IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

DHCED and DHCOD Technique of Visual Cryptography Scheme for Encrypted and Decryption

S. Ponnarasi[1*], T. Rajendran[2]

[1,2]Department of Computer Science, Government Arts and Science College, Kangeyam- 638108, India

Available online at: www.ijcseonline.org

Abstract**--**Visual Cryptography is a new cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such some way that the decipherment will be performed by human, with none decipherment algorithmic rule. Here we have a tendency to propose a knowledge activity in halftone pictures victimisation conjugate ordered video digitizing (DHCOD) algorithmic rule that could be a changed version of information activity in halftone pictures victimisation conjugate error diffusion technique (DHCED). We have a tendency to use this DHOCD algorithmic rule for proposing a brand new 3 part visual cryptography theme. DHCOD technique is employed to cover Associate in Nursing binary visual pattern in 2 or additional ordered dither halftone pictures, which may be from identical or completely different multi-tone pictures. In projected theme we have a tendency to shall generate the shares victimisation basic visual cryptography model so imbed them into a canopy image employing a DHCOD technique, so the shares are going to be safer and pregnant.

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

I. Introduction

In this paper we consider the protection of shares in visual cryptography and generating a lot of purposeful shares with relevance basic cryptologic theme. primarily visual cryptography is employed for the coding of visual data like written materials, matter pictures, and written notes, print and scanned etc. during a absolutely secure approach in order that the decoding are often performed by human sensory system.

Watermarking is that the technique of embedding the key image during a cowl image while not moving its sensory activity quality in order that the key image are often Halftoning could be a method of changing a grey scale image into a binary image. The [*fr1] toning technique is needed in several gift applications like facsimile (FAX), electronic scanning and repetition, and optical device printing etc.

Share generation for the visual cryptography also can be done by the construct of watermarking victimization some watermarking technique. we will use these watermarked shares for retrieving the hidden data. This effort will generate the purposeful shares instead of some shares having no data.

Since the invention of public-key cryptography in 1976 by Whitfield Daffier and Martin dramatist [1], various public key cryptologic systems are projected. All of those systems primarily based their security on the of resolution a mathematical problem. Over the years, several of the projected public-key cryptologic systems are broken and lots of others are incontestible to be impractical. Today, solely 3 kinds of systems ar thought of each secure and economical. samples of such systems and therefore the mathematical issues on that their security relies, are [2]

Integer factorization problem (IFP): RSA and Rabin Williams.

- **Discrete logarithm problem (DLP):** the U.S. governments Digital Signature Algorithm (DSA), the DiffieHellman key agreement scheme, the ElGamal encryption and signature schemes, the Schnorr signature scheme, and the Nyberg-Rueppel signature scheme.
- **Elliptic curve discrete logarithm problem (ECDLP):** the elliptic curve analog of the DSA (ECDSA), and therefore the elliptic curve analogs of the Diffie-Hellman key agreement theme, the ElGamal encoding and signature schemes, the scrounge signature sc hematin, and therefore the NybergRueppel signature theme.
- Here our projected theme can add the deserves of each visual cryptography moreover as watermarking, wherever we'll generate the shares exploitation basic visual cryptography model so we'll watermarked those shares exploitation some cowl pictures exploitation DHCOD. The decoding are same as within the visual cryptanalytic model i.e. by human sensory system.

II. VISUAL CRYPTOGRAPHY

Visual cryptography may be a cryptographical technique that permits visual data (pictures, text, etc.) to be encrypted in such the way that the decoding may be performed by humans (without computers). the primary visual cryptographical technique was developed by Moni Naor and Adi Shamir in 1994 [1]. It concerned ending the image into n shares in order that solely somebody with all n shares may decipher the image by overlaying every of the shares over one another. much, this may be done by printing every share on a separate transparency so putting all of the transparencies on high of every alternative. In their technique n-1 shares reveals no data regarding the first image. Fig one shows the operating of visual cryptography. we will bring home the bacon this by victimisation one in all following access structure schemes [8].

1:(2, 2) – Threshold VCS: this is often a simplest threshold theme that takes a secret image and encrypts it into 2 totally different shares that reveal the key image once they ar overlaid. No extra data is needed to make this sort of access structure.

2 :(2, n) – Threshold VCS: This theme encrypts the key image into n shares specified once any 2 (or more) of the shares ar overlaid the key image is discovered. The user are going to be prompted for n, the quantity of participants.

3 :(n, n) – Threshold VCS: This theme encrypts the key image into n shares specified only all n of the shares ar combined can the key image be discovered. The user are going to be prompted for n, the quantity of participants.

4:(k, n) – Threshold VCS: This theme encrypts the key image into n shares specified once any cluster of a minimum of k shares ar overlaid the key image are going to be discovered. The user are going to be prompted for k, the edge, and n, the quantity of participants.

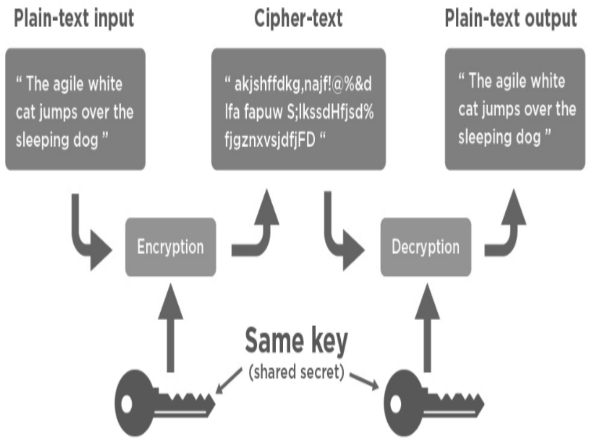

Plain-text input
Cipher-text
Plain-text output
" The agile white cat jumps over the sleeping dog "
" akjshffdkg,najf!@%&d lfa fapuw S;lkssdHfjsd% fjgznxvsjdfjFD "
" The agile white cat jumps over the sleeping dog "
Encryption
Decryption
Same key
(shared secret)

Figure 1. Working of visual cryptography

2.1 Model for visual cryptography

In this section we tend to formally outline VCS model, still as (k,n)-threshold VCS theme that was planned by Naor and Shamir .

Definition 1: playacting weight: the quantity of non-zero images in a very symbol sequence. in a very binary illustration, playacting weight is that the range of "1" bits within the binary sequence.

Definition 2: OR-ed k-vector: Given a j x k matrix, it's the k-vector wherever every tuple consists of the results of acting mathematician OR operation on its corresponding jx1 column vector.

Definition 3: AN VCS theme may be a 6-tuple (n, m, S, V,α, d). It assumes that every element seems in n versions referred to as shares, one for every transparency. every share may be a assortment of m black and white sub-pixels. The ensuing structure are often delineate by AN nxm mathematician Matrix S=[Sij] wherever Sij = one iff the jth sub-pixel within the ith share is black. Therefore, the gray level of the combined share, obtained by stacking the transparencies, is proportional to the playacting weight H(V) of the OR-ed m-vector V. This gray level is typically understood by the sensory system as black if H(V)≥ d and as white if H(V) &lt; d-αm for a few mounted threshold 1≤d≤ m and relative distinction α &gt; zero. α m, the distinction between the minimum H(V) price of a black element and therefore the most allowed H(V) price for a white element is termed the distinction of a VCS theme.

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:

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

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

2.4. [3.] For any set of with Q &lt; k, the 2 collections of Q x m matrices Bt for t€ obtained by proscribing every n x m matrix in Ct (where t = zero,1) to rows i1,i2, ...,iq square measure indistinguishable within the sense that they contain an equivalent matrices with an equivalent frequencies. In different words, any Q x n matrices S0 €B0 andS1 €B1 square measure identical up to a column permutation.

2.5. Condition initial and second defines the distinction of a VCS. The third condition states the protection property of (k,n)-threshold VCS. If we've got not been given k shares of the key image, one cannot gain any hint to decide the colour of our component, regardless having any quantity of computation resources.

2.6. Basic approach

Basic visual cryptography is based on breaking of pixels into some sub pixels 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.

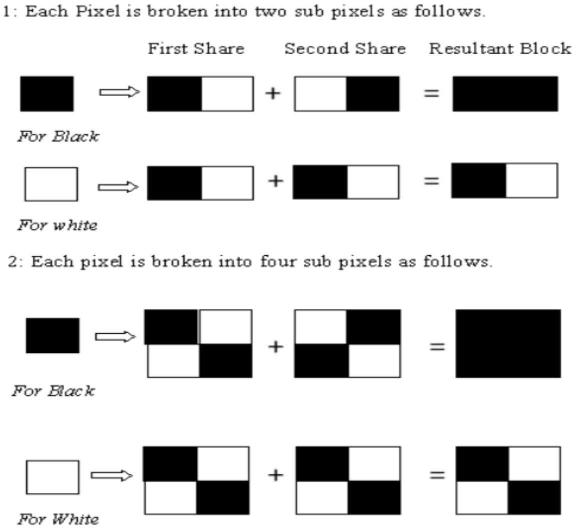

1: Each Pixel is broken into two sub pixels as follows.
First Share
Second Share
Resultant Block
+
=
For Black
For white
2: Each pixel is broken into four sub pixels as follows.
For Black
For White

Figure 2: Visual Cryptography

III. 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 half toning 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.,

$X\,2(i, j) = X1(i, j) \oplus (\sim H\,2(i, j))$

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.

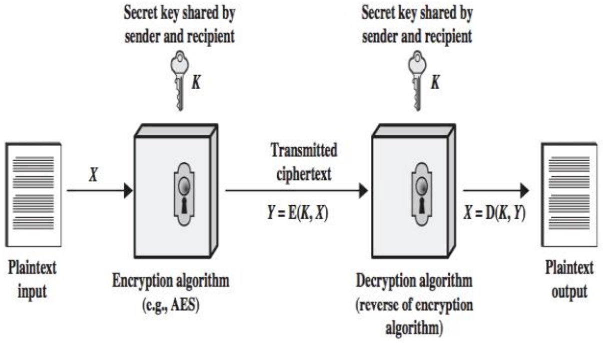
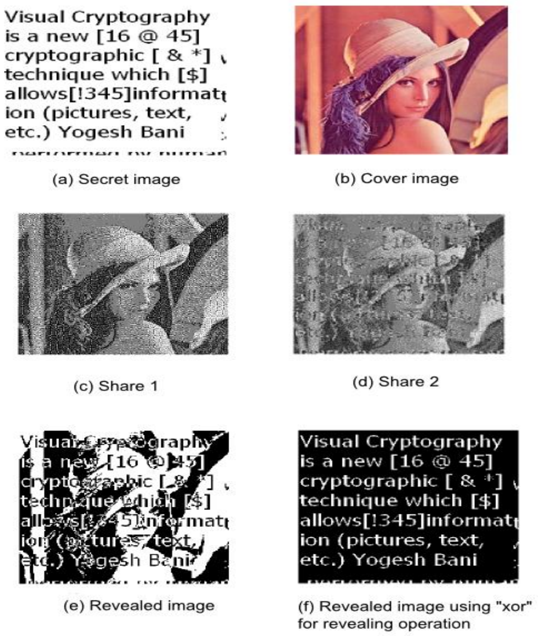

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

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 half toning 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 cannot 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.



(a) Secret image

(b) Cover image

(c) Share 1

(d) Share 2

(e) Revealed image

(f) Revealed image using "xor" for revealing operation

Figure 4. Simulation results of DHCOD

IV. 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 half toning we can use any half toning 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.

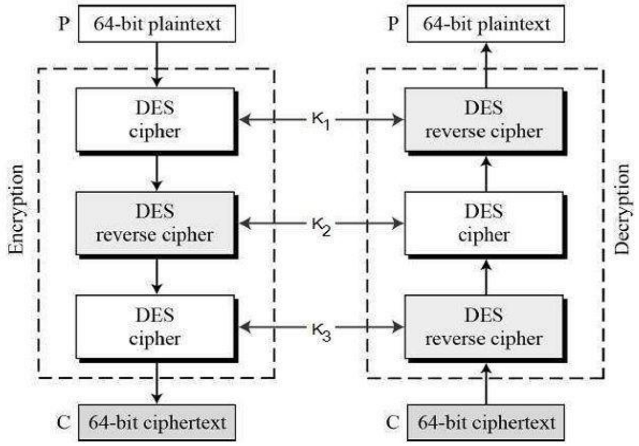
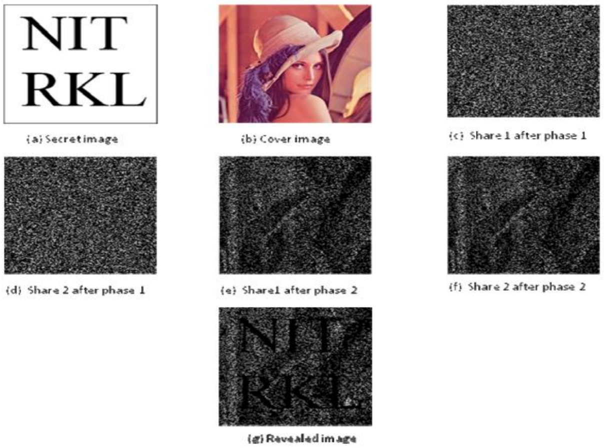


Figure 5. Structure of proposed scheme

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.



(a) Secret image (b) Cover image (c) Share 1 after phase 1 (d) Share 2 after phase 1 (e) Share1 after phase 2 (f) Share 2 after phase 2 (g) Revealed image

Figure 6. Simulation results of proposed scheme

V. CONCLUSION AND FUTURE SCOPE

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.

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.

[9] V. S. Miller, Uses of Elliptic Curve in Cryptography, ser. Lectures notes on Computer Sciences. New York, USA: Springer-Verlag, 1986, vol. 218, ch. Advances in Cryptography- Proceedings of Crypto85, pp. 417– 426.

[10] P. C. v. O. Alfred J. Menezes and S. A. Vanstone, Handbook of Applied Cryptography, 1st ed. CRC Press, 1996.

[11] D. R. Stinson, Cryptography: Theory and Practice, 2nd ed. CRC Press, 2002.