selected image:

The original image is displayed after the shares overlap with each other. This process is called

DECRYPTION. This scheme provides the user with enhanced visual color quality.

For encryption and decryption purpose used AES algorthhm.

Advanced Encryption Standard Algorithm (AES):

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S.National Institute of Standards and Technology (NIST) in 2001[8]

AES is a block cipher, but it does not use a Feistel structure. The block size of AES is 128-bit, but the key size may differ as 128, 192, or 256 bits [9].

Substitution: This method substitutes each byte of the block in the order of S-box. It provides an invertible transformation of blocks during encryption, with the reverse during decryption.

Shifting Rows: This operation performs left circular shifts of rows 1, 2, and 3 by 1, 2 and 3,

Mix Columns: This method multiplies each column of the input block with a matrix. The multiplication operation is just like matrix multiplication, except that it uses a Finite Field to multiply two elements and performs an XOR operation instead of addition.

Add Rounded Keys: This operation just applies an XOR operation to each byte of the input block and the current weight (key) matrix.

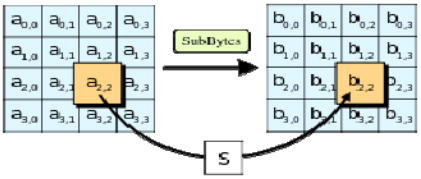
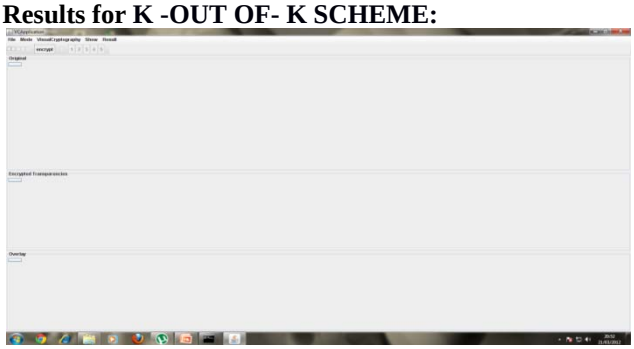
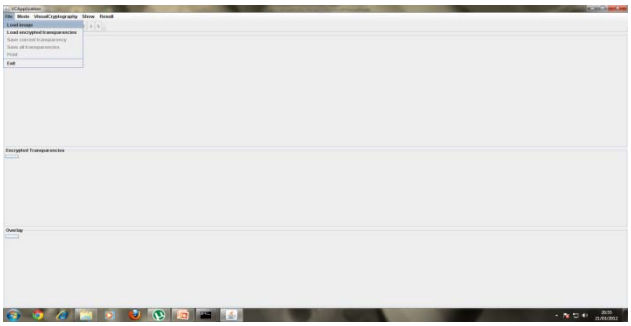


Figure2: the Sub-Bytes step, one of four stages in a round of AES

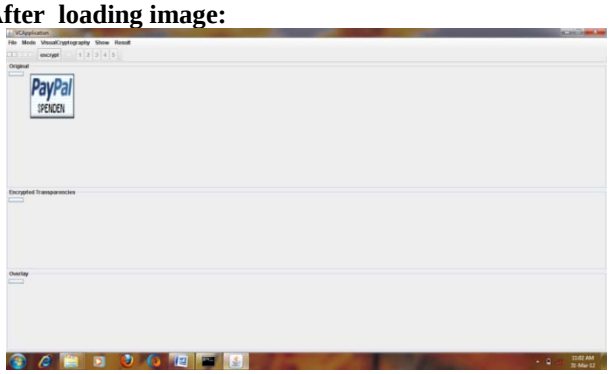
3. DATA ANALYSIS

Results for K -OUT OF- K SCHEME:

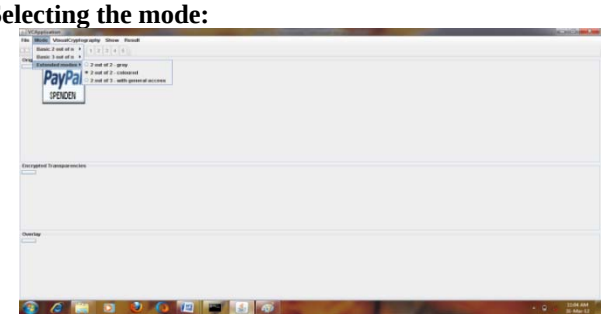




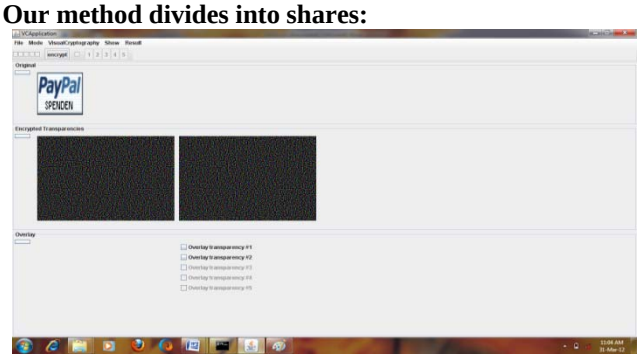
After loading image:



Selecting the mode:

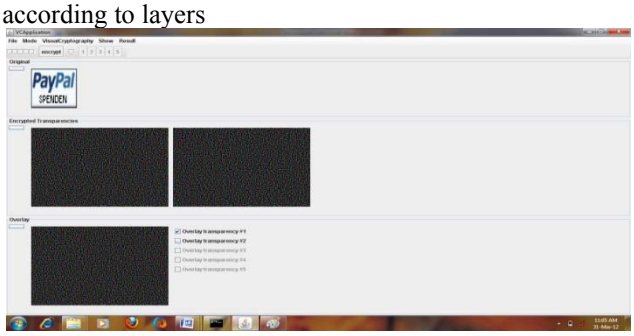


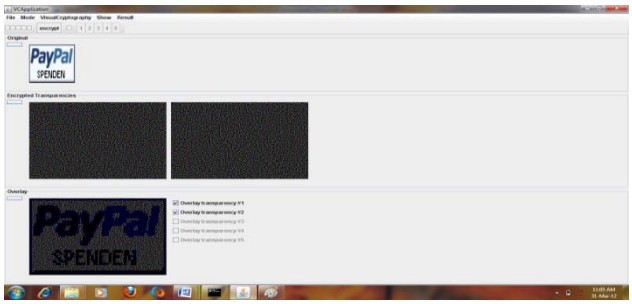
Our method divides into shares:



Over lay transperriences:

Over lay transperiences are shown in below figures according to layers

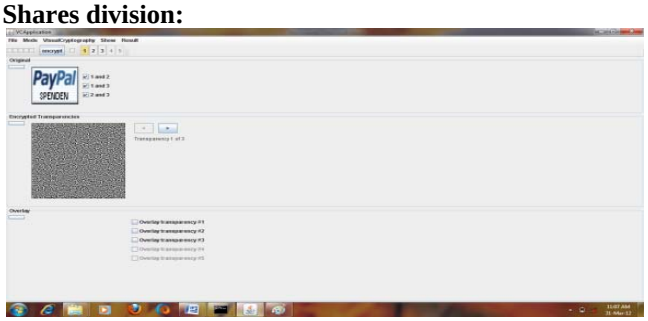




Results for K out of M:

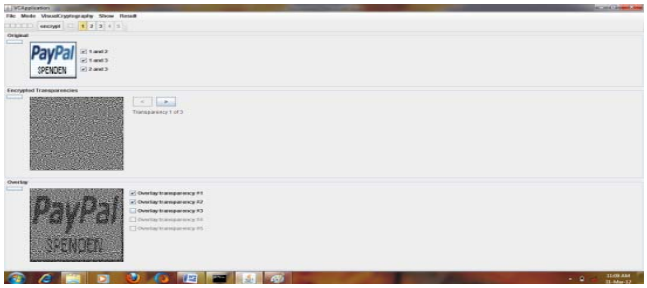
Selecting the shares:

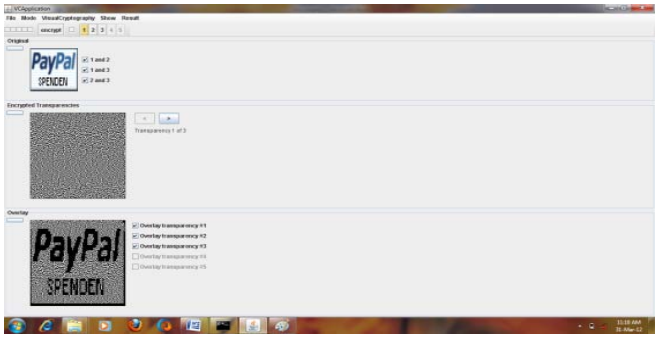
Shares division:



Over lay transperriences:

Over lay transperiences are shown in below figures according to layers





4.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 visual cryptography schemes for color images.

It is possible to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:

The color image visual cryptic filtering scheme can be used to maintain digital document trade marking.

Various multi-party security models are to combine at least some of the shares to form the original images.

Privacy preservation techniques (i.e., data transformation) can be considered for future enhancement.

REFERENCES

1. Color extended visual cryptography using error diffusion by inkoo kang,heung kyu loee
2. M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT '94*, 1994.
3. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, no. 2, pp. 86–106, 1996.
4. A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography," *Proc. IEEE Int. Conf. on Engineering of Intelligent Systems*, pp. 1–5, 2006.
5. M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking," in *Proc. IEEE International Conference on Multimedia and Expo*, 2004, pp. 975–978.
6. C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Optical Engineering*, 2005.
7. M. Naor and B. Pinkas, "Visual authentication and identification," *Advances in cryptology, LNCS*, vol. 1294, pp. 322–336, 1997