ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Review on Data Hiding in Halftone Images

Ranjeet Kumar Ranjan

Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India

Email Id: rkranjan@Galgotiasuniversity.edu.in

ABSTRACT: Yisual Cryptography (YC) is a hidden exchange method, initially introduced in a binary hidden file, called mutual random digital variations, is embedded in a K of N of YC. The portion is xeroxed and allocated to n canvases, one for each person, respectively. No individual understands how much a researcher has been given. One person or more can visibly show the hidden picture by combining all transparencies. Even if the computing power is unlimited, the key cannot be deciphered by anyone or although smaller people. YC is essentially a hidden picture storage system and is distinguished by its capacity to remotely restore without using machine.Visual Cryptography is an authentication method for the protection, by using the visual processing system, eyes, of sensory information such as printed pictures, handwritten notes etc. This is an approximation for data that is covered in halftone pictures. In this paper they focus on increasing the stability and robustness of VI-C shares and on creating more significant shares in the cryptographic specific scheme. This method uses an anatomical procedure and organized dithering's and is an amended version of DHCOD.

KEYWORDS*:* Secret shares, halftone images, visual cryptography, visual cryptography scheme (VCS), watermarking, mathematical morphology and DHCOD.

I. INTRODUCTION

Yisual Cryptography (YC) has been introduced for the first time in Euro-Crypt94. In a k out of YC, a hidden conditional image, called spontaneous random pattern shares, is represented in shadows frames. The shares are Xeroxed and disseminated to each contributor, between on n stencils. The share provided to the other contributor is unknown to no attendee. Each participant will visually reveal the truth picture by integrating transparencies. No one or fewer individuals can encode the secret although they have infinite computing power. YC is basically a private photo sharing program and is characterized by its unique restorability without device use. Someone other than those who started the processor are entitled to access secrets is keeping a secret out of the information. Confidentiality sharing describes a way to spread confidentiality among a community of stakeholders to enable a secret to be delegated to each participant. Each secret piece is called a share. Secrecy can only be reorganized if a fixed amount or enough securities are combined. While these shares are different, no details can be collected or viewed on the password. That is, because shares are divided, they are absolutely useless. As the basic package, and generalized to many implementations, the YC scheme suggested by "Naor and Shamir". Let us suggest a simple procedure for encoding a password using (2, 2) YC framework to demonstrate YC's basic concepts. Secrecy is broken in two pairs in unpredictable binary patterns under this system. Each hidden pixel shall be substituted by a two-sub-pixel unoverlapped block. An anti-overlapping block of two bytes would encrypt each byte p of the hidden binary file. There is no indication of the current pixel value in the site-pixel set. Anybody with just one share cannot disclose any confidential information. Both shares must be Xeroxed to transparent in order to decrypt the file. Rearranging these two transparencies will allow the secret to be visually recovered [1]–[6].

The visual cryptographic feature is shown in Figure 1. Although some contrast reduction is detected, the decoded picture is clearly identified. Definitions in the use of visual encryption are Figure 1 and Figure 2. Two procedurally generated photographs containing confidential information are presented in Figures 1(a) and (b). The authors of this paper clearly see the revelation as shown in figure c when printing both share on transparencies and overlapping them.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Shortly speaking, the YC technology applies to bi-nary photos in which the hidden picture is, whereas the other portion is created by randomly:

$$i + i = i; i = 0; 1; 2; :::; n$$

Therefore, it is not possible to conclude without it. This system offers complete safety and usability. Such features are found in visual cryptography:

Decryption (secret restoration) without the aid of a computing device.

Robustness against lossy compression and distortion due to its binary attribute.

Besides obvious implementations to concealing the documentation, there are also numerous YC programs, including particular entry structures, security of copyright, watermarking, graphical encryption and identification, and implementations for print and scanning, etc. In YC, the idea of watermarking [7]with a certain watermarking technologies will establish a share of the secrecy as shown in figure 1.

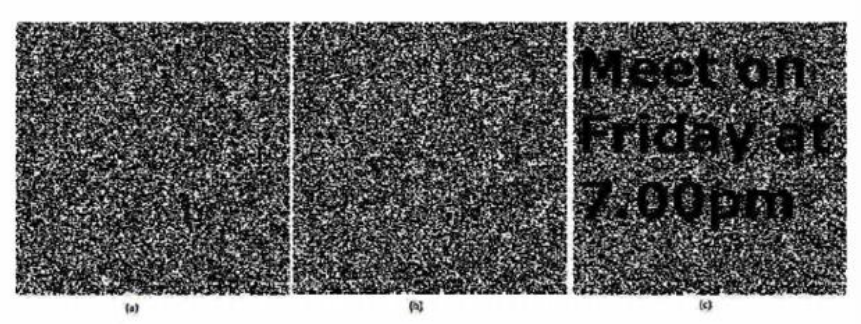

Fig.1: Working of Visual Cryptography

Recently, several different approaches were added. In order to reduce the lack of intensity in the restructured pictures, an author suggested an acceptable contrast k from n system. Another author suggested a more generic vs scheme focused on the framework of the temporary access[8]–[12]. The arrangement of access shall define eligible and excluded share subdivisions. From one of the accompanying access arrangement schemes which are shown in below table 1.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Table.1: Access Structure Schemes

1.	(2, 2) - Threshold VCS: Input - Secret Image to be encrypted. Encryption - Secret image is encrypted into two different shares. Decryption - each share is Xeroxed onto a transparency. Secret image can be revealed by overlapping the two transparencies. No additional information required.
2.	(2,n) - Threshold VCS: Input - Secret Image to be encrypted. Encryption - Secret image is encrypted into n different shares. Decryption - each share is Xeroxed onto a transparency. Secret image can be revealed by overlapping any two transparencies. The user will be prompted for n i.e. the number of participants.
3.	(n,n) - Threshold VCS : Input - Secret Image to be encrypted. Encryption - Secret image is encrypted into n different shares. Decryption - each share is Xeroxed onto a transparency. Secret image can only be revealed by overlapping all the n transparencies. The user will be prompted for n i.e. the number of participants.
4.	(k,n) - Threshold VCS: Input - Secret Image to be encrypted. Encryption - Secret image is encrypted into n different shares. Decryption - each share is Xeroxed onto a transparency. Secret image can be revealed by overlapping any k transparencies. The user will be prompted for k, the threshold and n, the number of participants.

Procedure is transparent and efficient. This depends upon two rules, namely organized prevaricating and quantitative morphology, used in the development of shares. Ordained dithering is an easy yet effective image generation algorithm. This paper proposed an anatomical procedure conducted on the hidden picture to render shares safer and resilient.

II. METHODOLOGY

This paper provides a short description of VC, expanded VC, half toning, watermarking, organized dithering, propagation of error and computational morphology in this portion.

A. The VC Concepts

In addition, the Visual Cryptography Scheme encodes a secret message to participants.
Every exchange displays completely fractal patterns in black and white and does not expose hidden photos knowledge alone. With a k outn method, you can decrypt the encrypted picture by piling the shares together, but you do not have sufficiently exposure to less than k stocks to decrypt.

B. Extended VC

A conditional concealed picture and n initial pictures are used as feedback in a traditional (k;n)-threshold EVC scheme (EVCS). N innocent encrypted shares are created with an estimation of original pictures that meet specific three requirements.

1) Any k out of the n shares can be used to recover the secret image.
2) Any less than k shares cannot be used to obtain any information about the secret image.
3) All the shares are meaningful images.

Figure 2 and 3 explains the basics of the VC:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

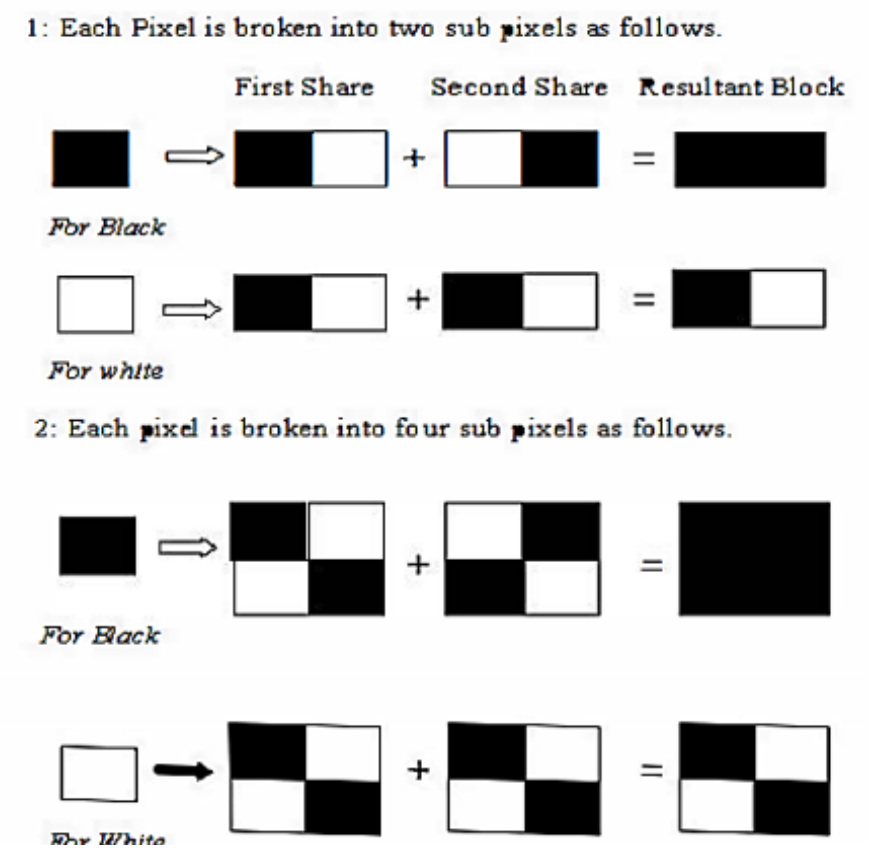

Fig.2: Basics of Visual Cryptography

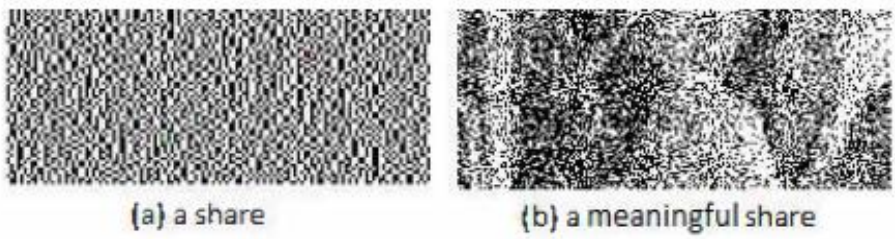

Fig.3: Difference Between a Normal Share (YC) and a Meaningful Share (EYCS)

C. Half-toning: It is the mechanism by which a gray picture is converted into a binary one. In a range of uses, such as FAX, laser processing and copying, and optical scanning respectively, this method is used. The description of half-toning is shown in Figure 4.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

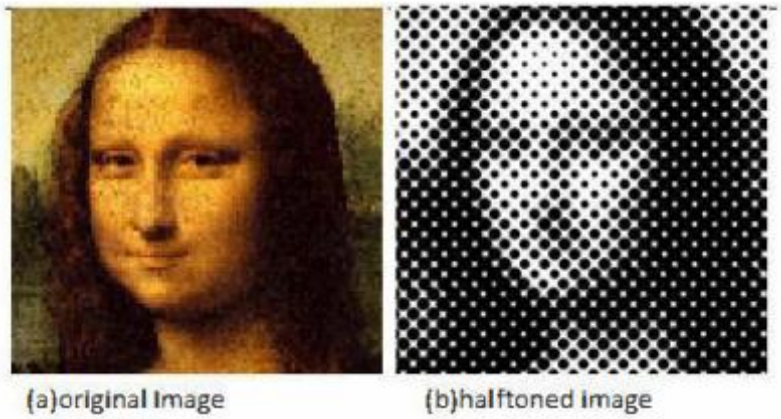

Fig 4: Half-toned Image

III. PROPOSED ALGORITHM

In this portion, the proposed data hide throughout halftone pictures, which is an altered version of available data hidden by the declension post-processing algorithm (DHCOD) in the half-ton setting, are provided using only a morphological process. Here, this paper has made three big algorithm improvements. After a binary representation is transformed, the first change takes the counterpart to the hidden object. The second change is the use of anatomy. The third change is the addition of the silhouette that we receive after the XOR installation on both shares. The implications of these improvements were discussed later. This paper has proposed an alternative scheme that would supplement the hidden picture and was not in DHCOD. The second major improvements are the use of morphological techniques to delete the existing pixels because only the target pixels will remain on them. It helps build healthier and better shares. Rather than ordering backtracking in a more economical way, authors could have used the mistake diffusion technique. Quantified error is usually propagated in adjacent pixels and it can also be likely to get a false result. Even if the same pixel's half toning is impaired. A white pixel will transform into black, for instance. Whereas they handle one pixel at a time in order to create a halftone image, this reduces the time taken. There we must, therefore, treat the image as pixel by pixel and it is very well that organized sharpness is used instead of confusing. Also, the DHCOD algorithm has been updated with the disclosing operation using XOR instead of AND. Compared with the previous tests, it will give you a better answer. This method can be regarded as an outstanding methodology specifically for intellectual property rights and other computational systems. After the "XOR" procedure of phase 2 it is better to change the picture supplement again, which improves the visual clarity of the information exposed.

Algorithm for the proposed algorithm is depicted below:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Step 1: First, add some noise to the secret image H. We will call this image as HI. Addition of noise introduces some stochastic factors between the original multi-tone image and the final share. This step is very significant as it breaks the direct correlation between the original multi-tone image and secret image.

Step 2: Calculate threshold value of HI i.e. secret image with added noise. Use the calculated threshold value to convert HI into a binary image. Let us call this H2.

Step 3: Complement the binary image H2. Let us call this H3. This step is performed to enhance the visual quality of the revealed image.

Step 4: Perform a morphological operation on the secret image H3. The operation will be performed in such a way that the secret image will be scanned in so that the interior pixels are removed. That is, a pixel is set to the value 0 if all of its 4- connected neighbors are I thereby leaving only the boundary pixels on.

Step 5: Generate the first share X1: Xl is generated by applying ordered dithering to H3 using Bayers matrix

Step 6: Generate the second share X2: X2 will be generated with the help of Xl and H3. Let HW be the collection of location of all white pixels in H3 and HB be the collection of location of all black pixels in H3

IV. RESULT

For the simulation of our research we have used the MATLAB lO.O method. Rare must be taken as a cover image of a text as a hidden picture and a sunset view. Share Generation For both the mathematical model of proposed work, the researchers even used MATLAB lO.O tool. Researchers have to seriously consider Rare as the secret picture and sunset picture a textual picture as the cover picture. Share 2 Generation: They have suggested the number of net dots and modified natural (continuous) pictures to halftones in order to simulate the initial gray or color rates of the intended binary depiction. The next addition to this halfway image is to be generated. A morphological process is then done. To order to eliminate the inner pixels, the corresponding halving-toned hidden image is screened, i.e., a vector is set to 0 for all values of 4-connected neighbors with interest as shown in Figure 5.

a. b.

Fig.5: Share Two Proposed Sheme, Revealed Image for DHCOD

V. CONCLUSION

Cryptography is an authentication method for the protection, by using the visual processing system, eyes, of sensory information such as printed pictures, handwritten notes etc. This is an approximation for data that is covered in halftone pictures. In this paper they focus on increasing the stability and robustness of VI-C shares and on creating more significant shares in the cryptographic specific scheme. This method uses an anatomical procedure and organized dithering's and is an amended version of DHCOD.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

This manual presents an authentication method of creating a VC framework with heavy security and reliability utilizing mathematical morphology and directed prevaricating. The morphological procedure effectively destroys existing pixels so that only the minimal pixels remain on it. Ordered dithering is being used to create a share of pixels in addition to manufacture a picture of a semi-determined great quality. It is clear that there is a balance between authentication partners contrast and decryption share, but we can understand hidden grayscale notes with low comparison. The neural network instituted for bitmap images may be widely employed in many VC strategies.

REFERENCES

[1] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "HiDDeN: Hiding data with deep networks," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018.
[2] T. Jitha Raj and E. T. Sivadasan, "A survey paper on various reversible data hiding techniques in encrypted images," in Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015, 2015.
[3] W. Mazurczyk and S. Wendzel, "Information hiding," Commun.ACM, 2017.
[4] A. Panchani and H. Doshi, "International Journal of Advance Engineering and Research," Int. J. Adv. Eng. Res. Dev., 2017.
[5] A. Achuthshankar, A. Achuthshankar, K. P. Arjun, and N. M. Sreenarayanan, "Implementation of reversible Data Hiding in Encrypted Image using A-S Algorithm," in Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015, 2016.
[6] M. Fallahpour, D. Megias, and M. Ghanbari, "Reversible and high-capacity data hiding in medical images," IET Image Process., 2011.
[7] S. Sachdev, A. Nayak, and T. Pradhan, "Data hiding in halftone images using mathematical morphology and conjugate ordered dithering," in 2014 International Conference on High Performance Computing and Applications, ICHPCA 2014, 2015.
[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., 2004.
[9] B. Saha and S. Sharma, "Steganographic techniques of data hiding using digital images," Defence Science Journal. 2012.
[10] C. H. Son, K. Lee, and H. Choo, "Inverse color to black-and-white halftone conversion via dictionary learning and color mapping," Inf. Sci. (Ny)., 2015.
[11] J. M. Guo and Y. F. Liu, "Hiding multitone watermarks in halftone images," IEEE Multimed., 2010.
[12] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," in Procedia Computer Science, 2015.