A Novel Visual Cryptography Scheme

Debasish Jena[1], Sanjay Kumar Jena[2]
[1]*Centre for IT Education, Biju Pattanaik University of Technology, Orissa 751010, India*
[2]*Department of Computer Science & Engineering,*
National Institute of Technology Rourkela, Orissa 769 008, India
debasishjena@ieee.org, skjena@nitrkl.ac.in

Abstract

Visual Cryptography is a new cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human, without any decryption algorithm. Here we propose a Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm which is a modified version of Data hiding in halftone images using conjugate error diffusion technique (DHCED). We use this DHOCD algorithm for proposing a new three phase visual cryptography scheme. DHCOD technique is used to hide an binary visual pattern in two or more ordered dither halftone images, which can be from the same or different multi-tone images. In proposed scheme we shall generate the shares using basic visual cryptography model and then embed them into a cover image using a DHCOD technique, so that the shares will be more secure and meaningful.

Keywords –Secret shares, Halftone images, Visual cryptography, VCS, Watermarking, DHCED and DHCOD

1. Introduction

In this paper we consider the security of shares in visual cryptography and generating more meaningful shares with respect to basic cryptographic scheme. Basically visual cryptography is used for the encryption of visual information like written materials, textual images, and handwritten notes, print and scanned etc. in a perfectly secure way so that the decryption can be performed by human visual system.

Watermarking is the technique of embedding the secret image in a cover image without affecting its perceptual quality so that the secret image can be revealed by some process.

Halftoning is a process of converting a gray scale image into a binary image. The halftoning technique is required in many present applications such as facsimile (FAX), electronic scanning and copying, and laser printing etc.

Share generation for the visual cryptography can also be done by the concept of watermarking using some watermarking technique. We can use these watermarked shares for retrieving the hidden information. This effort can generate the meaningful shares rather than some shares having no information.

Here our proposed scheme will add the merits of both visual cryptography as well as watermarking, where we will generate the shares using basic visual cryptography model and then we will watermarked those shares using some cover images using DHCOD. The decryption will be same as in the visual cryptographic model i.e. by human visual system.

2. Visual cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994 [1]. 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 reveals no information about the original image. Fig 1 shows the working of visual cryptography. We can achieve this by using one of following access structure schemes [8].

1:(2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional

978-0-7695-3516-6/08 $25.00 © 2008 IEEE
DOI 10.1109/ICACC.2009.109

information is required to create this kind of access structure.

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

3 :(n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4:(k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

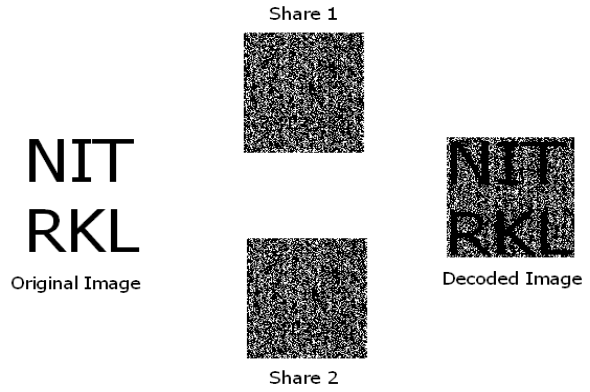

Figure 1. Working of visual cryptography

2.1. Model for visual cryptography

In this section we formally define VCS model, as well as (k,n)-threshold VCS scheme that was proposed by Naor and Shamir .

Definition 1: Hamming weight: The number of non-zero symbols in a symbol sequence. In a binary representation, Hamming weight is the number of "1" bits in the binary sequence.

Definition 2: OR-ed k-vector: Given a j x k matrix, it is the k-vector where each tuple consists of the result of performing Boolean OR operation on its corresponding jx1 column vector.

Definition 3: An VCS scheme is a 6-tuple (n, m, S, V,α, d). It assumes that each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white subpixels. The resulting structure can be described by an nxm Boolean Matrix S=[Sij] where Sij = 1 iff the jth subpixel in the ith share is black. Therefore, the grey level of the combined share, obtained by stacking the transparencies, is proportional to the Hamming weight H(V) of the OR-ed m-vector V. This grey level is usually interpreted by the visual system as black if H(V)≥ d and as white if H(V) < d-αm for some fixed threshold 1≤d≤ m and relative difference α > 0. α m, the difference between the minimum H(V) value of a black pixel and the maximum allowed H(V) value for a white pixel is called the contrast of a VCS scheme.

Definition 4: VCS Schemes where a subset is qualified if and only if its cardinality is k, are called (k,n)-threshold visual cryptography schemes. A construction to (k,n)-threshold VCS consists of two collections of n x m Boolean matrices C0 and C1, each of size r. To construct a white pixel, we randomly choose one of the matrices in C0, and to share a black pixel, we randomly choose a matrix in C1. The chosen matrix will define the color of the m subpixels in each one of the n transparencies. Meanwhile, the solution is considered valid if the following three conditions are met:

[1.] For any matrix S in C0, the "or" operation on any k of the n rows satisfies H(V) < d-αm.

[2.] For any matrix S in C1, the "or" operation on any k of the n rows satisfies H(V) ≥d.

[3.] For any subset {i1 i2,... iq} of {1, 2,.. .n} with q < k, the two collections of q x m matrices Bt for t€{0,1} obtained by restricting each n x m matrix in Ct (where t = 0,1) to rows i1,i2, ...,iq are indistinguishable in the sense that they contain the same matrices with the same frequencies. In other words, any q x n matrices S0 €B0 andS1 €B1 are identical up to a column permutation.

Condition first and second defines the contrast of a VCS. The third condition states the security property of (k,n)-threshold VCS. If we have not been given k shares of the secret image, one cannot gain any hint in deciding the color of our pixel, regardless having any amount of computation resources.

2.2. Basic approach

Basic visual cryptography is based on breaking of pixels into some subpixels or we can say expansion of pixels. Fig 2 shows two approaches for (2, 2) – Threshold VCS. In this particular figure first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel BT+TB=BB or TB+BT=BB and for white pixel BT+BT=BT or TB+TB=TB. Similarly second

approach is given where each pixel is broken into four sub pixels. We can achieve 4C2 =6 different cases for this approach.

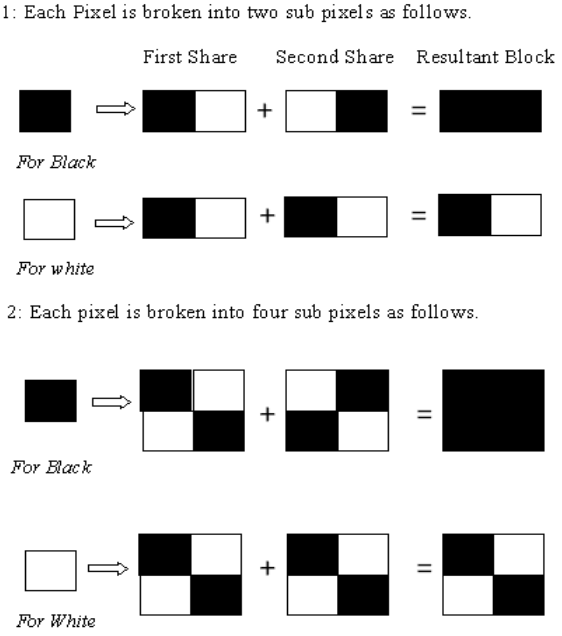

Figure 2: Visual Cryptography

3. Proposed algorithm— Data Hiding in Halftone Images using Conjugate Ordered Dithering (DHCOD)

In this section the proposed Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm is given, which is a modified version of existing Data hiding in halftone image by conjugate error diffusion (DHCED) algorithm. Here we have done two major changes in DHCED. First change is noise inclusion step in the secret image. Second change is in the halftoning technique. Here we have taken ordered dithering technique with respect to error diffusion technique in DHCED. Advantages of these changes are given in section 3.2.

3.1 DHCOD algorithm

Let X is the cover image and H is the image to be hidden i.e. secret image.

Step1: Add some noise to the secret image i.e. H. Let us call it as H1.It introduces some stochastic factors between the original multi-tone images and final share. This step is very important to break the direct correlation between multi-tone and share images.

Step 2: Convert the noisy secret image i.e. H1 into binary image. Let us call it as H2.

Step 3: Generate the first share X1: X1 will be nothing but a dithered halftone image generated by the cover image X. We can use dithering technique to generate the halftone image. In DHCED error diffusion technique was used to generate the halftone images [2].

Step 4: Generate the second share X2:X2 image will be generated with the help of X1 and the image H2. Let HB is the collection of location of all black pixels in H2 and HW is the collection of location of all white pixels in H2.

For all pixel (i, j) which belongs to HW, the pixel X2(i, j) is same as the co-located pixel X1(i, j) in X1. For all pixel (i, j) which belongs to HB, the pixel X2(i, j) will be XOR of co-located pixel in X1 and negation of collocated pixel in H2. i. e.,

$$X2(i,j) = X1(i,j) \oplus (\sim H2(i,j))$$

We can reveal the image with the simple AND operation of X1 and X2 i.e. X1&X2. Fig 3 shows the working model of proposed DHCOD.

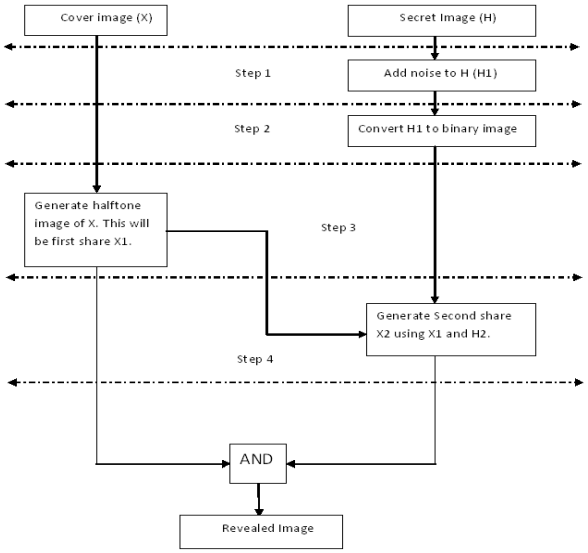

Figure 3. Working model of DHCOD algorithm

3.2. Comparison of DHCOD with DHCED

First change in DHCOD is the noise inclusion step in the secret image which was absent in DHCED technique. It breaks the direct correlation between multi-tone and share images. Second major change is use of ordered dithering technique with respect to error diffusion technique in DHCED in order to generate the

halftone image. As we know error diffusion technique spreads the quantized error in neighboring pixels which can affect in halftoning of that pixel and we might get wrong value for e.g. a pixel which should be a black one can turn to a white pixel. While in ordered dithering we deals with individual pixels and it is takes less computation to generate the halftone image. Since this work is completely based on pixel by pixel manner so it is better to use ordered dithering with respect to error diffusion. We have also made a small change in the revealing operation of DHCOD algorithm which shows a dramatically good result in the revealed image. If we change the revealing operation from "AND" to "XOR" then we get a very clear secret image without any cover image. But we can not use this for visual cryptography since we are performing XOR operation and it does not work for stacking of shares. But it may be very useful in copyright protection and other cryptographic scheme. Figure 4 shows the simulation results of DHCOD.

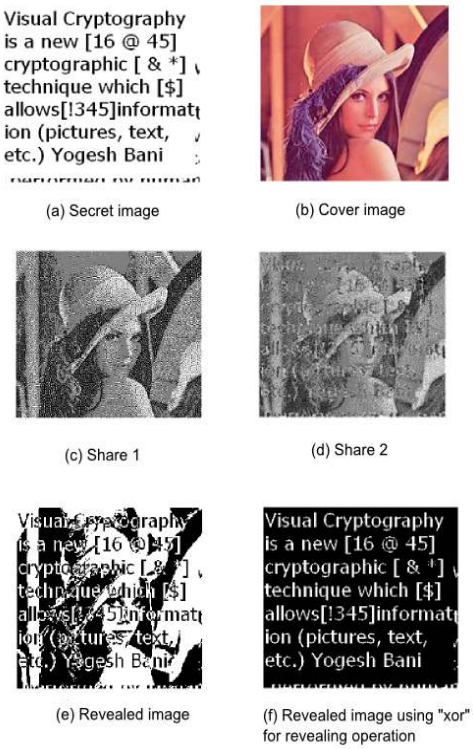

Figure 4. Simulation results of DHCOD

4. Proposed scheme: A New Three Phase Visual Cryptography Scheme

We are proposing a new scheme for visual cryptography which will use DHCOD technique to embed the generated shares into some cover image. Proposed scheme consists three different phases which are described under following subsection.

4.1 Phases of Proposed Scheme

Phase 1- Visual Cryptographic Encryption: In this very first phase we will do visual cryptography encryption. It consists generation of shares using any basic visual cryptography model. Visual cryptographic solutions operate on binary inputs. Therefore, natural (continuous-tone) images must be first converted into halftone images by using the density of the net dots to simulate the original gray or color levels in the target binary representation. For halftoning we can use any halftoning technique as error diffusion, thresholding, ordered dithering [4, 6] etc. So the result of this phase will be different unintelligible shares of black and white pixels.

Phase 2- Generation of Watermarked Shares using DHCOD: This is the second phase of our approach which will embed shares generated from the first phase into some cover images. For watermarking we will use DHCOD algorithm discussed under section 3. Use of watermarking will give an added advantage of double security over other visual cryptographic schemes. Result of this phase will be different meaningful shares consisting some cover image.

Phase 3- Visual Cryptographic Decryption: This is the last phase of proposed scheme. In this phase we will do visual cryptographic decryption. As we know that visual cryptographic decryption does not need any type of decryption algorithm or computation. It uses human visual system for decryption which is the core advantage for which visual cryptography was developed. We will have different shares embedded in some cover image as the result of second phase. Now we can decrypt the original secret image by overlapping of shares. The result of this phase will be an image consisting secret image as well as cover image. Fig 5 is the structure of proposed scheme.

4.2 Merits and Demerits of Proposed Scheme

Proposed scheme provides a high-level security. First phase i.e. visual cryptographic encryption adds the advantages and security of basic schemes. Then phase two adds the advantage and security DHCOD algorithm. Here we get the shares with some information as some image can be shown in the shares with respect to completely black and white pixels in basic scheme. Since it provides better security so it is most useful in transmission of financial documents.

More applications can also be developed which require a high level security. As we know no scheme can be perfect in all aspects. This scheme also has drawbacks as the quality of the revealed image is not rich. Since it uses second phase takes the input as the result of first phase i.e. visual cryptographic encryption so definitely it will have the low contrast. But it provides the more secure shares so we can compromise with this.

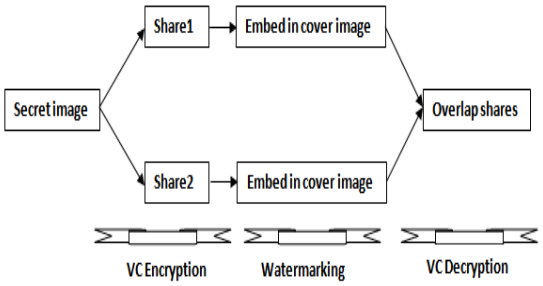

Figure 5. Structure of proposed scheme

4.3. Simulation Results

Fig 6 shows the simulation results of proposed scheme. For simulation we have used MATLAB 7.0 tool. We have taken a textual image of size 256 x 256 as secret image and lena image of 256 x 256 as cover image.

5. Conclusion

Visual cryptography is the current area of research where lots of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are many possible enhancements and extensions exist of the basic visual cryptographic model introduced till now. One such enhancement we are trying to do. There are other areas also in visual cryptography which are still open where no satisfactory results yet achieved as color visual cryptography, enhancement of image shares with respect to contrast, size, quality and clarity of revealed image. Researchers are still busy for finding the new application where visual cryptography can be used.

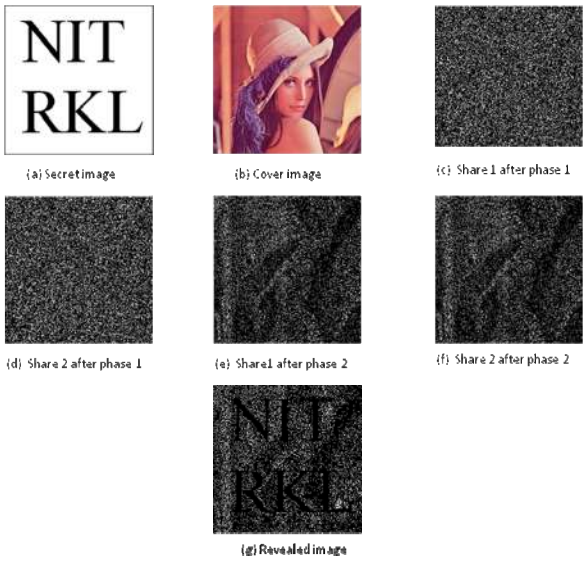

Figure 6. Simulation results of proposed scheme

10. References

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

[2] Ming Sun Fu and Oscar C. Au "Data hiding in halftone images by conjugate error diffusion" D-7803-7761-3/03 © 2003 IEEE.

[3] Ming Sun Fu and Oscar C. Au "Joint Visual cryptography and watermarking". 0-7803-8603-5/04 © 2004 IEEE.

[4] Zhongmin Wang and Gonzalo R. Arce "Halftone visual cryptography through error diffusion" ISBN 1-4244-0481-9/06 © 2006 IEEE, pp.109-112.

[5] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo "Halftone Visual Cryptography" 0-7803-7750-8/03 © 2003 IEEE,

[6] Notes "Digital Image Processing Laboratory: Image Halftoning" April 30, 2006. Purdue University.

[7] Lingo Fang and Bin Yu "Research on pixel expansion of (2,n) Visual threshold scheme" 2006 1st International Symposium on Pervasive Computing and Applications.

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129, No. 2, (1996), pp. 86-106.