International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 02 Issue 01 | 2014

COLOR EXTENDED OPTICAL CRYPTOGRAPHY USING RANDOM SHARES FOR VISUAL TRANSFERRING SCHEME

Veena Hemke[1], Ranjana Shende[2]
Department of Computer Science & Engineering,
G.H.R.I.E.T.W., Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, India

ABSTRACT

The paper proposes a work on color extended optical cryptography using random shares, having ability of hiding of securing confidential data without mounting the pixels. optical cryptography scheme allows encoding of secret image into 'n' shares which are distributed to the participants for providing safety against hacker and sight, in this less than n cannot recover the secret image. previous method in the literature shows good result for black and white or gray level image, however they are not sufficient to applied to color image due to different color structure. some method for color optical cryptography are not satisfactory because they are expanding the image exponentially .and making the size of image double,in terms of meanigfull share with low visual quality. The new method overcome with the previous method and generates pleasent shares.

keywords- Visual cryptography, visual secrete sharing, shares, participants

I. INTRODUCTION

It is common to transfer digital data via internet .with the coming generation of of electronic commerce, there is an urgent need to solve the problem of data security in today's network environment. In this paper for developing the security of shares in visual cryptography and generating more meaningful shares with respect to minimum pixel expansion and cryptographic scheme. To prevent integrity digital contents from being intercepted by unauthorized parties is a critical demand in information security. With the increasing demand of the internet, which makes possible the access or distribution of digital database, such a demand becomes even more significant in security aspect. Even with the so much growth of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example a place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Traditional cryptographic skills recommend plenty of solutions by encrypting the digital data into a cipher text that cannot be recognized by illegal intruders. Yet the decryption of the protected ciphertext needs mechanical computations. Basically visual cryptography is used for the encryption of visual information like written data, textual picture, and handwritten data, print material and scanned Databases, etc. In a perfectly secure way so that the decryption can be performed by the human visual system, without use of mechanical computations.

Visual cryptography is one of the best known techniques to protect data .It is the art of sending and receiving secret messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. We can achieve this by one of the following access structure schemes.

1.(2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that gies the secret image only when they are stacked. No additional information is required to create this kind of access structure.

2.(2,n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two(or more) of the shares are stacked the secret image is disclose. The user will be prompted for n, the number of participants.

3.(n,n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be disclose. The user will be prompted for n, the number of participants.

4.(k,n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are stacked the secret image will be revealed.

The use of the colour visual cryptography is that now a day's majority of the people more often used the colour images and interact with them more frequently. Natural colour image can be used to share secrets; this provides a very helpful cover for unsuspicious hiding the fact that any encryption has taken place at all.

II. EARLIER WORK

It is the best known techniques to secure data. It is the technique of sending and receiving scrambled messages that can be decrypted only by the sender or the receiver. Encryption and decryption are done by using mathematical recursive algorithms in such a way that no one but the authorized recipient can decode and read the message. Naor and Shamir [1] proposed the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of the image among multiple participants. The summary points of Naor and Shamir's scheme are

- The confidential data can be divided into n parts.
- Any k or more than k parts can decode the scrambled data
- Any k -1 or fewer than k parts cannot decode the information.

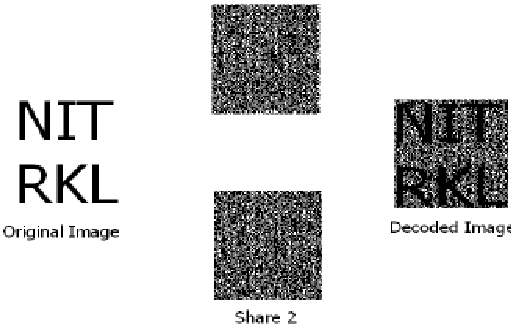

Fig 1: Working model for visual cryptography developed by naor and Shamir

Each pixel of image 'I' is represented by 'm' sub-pixels in each of the 'n' shared images. The resulting structure of each shared image is described by Boolean matrix 'S' Where S=[Sij] an [n x m] matrix Sij=1 if the jth sub pixel in the ith share is black Sij=0 if the jth sub pixel in the ith share is White When the shares are stacked together secret image can be seen but the size is increased by 'm'times. the disadvantage of this process is that the decryption becomes 'lossy'.

2.1 Extended visual cryptography

Giusppe, Atenies, Carlo Blundo,Alfred De Santis and Douglas R.Stinson[2,3] address the extended capabilities for visual cryptography. extended visual cryptography takes the idea of visual cryptography further by creating shares which are meaningfull to everyone who views them.

2.1.1 Half tone visual cryptography

The meaningful shares generated in Extended visual cryptography proposed by Mizuho Nakagima and Yasushi Yamguchi[4,5] was of poor quality which again increases the suspicion of data encryption process. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the shares and meaningful . In halftone visual cryptography using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and the Security of the meaningful transparencies or shares.

2.1.2 Cheating immune visual cryptography system

Yang and Laih presented two type of cheating prevention ,one type is used to online trust authority to perform verification between participants. The second type involved changing visual cryptography scheme whereby stacking the two share reveals the verication image. Another cheating prevention scheme described by Horng, whereby attacker knows an exact distribution of black and white pixel of each share of honest participants they will able to attack and cheat the scheme, so for that they developed method for prevents the attacker from obtaining this distribution.

2.2 Dynamic visual cryptography

The core idea behind the dynamic visual cryptography is to increase the overall capacity of the visual cryptography system. This means that using 2 shares, we can potentially hide 2 or more secrets. Multiple secret sharing is useful when it comes for hiding more than 1 piece of information within a set of shares. Basic multiple secret sharing problem 1st addressed by wu and chin [6] in that they concealed two secrets within two set of shares within s1 and s2. The 1st secret is revealed when s1 and s2 are staked. The second become available when s1 rotated anticlockwise and superimposed with s2.due to nature of angle required for revealing the secrets (90^0 18^0,or 27^0) and the fact that scheme can share at most 2 secrets it becomes apparent that it is quite limited in use.

2.3 Colour visual cryptography

The researches in visual cryptography leads to the degradation in the quality of the decoded binary and gray scale images, which makes it inefficient for protection of colour image .F. Liu,C.K. Wu X.J. Lin proposed a new approach on visual cryptography for coloured images. They proposed following approaches as follows:

- The first approach to realize colour visual cryptography scheme is to print the colours in the
- secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded colour image.
- The second approach converts a colour image into black and white images on the three colour channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white visual cryptography scheme to each of the colour channels. This results in decrease of pixel expansion or more no of pixel but reduces the quality of the image due to halftone process.
- The third approach utilizes the binary Representation of the colour of a pixel and encodes the secret image at the bit-level. This results in better quality but requires devices for decoding process.

2.4 Progressive Visual cryptograph

Progressive visual cryptography takes into consideration the premise of the perfect secret recovery and high quality secret reconstruction. The annoying presence of loss of the contrast makes traditional visual cryptography scheme practical only when the quality is not issue which is relatively rare.

2.4.1 **Halftones based gray scale and colour visual cryptography**

The use of the digital halftoning is for the purpose of converting gray scale image into monochrome or binary image. Once we have a binary or monochrone image, then the original visual cryptography technique can be applied. For colour image, there are 2 alternatives for applying digital halftoning. One is two split the colour image into channel of cyan, maganta, and yellow. Then each channel is treated as gray scale image to which halftoning and visual cryptography is applied one by one on each share without considering the working of other shares. After the monochrome shares are generated for each channel, channels are combined separately to create the separate shares. this is the approach presented in [7]. The alternative approach would be directly apply colour halftoning then perform the separation into colour channel followed by the application of visual cryptography to each channel independently.

2.4.2 **Visual cryptography with perfect restoration**

The application of digital halftoning technique result in some downgrading of original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. in this method a new encoding method which allow to transform gray scale image and colour image into digital without loss of any information.

III. PROPOSED WORK

As protecting digital data in the network securely is one of the challenges in any informational system. Here visual cryptography technique is applied for the hiding the confidential data in the system. In this system there are two modules: encoding module and decoding module. The overall process of encryption phase consists of several steps which are explained as follows. In this colour image is converted into cym(canny, yellow, and maganta) channel format. On each of the channel images colour error diffusion technique is applied. The respective channel images are divided into n number of transparencies, with any m number of transparencies the encoded data can be perfectly reconstructed and without complete knowledge of m-1 shares reveals no information about the original image. [9] [10]. The share is obtained by using random grids. Random grid is defined as a transparency comprising a n-dimensional array of fully transparent or totally opaque pixel, with the n types of pixel are equally like to occur. So with the help of random grids size of the pixel remain same. The shares obtained after random grids are enveloped in the innocent covers using invisible digital technique.

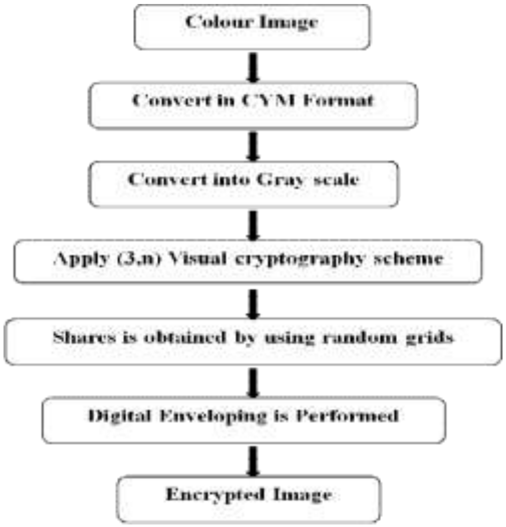
Colour Image
Convert in CYM Format
Convert into Gray scale
Apply (3,n) Visual cryptography scheme
Shares is obtained by using random grids
Digital Enveloping is Performed
Encrypted Image

Fig 2: Encryption process for digital data

The decryption process is the opposite process of the encryption process. In the decryption process the shares are superimposed together and the n×k block is sub sampled in such a way that it is converted into a single pixel and the size of the decrypted image is same as the original image.

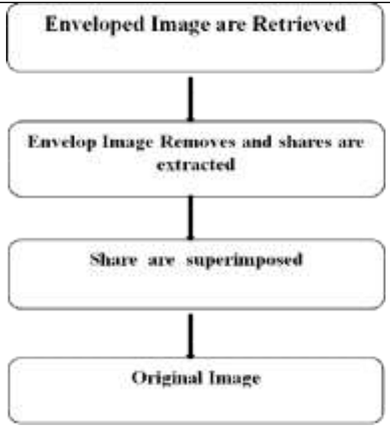
Enveloped Image are Retrieved
Envelop Image Removes and shares are extracted
Share are superimposed
Original Image

Fig 3: Decryption process

IV. SIMULATION RESULTS

In this section, we provide some experimental results to illustrate the effectiveness of the proposed method.

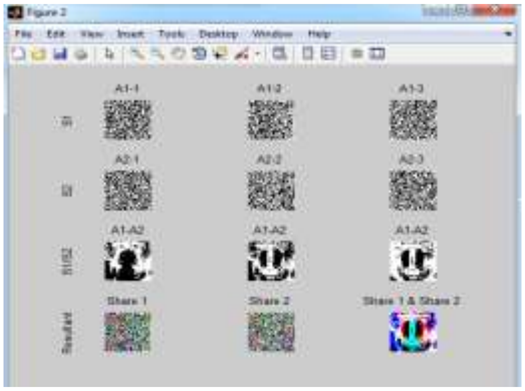

Fig. Color extended visual cryptography output

V. CONCLUSION

The feasibility and applicability of these algorithms are sound in the visual sense.In this A2 or A3, achieves the better light contrasts for the qualified sets" depends on the access structure given (i.e., some favor A2, while others prefer A3); nevertheless, for any access structure, A2 may deliver different light contrasts for different qualified sets, while A3 produces a constant one.The light transmissions of the encoded shares by either A2 or A3 may be different; and different participants in A3 may receive the same share, while those in A2 obtain distinct ones.The extensions of A2 and A3 are capable of dealing with the sharing of a color image.

REFERENCES

[1] M.Naor and A. Shamir "Visual cryptography". Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995

[2]G.Ateniese,C.Blundo,A.DeSantis,D.R.Stinson, visual cryptography for general Access structures,Proc.ICALP96,Springer,Berlin,1996,pp.416-428

[3]G.Ateniese,C.Blundo,A.DeSantis,D.R.Stinson,extended capabilites for visual cryptography theoretical computer science,250(1-2) 143-161,2001

[4] Chang-Chou Lin , Wen-Hsiang Tsai, Visual cryptography for gray-level images by dithering techniques

[5]Nakajima, M. and Yamaguchi, Y., Extended visual cryptography for natural images. Journal of WSCG. v10 i2. 303-310

[6] C.C Wu and L.H.Chen. A study of visual cryptography, master's thesis Institute of computer and information science ,national chiao tung university,Taiwan R.O.C.,1998.

[7] Y.C.Hou, C.Y.Chang, and S.F.Tu. Visual cryptography for color images based on Halftone technology,in International Conference on Information System, Analysis and Synthesis world Multiconference on Systemics Cybernetics and Informatics.Image,Acoustic,Speech and Signal Processing: Part II ,2001

[8] Email Praun, Fugus Hoppe, Matthew webb, and Adam Finkelstein. Real time Hatching. In Siggraph 01: Proceding of the 28th Annual Conference on Computer Graphics and Interactive Techniques, Pages 579-584, New York, NY,USA,2001.ACM

[9]C.N. Yang, C.S. Laih, New colored visual secret sharing Scheme, Design, codes and cryptography, vol. 20, pp.325-335, 2000.

[10] P. Ranjan, "Principles of Multimedia", Tata McGraw Hill, 2006. 8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inform. Comput., vol. 129, no. 2, pp. 86–106, 1996.

[11] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," Theor. Comput. Sci., vol. 369, nos. 1–3, pp. 169–182, 2006.

[12] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.

[13] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptology, vol. 12, no. 4, pp. 261–289, 1999.

[14] M. Bose and R. Mukerjee, "Optimal (k, n) visual cryptographic schemes for general k" Designs Codes Cryptography, vol. 55, no. 1, pp. 19–35, 2010.

[15] S. J. Shyu and K. Chen, "Visual multiple secrets sharing by circle random grids," SIAM J. Imaging Sci., vol. 3, no. 4, pp. 926–953, 2010.