International Journal of Electronics and Communication Engineering (IJECE)
ISSN 2278-9901
Vol. 2, Issue 4, Sep 2013, 59-66

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AUTHENTICATION BY COLOR VISUAL CRYPTOGRAPHY USING VISUAL INFORMATION PIXEL SYNCHRONIZATION AND ERROR DIFFUSION

MRUNALI T. GEDAM & VINAY S. KAPSE

Rashtrasant Tukdoji Maharaj Nagpur University, Tulsiramji Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

Visual Cryptography is a technique which is used to secure the images. Our proposed system based on VIP synchronization and error diffusion technique is a color visual cryptography encryption method that produces meaningful color shares with high visual quality. The VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and Degradation of colors is avoided with the help of pixel synchronization. In Error diffusion the quantization error at each pixel level is filtered and fed as the input to the next pixel. In this way low frequency difference between the input and output image is minimized and give quality images. An experimental result shows that our proposed scheme shows better performance of proposed color image visual cryptography scheme measured in terms of PSNR value than existing scheme. The results showed that the noise effects such as blurring on the restoration of original image are removed.

KEYWORDS: Color Meaningful Shares, Digital Halftoning, Error Diffusion, Secret Sharing, Visual Cryptography (VC)

INTRODUCTION

With the coming era of the internet more and more multimedia data are transmitted and exchanged on the network system with rapid speed. In electronic commerce there is a need to solve the problem of ensuring information safety in today's increasingly open network environment. The encryption is a very important field in the present era in which information security is an important issue in communication and storage of images, the encrypting technologies of traditional cryptography are used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

There is a need of visual cryptography is encryption field helps to provide security on images and data such as confidentiality, entity authentication and data origin authentication. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms.

The basic principles of Visual Cryptography, each pixel of secret binary image are cryptographically encoded into m black and white sub-pixel in each share. If secret image pixel is white, encode with a set of four sub-pixels each sub-pixel has equal probability it contains two of them white and two of them black, thus, the sub-pixel set gives no clue as the original value of pixel. When a decrypted sub-pixel has two white and two black pixels indicate that the decoded pixel is a white. On the other hand a decrypted sub-pixel having four black pixels indicates that the decoded pixel is black.

RELATED WORK

Several new methods for VC have been introduced recently in the literature. Visual cryptography (VC) is a type of secret sharing scheme introduced by Naor and Shamir [1] presented a k-out-of-n scheme of visual cryptography, a secret binary image is encoded in to n shares and distributed amongst n participants, one for each participant. No participant knows the share given to another participant. By stacking the k shares decode the secret image. Less than k shares cannot be decoded by secret image. Ateniese [2] presented 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 of forbidden subset cannot recover secret image. M. S. Fu et. al. [3] Presented Joint visual cryptography and watermarking (JVW) algorithm. In this researcher paper they work on both watermarking and visual cryptography involve a hidden secret image. For visual cryptography secret image encoded into shares, more shares are required to decode the secret image. For watermarking secret image embedded into watermark halftone image.

C. S. Hsu et. at. [4] Presented research work visual cryptography and sampling method used for digital images copyright protection. This method can register multiple secret images without altering the host image and can identify the rightful ownership without resorting to the original image. Chang-Chou Lin et. al. [5] presented visual cryptography for gray level images by dithering techniques. Instead of using gray sub-pixels directly to constructed shares, a dithering technique is used to convert gray level images into binary images and a visual cryptography method for binary images is then applied to the resulting dither image. M. Nakajima et. al. [6] developed extended visual cryptography for natural images constructs meaningful binary images as shares.

This will encode secrets image more securely in to a shares and also describes the contrast enhancement method to improve the quality of the output images. Zhou et. al. [7] Presented halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel ‘p’ is encoded into an array of Q1 X Q2 (‘m’ in basic model) sub pixels, referred to as halftone cell, in each of the ‘n’ shares. by using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

Plataniotis, et.at.[8] Presented Colour image secret sharing The method operates in the decomposed bit-levels of the input colour vectors to change both spatial and spectral correlation characteristics of the share outputs and produce random, colour-noise-like images for secure transmission and access. The decryption process satisfies the perfect reconstruction property and recovers the original colour image by logically decrypting the decomposed bit vector-arrays of the colour shares.

THE PROPOSED APPROACH

VIP Synchronization

In this section, we describe the encryption method for color meaningful shares with VIP synchronization. The secret color message is cryptographically encoded into original cover images; this encryption process is called shares. By using VIP synchronization generating meaningful shares image. We describe the VC matrix derivation method for VIP synchronization from a set of standard VC matrices

Matrix Derivation with VIP Synchronization

Our encryption method focuses on VIP synchronization across color channels and error diffusion. 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 is s number of VIPs, denoted as ci and the remaining (m-s) 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 sub-pixels across the three color channels, VIP represents accurate colors of the original cover image.

VIP synchronization matrices generation process is:

In given basis matrices S0 and S1 of (2, 2)-VCS with m = 4, r= 2 and a given s = 1:

In m sub-pixels of the encrypted share, there is s number of VIPs, denoted as ci and r number of message information pixel.

$$S0 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad 1= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

The first row in each of the matrices S0 and S1 are (1100) and (1100). We begin by inserting the c1 in the first row of each matrix as ($11C_10$) and ($11C_10$). That is, the 0s at the third position in each row is replaced with C_1.

For the second rows in S0/S1 matrices 0 is not found in the same position then switch the first and last bits of S1 leading (1010)then replace 0 with C2 resulting in($1C_210$) for S0 and ($0C_211$) for S1. So far we have matrices $S_1^{c1c2}$and S_0^{c1c2} as:

$$S_0^{c1c2} = \begin{pmatrix} 1 & 1 & c1 & 0 \\ 1 & C2 & 1 & 0 \end{pmatrix} \; S_1^{c1c2}= \begin{pmatrix} 1 & 1 & c1 & 0 \\ 0 & C2 & 1 & 1 \end{pmatrix}$$

The 'OR' row vectors in S0 gives (1110); however that of S1 produces (1111). These two matrices are distributed across the color channel of secret message image.

If secret image pixel is 0 encode with S_0^{c1c2} matrices sub-pixel and if secret image pixel is 1 encode with S_1^{c1c2} matrices sub-pixel and generate two encrypted share images.

$$S1= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad S0= \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

The first row in each of the matrices S1 & S0 are (1100) and (1100). We begin by inserting the C1's in the first row of each matrix as (1 1 C1 0) and (1 1 C1 0) the 0s at third position in each row is replaced with C1.

$$S1^{c1,c2} = \begin{pmatrix} 1 & 1 & c1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad S0^{c1,c2} = \begin{pmatrix} 1 & 1 & c1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

For the second rows, the condition of S0 & S1 is 0 not found then Switch the second and the third bits of s1. The condition S0 &S1 is 0 found at third position and replace them with C2 resulting in (0 C2 1 1) for S1 and (1 C2 1 0) for S0 the matrices $S1^{c1,c2}$ and $S0^{c1,c2}$ as:

$$S1^{c1,c2} = \begin{pmatrix} 1 & 1 & c1 & 0 \\ 0 & c2 & 1 & 1 \end{pmatrix} \quad S0^{c1,c2} = \begin{pmatrix} 1 & 1 & c1 & 0 \\ 1 & c2 & 1 & 0 \end{pmatrix}$$

If secret image pixel is 0 encode with S_0^{c1c2} matrices sub-pixel and if secret image pixel is 1 encode with S_1^{c1c2} matrices sub-pixel and generate two encrypted share images.

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 halftone ahead of the encryption stage as:

$$I(p,q)=[IC(p,q), IM(p,q), IY(p,q)] \in \{0,1\}^3 \quad (1)$$

Where, $1 \le p \le k1$, $1 \le q \le k1$ is a pixel of the message image at location(p,q) composed of three binary bits $xC(p,q), xM(p,q), xY(p,q)$ representing values for Cyan, Magenta and yellow color channels. Each message pixel composed of 3 b is encoded and expanded to sub-pixels of length *m* in the encrypted shares *i* as

$$I^i(p',q') = \in \{S0^{c1,\dots cn}[i], S1^{c1,\dots cn}[i]\}3 \quad (2)$$

Each $I^i(p',q')$ corresponds to subpixels on three channels starting at the position (p',q') and each subpixel takes one of the rows in $S0^{c1,\dots cn}$ or $S1^{c1,\dots cn}$ according to the bit value of the corresponding color channel of the message pixel.

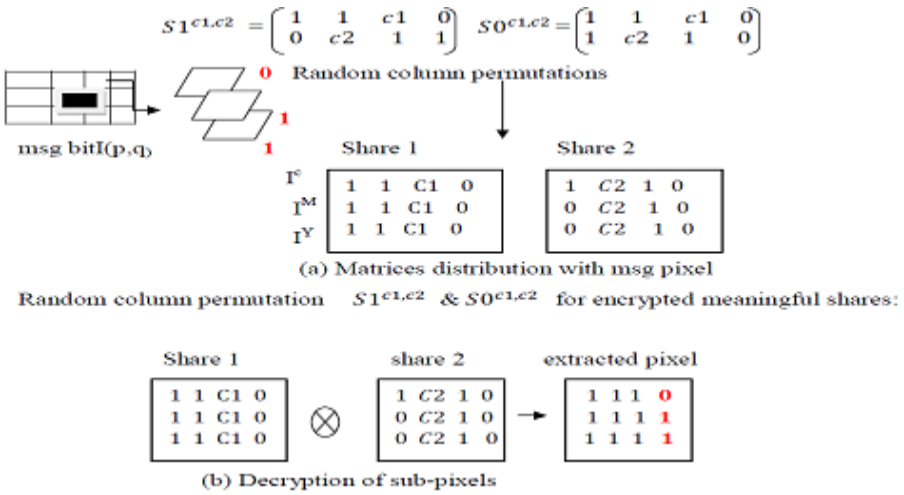

Figure 1: Matrices Distribution of (2, 2)-Color EVC

Figure 1(a) shows the matrices distribution along with each message pixel. Each binary bit on three color channels of message pixel is expanded into four sub-pixels on corresponding color channels throughout the encryption shares by taking the matrix $S0^{c1,c2}$, $S1^{c1,c2}$ Since the VIPs are placed at the same spot on the ith row in matrices $S0^{c1,c2}$ and $S1^{c1,c2}$, each encrypted subpixels has the VIPs at the same positions throughout the color channels, where colored in red in the figure. This feature makes the shares carry accurate colors of the original image after encryption. Figure 1(b) depicts a decryption mechanism by the unit of sub-pixels showing how they present the desired color of the original message pixel. Decrypted sub-pixels represent the intended color, the same as that of the original message pixel, where colored in red.

Share Generation via Error Diffusion

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. Fig2.Shows a binary error diffusion diagram designed for our scheme. To produce the *i*-th halftone share, each of the three color layers is fed into the input. Let *fij*(*m*, *n*) be the (*m*, *n*)-th pixel on the input channel *j* ($1 \le i \le n$, $1 \le j \le 3$)) of i^{th} share.

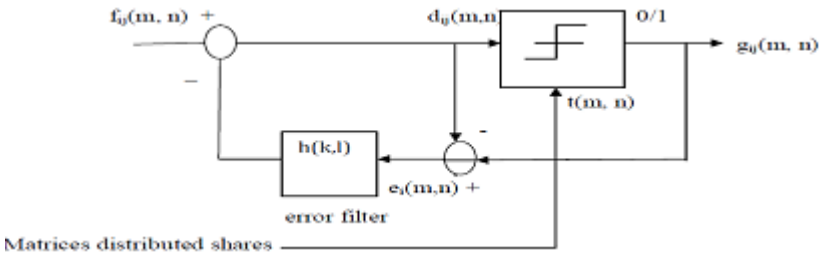

Figure 2: Error Diffusion

The input to the threshold quantization is:

$$g_{ij}(m,n) = \begin{cases} 1 \text{ , if } d_{ij}(m,n) \geq t_{ij}(m,n) \\ 0, \text{ Otherwise} \end{cases}$$

$d_{ij}(m,n)$ is the sum of input pixel value and diffused error, $g_{ij}(m,n)$ is the output quantized pixel value and $t_{ij}(m,n)$ is the threshold be position dependent.

$$dij(m,n) = fij(m,n) - \sum_{k,l} h\,(k,l)eij(m-k,n-l) \tag{3}$$

Where $h(k, l) \in H$ and H is a two dimensional error filter. The $eij(m, n)$ is a difference between $dij(m, n)$ and $gij(m, n)$. The $gij(m, n)$ is a quantized output pixel value given by :

The recursive structure of the block diagram indicates that the quantization error $eij(m, n)$ depends on not only a current input and output but also the entire past history. The error filter minimizes low frequency differences between the input and output images and consequently it produces pleasing halftone images to human vision. In this process of generating halftone shares via error diffusion is that the message information components, are predefined on the input shares such that they are not modified during the halftone process. After applying the error diffusion on share, generate final encrypted meaningful shares are pleasant to human eyes with high visual quality.

RESULTS AND DISCUSSIONS

The experimental simulation is conducted by using the image processing software package (MATLAB). The color image is stored in MATLAB as an M- by- N by 3 data array that defines Red, Green, Blue (cyan, magenta, and yellow respectively) color components for every individual pixel. The color of each and every pixel is defined by the combination of the Red, Green, Blue (cyan, magenta, and yellow respectively) intensities stored in each color plane at the pixel's location. I provide some experimental results to illustrate the effectiveness of the proposed method. The Original color images are ‘Lena’, ‘Baboon’, and ‘Pepper’ of size 256 × 256 in natural colors is provided for the share generation.

(a) Secret Message Image **(b) Input Baboon Image** **(c) Input Pepper Image**

(d) Output Baboon Image **(e) Output Pepper Image** **(f) Extracted Secret Image**

Figure: 3. Experimental Results of Proposed Scheme

(a) input encrypted share image of baboon (b) input encrypted share image of pepper (d) output share image baboon with error diffusion (f) output share image pepper with the error diffusion. PSNR: (d) PSNR= 31.6884 (e) PSNR= 30.4964

Table 1: Result Analysis of Proposed Scheme

Sr. No.	Color Shares with Error Diffusion	Existing Method PSNR	Proposed Method PSNR	Proposed Method MSE
1	Lena	10.83 dB	30.8174 dB	53.8692
2	baboon	10.84 dB	31.6884 dB	44.0798
3	Pepper	11.23 dB	30.4964 dB	41.6542
4	flower	11.23 dB	31.9342 dB	58.002

CONCLUSIONS

I concluded that to improve the quality of encrypted share images. I have to use encryption method to construct color visual cryptography Scheme with VIP synchronization and error diffusion for visual quality improvement. In this process I have to encode the secret image using VIP synchronization matrices and generate encrypted color shares, then I apply error diffusion on encrypted share and generate meaningful color share with high visual quality images pleasant to human vision.

In experimental result of our proposed scheme, I have taken different images and calculate their PSNR. I conclude that the peak-signal-noise ratio of encrypted share image with error diffusion of our proposed scheme are better performance than existing scheme and also remove the noise effect such as blurring on share images are removed as a result more clarity on restoration of original share images.

In the future, I will more improve the quality of share images by removing noising effect completely that help to reduce error rate and increase peak-signal-noise ratio. It also used in biometric application in which I will hide thumb in our face image and then generate meaningful encrypted shares, when two shares are created, one is stored in the Bank database and the other is kept by the customer. For all transactions customer has to present his share. This meaningful encrypted share is stacked with the first share to get the original thumb image that help to authenticate the customer.

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. M. S. Fu and O. C. Au, "Joint visual cryptography and watermarking,"in *Proc. IEEE Int. Conf. Multimedia Expo*, 2004, pp. 975–978.
4. 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.
5. 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.
6. M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG*, vol. 10, no. 2, 2002.
7. 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.
8. R. Lukac and K. N. Plataniotis, "Colour image secret sharing," *Electron. Lett.*, vol. 40, no. 9, pp. 529–531, Apr. 2004.
9. E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in *Proc. IEEE Int. Conf. Image Process.*, 2006, pp. 97–100.
10. Y. C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, pp. 1619–1629, 2003
11. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4 pp 383–396, Sep. 2009.
12. C.M. Hu and W.G. Tzeng, "Cheating Prevention in Visual Cryptography," *IEEE Transactions on Image Processing*, Vol. 16, No. 1, pp. 36-45, 2007.