Volume 2, Issue 3, March 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing Images Using Colour Visual Cryptography and Wavelets

Sagar Kumar Nerella*
Department of CSIT, JIIT,Noida(U.P),INDIA
sagarkumarnerella@gmail.com

Kamalendra Varma Gadi
Department of CSIT JIIT,Noida(U.P),INDIA

RajaSekhar Chaganti
Department of ECE, JIIT,Noida(U.P),INDIA

Abstract— **Visual Cryptography is a new Cryptography technique which is used to secure the images. In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share images gets the image. The initial model developed only for the bi-level or binary images or monochrome images. Later it was advanced to suit for the Colour Images means Gray Images and RGB/CMY Images. For the RGB/CMY Images different methods are developed based on the colour decomposition techniques. In this paper we propose a new way of performing colour visual cryptography using wavelet technique. Wavelet technique is used to convert the Colour Image to Gray Image. The important feature of the Visual Cryptography is decryption doesn't require any computer and it requires less computational power.**

Keywords— **Image Security, Visual Cryptography, Secret Sharing Schemes, Digital Halftoning, Error Diffusion, Wavelet, Antonini 9/7 Filter.**

I. INTRODUCTION

The field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

In order to transmit secret images to other people, a variety of encryption schemes have been proposed. Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For an example, consider a bank vault that must be opened everyday by five tellers, but for security purposes it is desirable not to entrust any two individuals with the combination. Hence, a vault-access system that requires any three of the five tellers may be desirable. In this situation the traditional cryptography systems fail because they need to authenticate the five tellers or 3 of them at a time using single key. This was solved by the Secret Sharing Scheme proposed by the Adi Shamir in 1979. It refers to method for distributing a secret amongst a group of participant's, each of whom is allocated a share of the secret. The secret can be reconstructed only when sufficient number of shares is combined together; individual shares are of no use on their own.

In Secret Sharing Scheme, both the sharing phase and the reconstruction phase involve algorithms that are run by computers (specially, a dealer runs a distribution algorithm and a set of qualified parties can run a reconstruction algorithm). In Visual Secret Sharing Scheme, the decryption phase needs no computer power but it has all the properties of Secret Sharing Schemes.

Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

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.

This technique is called as (k,n) VCS model where k represents the minimum no. of shares needed to decrypt the

secret image(image which is to be secured) and n represents the no of shares generated by the scheme.

Rest of the paper is organized as follows: Section-II contains the various Image Encryption Methods. Section-III gives the detailed description of the Visual Cryptography model given by Noar and Shamir. Section-IV gives the description of the Visual Cryptography applied for gray images and colour Images. Section –V describes our model for encrypting colour images using the Wavelet theory under the Visual Cryptography model of Noar and Shamir.

II. IMAGE ENCRYPTION TECHNIQUES

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. Technique for Image Encryption using Digital Signatures

Aloka Sinha and Kehar Singh have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

B. Image Encryption using SCAN

S.S. Maniccam and N.G. Bourbakis have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. The drawback of the algorithm is that it takes long time to encrypt.

C. New Encryption Algorithm for CryptoSystems

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen use one of the popular image compression techniques, vector quantization to design an efficient cryptosystem for images. The scheme is based on vector quantization (VQ), cryptography, and other number theorems. In VQ, the images are first decomposed into vectors and then sequentially encoded vector by vector. Then traditional cryptosystems from commercial applications can be used.

D. Mirror Like Image Encryption Algorithm

Jiun-In Guo and Jui-Cheng Yen have presented an efficient mirror-like image encryption algorithm. Based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm consists of 7 steps. Step-1 determines a 1-D chaotic system and its initial point x(0) and sets k = 0. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates binary sequence from chaotic system. Steps-4,5,6, and 7 rearrange image pixels using swap function according to the binary sequence. But no authentication scheme was there.

E. New Chaotic Image Encryption Algorithm

Jui-Cheng Yen and Jiun-In Guo have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point x(0), row size M and column size N of the image f, iteration number no, and μ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels. But no authentication scheme was there.

F. Double Random Phase Encoding

Shuqun Zhang and Mohammad A. Karim have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multi-channels methods.

III. VISUAL CRYPTOGRAPHY[2]

We proceed by first describing the (2,2) VCS model and after words the generalized model with its definitions and properties.

In VCS the secret image which to be shared secretly is divided into parts called shares. Dividing into parts exactly mean each and every pixel of the secret image is copied in to share images in a combination of m number of black and white pixel combinations. This is called dividing the image into parts to from share images and the process is called pixel expansion. Dividing/copying a pixel into share images as a combination of black and white pixels is called sharing a pixel.

The person who divides the secret image into shares and distributes them among participants is called dealer.

A. (2,2) VCS Model

In (2,2) VCS the first 2 represents the minimum no. of share images needed to recover a secret image. The second 2 represents the total no .of share images produced.

The VCS model is dependent on the basis matrix which forms the entire model. In linear algebra basis is a set of linearly independent vectors, can represent every vector in the vector space. The entire model of (2,2) VCS can be described

by tow basis matrices one for a black pixel and one for a white pixel. The basis matrices of (2,2) VCS are:

$$B1=\begin{matrix}1 & 0\\ 0 & 1\end{matrix} \text{ and } B0=\begin{matrix}1 & 0\\ 1 & 0\end{matrix}$$

In a basis matrix element 1 means the presence of a black pixel in the share image generated from this matrix and element 0 means the presence of a white pixel. The rows of a basis matrix correspond to the share images and describe how the pixel in secret image is divided in share image. For example consider the pixel to be shared is black pixel, and then the dealer takes the B1 basis matrix and examines the rows. For the share1 image he copies the black pixel as a combination of black pixel and white pixel as in 1st row of B1 matrix. For the share2 image he copies black pixel as a white and black pixel combination as in 2nd row of the B1 matrix. In the same way for the white pixel ,share1 image gets the pixel as in 1st row of B0 matrix and share2 image gets the pixel as in 2nd row of B0 matrix.

To produce the random output we permute the basis matrices to form a set of permuted basis matrices. The permuted basis matrices are

$$C1=\{\begin{matrix}1 & 0\\ 0 & 1\end{matrix},\ \begin{matrix}0 & 1\\ 1 & 0\end{matrix}\} \text{ and } C0=\{\begin{matrix}1 & 0\\ 1 & 0\end{matrix},\ \begin{matrix}0 & 1\\ 0 & 1\end{matrix}\}$$

So to share a black pixel dealer chooses randomly one of the matrixes from set C1 and copies/shares the pixels according to the rows of the selected matrix. In the same way for the white pixel also, dealer chooses a matrix from set C0 and copies/shares the pixels according to the rows of the matrix.

As described earlier in VCS model to recover/decrypt the secret there is no need of computing power. Take printout of the share images generated on to a transparency and overlapping transparencies will get the secret image. This is possible because of the basis matrix structure used and the decryption process is a simple Boolean-or operation performed by our human visual system not by the computer. This decryption is possible because of the Basis matrix structures used. Assume to share a black pixel we have chosen the first matrix of set C1, so share1 gets the pixel as 1 0 and share2 gets the pixel as 0 1. When we overlap them on one another Boolean-or operation is done by the human visual system, so the Boolean-or of the vector 1 0 with the vector 0 1 produces the vector 1 1 means two black pixels. In the same way for a white pixel say we chosen the first matrix of set C0 so share1 gets the pixels 1 0 and share2 gets the pixel as 1 0 the overlapped result i.e Boolean-or ,is the vector 1 0 i.e as a combination of black and white pixel. Since we are coping single pixel as a combination of two pixels the pixel expansion of the scheme is two. Since the overlapped result of the black pixel results two black pixels and the overlapped result of the white pixel results as one black pixel and one white pixel, the resulting image looks more darker which is due to loss of the contrast (loss of white pixels). The contrast of the scheme is ½.

B. General Description/Definition of VCS

VCS assumes the secret image consists of a black and white pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares) as a combination of m black and white pixels. The pixels in each share are printed in a very close proximity to each other the individual contribution is averaged by the human visual system. The entire structure is defined by a nxm Boolean matrix S= $[s_{ij}]$ where $s_{ij}=1$ if jth sub-pixel in ith share /transparency is black. When all the shares are overlapped/stacked together in a way which properly aligns the subpixels we see a combined share whose black pixels are represented by the Boolean or of the rows $i_1,i_2, ...i_n$ in S. The grey level of the combined share is given by the Hamming Weight H (V) of the or ed m-vector V. This grey level is interpreted by human visual system as black if H (V) as black if H (V) >= d and as white if H (V) < d- αm for some fixed threshold $1 \le d \le m$ and relative difference $\alpha > 0$.

Definition of the VCS Model:

Solution to the K out of N visual secret sharing scheme consists of two collections of nxm Boolean Matrices C0 and C1. To share a white pixel dealer randomly chooses one of the Boolean matrices from C0 and to share a black pixel the dealer chooses randomly one of the matrices from set C1. The chosen matrix defines the color of the m subpixels in each of the shares. The solution is considered valid only if the following conditions are met:

1. For any S in C0, the "or" of V of any k of the n rows satisfies H (V) < d- αm
2. For any S in C1, the "or" of V of any K of the n rows satisfies H (V) >= d
3. For any subset {i1,i2,..in} of {1,2,...n} with q<k, the two collections of matrices Dt for t ϵ {0,1} obtained by restricting the each nxm matrix in Ct (where t=0,1) to rows i1,i2,..iq are indistinguishable.

Condition 3 ensures the security of the system i.e. inspecting fewer than k shares will not provide any information regarding the secret image. But k or more than k shares will be able to recover the secret image successfully.

C. Properties of VCS model

1) Pixel Expansion (m)
   a) The number of pixels in a share. This represents the loss in resolution from the original picture to the shared one.
2) Contrast (α)
   a) The relative difference in weight between combined shares that come from a white and black pixel in the original picture. This represents the loss of contrast.
3) Size of the Collections C1 and C0
   a) Represents the number of matrices in the collections C1 and C0. They need not be same but in most cases it is.

D. Limitations of Initial VCS Model

The initial model described above is applicable only for the black and white images (or) monochrome images (or) 1-bit depth images. So several methods are proposed on how to adopt the VCS model for Colour Images i.e. gray colour and full RGB/CMY colour images.

IV. VISUAL CRYPTOGRAPHY FOR GREY COLOUR IMAGES

As described earlier in the section-III the initial VC model is not applicable for the Gray and Colour Images. Several proposals were made for both the gray and colour images. For the gray colour images the techniques is Digital Half toning. In Digital Half toning the techniques used are Error-Diffusion Filters, Random Dithering, Ordered Dithering, Direct Binary Search, Blue Noise Mask Dithering etc. Among all the Error-Diffusion filter approach performs faster and produces good results acceptable as produced by the Direct Binary Search.

In our model we have adopted the Error-Diffusion Approach for Applying VC to Gray colour images.

A. *Digital Half toning*

Halftone is the reprographic technique that simulates continuous tone imagery through the use of dots, varying either in size, in shape or in spacing. "Halftone" can also be used to refer specifically to the image that is produced by this process. Where continuous tone imagery contains an infinite range of colours or greys, the halftone process reduces visual reproductions to a binary image that is printed with only one colour of ink. This binary reproduction relies on a basic optical illusion—that these tiny halftone dots are blended into smooth tones by the human eye. At a microscopic level, developed black-and-white photographic film also consists of only two colours, and not an infinite range of continuous tones.

Digital Half toning is producing halftone image from a continuous tone image using halftone algorithms through computer. In our method we adopted the Error Diffusion technique developed by Floyd described below.

B. *Floyd Error-Diffusion Filter*

The Floyd-Steinberg dithering algorithm[5] is based on error dispersion. The error dispersion technique is very simple to describe: for each point in the image, first find the closest color available. Calculate the difference between the value in the image and the color you have. Now divide up these error values and distribute them over the neighboring pixels which you have not visited yet. When you get to these later pixels, just add the errors distributed from the earlier ones, clip the values to the allowed range if needed, then continue as above. For the gray scale to monochrome conversion the closest colour available is given by simple thresholding operation.

The Diffusion filter used is:

$$\text{Filter} = \begin{matrix} & * & 7 \\ 3 & 5 & 1 \end{matrix}$$

'*' indicates the current pixel we are processing. After obtaining the closest colour value, calculate the error value by comparing the value with the original value of the pixel and the difference is obtained to the neighbouring as a fraction indicated by the element in the filter. The next pixel to the current pixels will get 7/16 of the error value and the pixel below it gets the 5/16 of the error value likewise for the rest of the neighbouring pixels the error is distributed.

The result of applying Error-Diffusion filter on Figure2 is shown in Figure 3.

Fig 1.Lena Colour Image

Fig 2.Lena Gray Image generated from Colour Lena Image by the Wavelet Technique.

Fig 3 Halftone Image Generated from the Gray Image using Floyd Diffusion Filter.

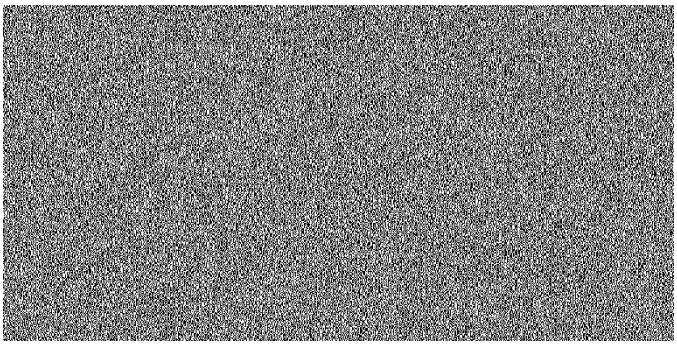

Fig 4.Share 1 Generated from the Figure3 under the (2,2) VCS model

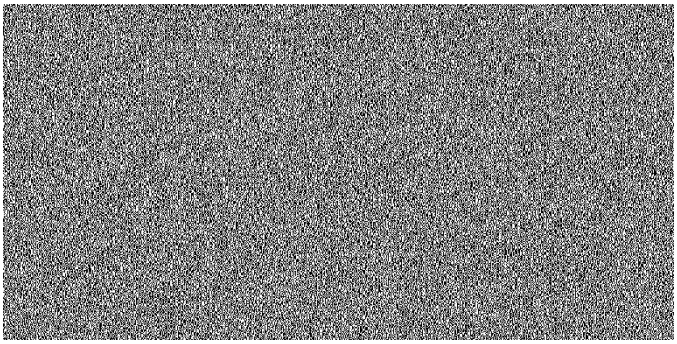

Fig 5.Share 2 Generated from the Figure3 under the (2,2) VCS Model.

Fig 6.Recovered Secret Image obtained by Stacking the Share1 and Share2 Images.

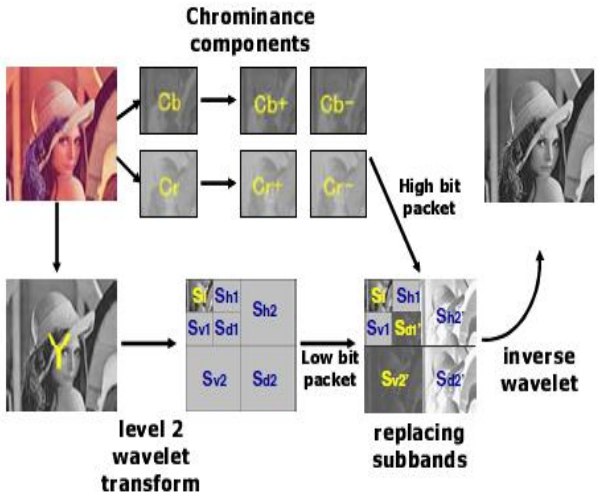

Fig 7.Figure Showing the Generation of Gray Image from the Colour Image using Wavelet Technique.

V. VISUAL CRYPTOGRAPHY FOR COLOUR IMAGES

As described earlier the VCS model is not applicable for the colour images. Several algorithms were proposed Ref [3], [4], [8] to apply VCS model for Colour Images. They are based on the approach of colour channel decomposition generating the 3-gray versions of the colour images. Later on applies the Diffusion Filters to get the Halftone images and then applies the VC on them and combines the result in a way producing the colour halftone images.

A. *Proposed Wavelet Model:*

The Approach we used in our method is different from the existing ones in a way that we have used the Wavelet Technique[1] to convert the Colour Image to Generate the Gray Colour Image which is the Intensity Image formed from the YC_bC_r Colour Space.

The process of generation of gray image from a colour image using wavelet technique is shown in Fig 7.

The Wavelet Filter used is Antonini 9/7 filter.

The Encryption Process can be described in Steps as Follows:

1. Convert the RGB Image to YCbCr Image.

2. Apply the two level discrete wavelet transform on the Y image so that it gets divided in to seven bands.
   Y-->(s_1,s_{h1},s_{v1},s_{d1},s_{h2},s_{v2},s_{d2})
3. Reduce Cb and Cr by ½, construct Cb+,Cb-,Cr+,Cr- and reduce Cb- further to ¼ of its original size.
   Where Cb+ is Cb if Cb >0 otherwise 0
   Cb- is Cb if Cb<0 otherwise 0
   Same arrangement for Cr also.
4. Replace Subbands
   Sd1←Cb-,Sh2←Cr+,Sv2←Cb+,Sd2←Cr-
5. Take inverse wavelet transform to obtain the grey image.
   (Sl,Sh,Sv,Cb-,Cr+,Cb+,Cr-)→ Y' is the grey image
6. Apply Error-Diffusion Filter on the obtained grey image Y'.
7. Apply the VCS Model on the generated halftone image from step6.
8. Distribute the shares to the participants

The Decryption process is very simple take print out of the generated shares on the transparencies. Overlapping the transparencies on top of the other gets the secret image.

The result of applying the proposed model for colour image and the intermediate images generated are shown in figures 1 to 6 respectively.

VI. CONCLUSIONS

The VCS model described is very useful in providing mutual authentication among a group of participants as a whole. The Areas where we can use this are securing the bank financial statements, Video Watermarking, Remote Voting etc.

The proposed model secures only one secret image this can be extended to secure multiple secret images.

The proposed model does not produce the image of optimal contrast which can be enhanced and also the pixel expansion of the share increases as the k value in (k,n) VCS increases.

REFERENCES

[1] *K. Braun and R. L. de Queiroz, Color to Gray and Back: Color Embedding Into Textured Gray Images, Proc. IS&T/SID 13th Color Imaging Conference, pp.120-124, 2005.*

[2] *Moni Naor and Adi Shamir, "Visual cryptography", in Proceedings of Advances in Cryptology EUROCRYPT 94, LNCS Vol. 950, pages 1-12. Springer-Verlag, 1994.*

[3] *Nagaraj V. Dharwadkar , B.B. Ambedker, S.R. Joshi, "Visual Cryptography for Color Image using Color Error Diffusion", ICGST-GVIP Journal ,volume 10, issue 1,February 2010.*

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

[5] *R.W. Floyd and L. Steinberg, "An adaptive algorithm for spatial grayscale", Proc.SID, 17/2:75–77, 1975.*

[6] *Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36 (2003), 1619-1629.*

[7] *Zhi Zhou , Gonzalo R. , Giovanni Di Crescenzo,"Halftone Visual Cryptography", in Proceedings of IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006,pp 2441-2454*

[8] *HOU Y.C.: 'Visual cryptography for color images', Pattern Recognit., 2003, 1773, pp. 1–11.*

[9] *Tzung-Her Chen and Kai-Hsiang Tsao, "Visual secret sharing by random grids revisited", Pattern Recognition, 42(9):2203 - 2217, 2009. Elsevier Science Inc. New York, NY, USA.*

