Novel Encryption method for Grayscale Halftone Images using Random numbers

[1]Manjula D. C., [2]Vijaya C.

PG student, M .Tech (Digital Electronics), Professor and Dean (Academic Program)
Dept. of Electronics &Communication Engineering
S.D.M. College of Engineering and Technology Dharwad, Karnataka
Email: [1]manjula.dc99@gmail.com, [2]vijayac26@yahoo.com

Abstract— Cryptography is derived from the Greek words kryptós, "hidden", and gráphein, "to write" or "hidden writing''. It is a means of transforming data in a way that renders it unreadable by anyone except the intended recipient. Visual cryptography (invented by Naor & Shamir in 1994) is a method for securely encrypting messages in such a way that the recipient won't need a computer to decrypt them. It is the technique that divide the secret image into n multiple shares. Each share constitutes some information and when k shares out of n stack together the secret will reveal. However less than k shares do not work. In this paper a novel encryption method is used for gray scale halftone images using random numbers. The size of the retrieved image is same as the size of input secret image. Extra security is added by introducing keys, which are same at both encryption and decryption. This leads to no degradation in image quality as desired in certain image processing applications.

Index Terms— Gray scale halftone image, Key, random numbers, Pixel reversal, Shares, Visual Cryptography.

I. INTRODUCTION

Digital Image processing is the technology of applying a number of computer algorithms to process digital images. The outcome of this process can be either images or a set of representative characteristics or properties of the original images. An image may be defined as a two-dimensional function, f(x, y), where x and y are spatial coordinates, and the amplitude values of f are all finite, discrete quantities. Digital image processing directly deals with an image, which is composed of many image points. These image points, also namely pixels, are of spatial coordinates that indicate the position of the points in image, and intensity (or gray level) values [1]. The applications of digital image processing have been commonly found in robotics, forensics, medical imaging, remote sensing and photography. The main purpose of digital image processing is to allow human beings an image of high quality or descriptive characteristics of the original image. A colorful image accompanies higher dimensional information than a gray image, as red, green and blue values are typically used in different combinations to reproduce colors of the image in the real world. The applications of digital image processing are widely used in the area of cryptography.More specifically, cryptography schemes have found immediate applications in certain types of protocols, including authentication and identification [2], and copyright protection and watermarking [3], [4]. With the coming era of Internet, more and more data are transmitted and exchanged on the networked systems to enjoy the rapid speed and convenience. However, in the cyberspace the availability of duplication methods encourages the violation of intellectual property rights of digital data. Therefore, the protection of rightful ownership of digital data has become an important issue in recent years. Cryptography concerns four main goals: Message Confidentiality (or privacy), only an authorized recipient should be able to extract the contents of the message from its encrypted form. Message Integrity, the recipient should be able to determine if the message has been altered. Sender authentication validates the source of a message to ensure the sender is properly identified. Sender non-repudiation, establishes sender identity so that the entity cannot deny having sent the message, Access Control – Access to an object requires access to the associated crypto keys in many systems (e.g. login).

Computer security people often ask for non-mathematical definitions of cryptographic terms. The basic terminology is that cryptography refers to the science and art of designing ciphers, cryptanalysis to the science and art of breaking them, while cryptology often shortened to just crypto, and is the study of both. The input to an encryption process is commonly called the plaintext, and the output the cipher text. There are a number of cryptographic primitive's basic building blocks, such as block ciphers, stream ciphers, and hash functions. Block ciphers may either have one key for both encryption and decryption, in which case they're called shared key (secret key), or have separate keys for

encryption and decryption, in which case they're called public key or asymmetric [5]. Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994[6], decryption was through human visual system no computations were required at the decryption. 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 the human visual system. Suppose the data D is divided into n shares, D can be reconstructed from any k shares out of n, complete knowledge of k-1 shares reveals no information about D, k of n shares is necessary to reveal secret data. The paper has been classified into five categories. Section I throws the light overview of digital image processing and cryptography. Section II discusses the previous works. Section III describes the proposed work where encryption and decryption algorithms are implemented. Section IV outlines the result analyses of the algorithms on different grayscale halftone images. Section V exposes the conclusion of the proposed design and its future work.

II. PREVIOUS WORK

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 the human visual system. Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994.

A. Basic Concept of (2,2) VC scheme

To illustrate the principles of VC, consider the simplest two out of two visual threshold scheme where each pixel p of the SI (Secret Image) is encoded into a pair of subpixels in each of the two shares. If p is white, one of the two columns tabulated under the white pixel in Figure.1 is selected. If p is black, one of the two columns tabulated under the black pixel is selected. In each case, the selection is performed by randomly flipping a fair coin, such that each column has 50% probability to be chosen. Then, the first two pairs of subpixels in the selected column are assigned to share 1 and share 2 respectively. Since, in each share, p is encoded into a black–white or white–black pair of subpixels with equal probabilities, independent of whether p is black or white, an individual share gives no clue as to the value of p. In addition, as each pixel is encrypted independently, no secret information can be gained by looking at groups of pixels in each share. Now consider the superposition of the two shares as shown in the last row of Figure.1, if a pixel p is white, the superposition of the two shares always outputs one black and one white subpixel, no matter which column of subpixel pairs is chosen during encoding. If p is black, it yields two black subpixels. There is a contrast loss in the reconstruction; however the decoded pixel is readily visible. Superimposing these two shares leads to the output secret as in this technique two shares are generated from the original secret image and by stacking the two shares the secret image is revealed. In this concept one white or black pixel will divide into two subpixel. The size of the shares and the size of retrieved image is double the size of input secret image [7].

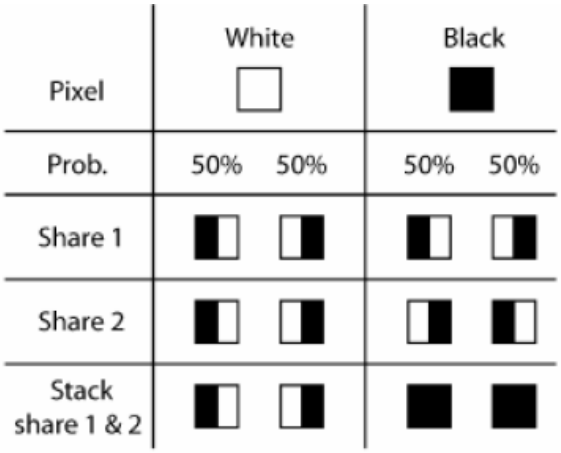


Figure1: Construction of (2,2) VC Scheme[7]

Generalization of (k, n) secret sharing scheme

Naor-Shamir[2] generalized their results by using the following theorem.

Lemma: There is a (k, k) scheme with m=2k-1, α=21-k and r= (2k-1!). We can construct a (5, 5) sharing, with 16 subpixels per secret pixel and 1 pixel contrast, using the permutations of 16 sharing matrices.

Theorem: In any (k, k) scheme, m≥2k-1 and α≤21-k.

Theorem: For any n and k, there is a (k, n) visual secret sharing scheme with m=log n 2O (k log k), α=2 - Ώ (k).

III. PROPOSED WORK

This scheme is mainly based on pixel reversal and randomization. The focus is on security and quality of the image. The algorithm employs same secret key for encryption and decryption purpose to ensure least or no degradation in image quality. It is highlighted in step no. 3 and 5.

A. Encryption Algorithm

The input to the algorithm is the secret halftone gray scale image (SI), Where SI is matrix Si j where i and j shows pixel positions and i, j= 1, 2, 3… n. All steps of algorithm are shown below.

Step 1: Pixel Si j with position i and j is the input called original pixel.

Step 2: Apply pixel reversal i.e. Si j´ = 255 - Si j

Step 3: key 1 is set and random numbers are generated (0.1 to 0.9), the generated random numbers are multiplied with Si j´ to reduce Si j´ randomly.

Step 4: Take the difference of Si j´ with original pixel Si j.

Step 5: Using same key1 the random number generated is used to reduce reversed value of Si j´.

Step 6: Apply pixel reversal i.e. Si j´´ = 255 - Si j´.

Step 7: Store in matrix as image called share 1.

Step 8: Take the difference of two random number generators with original pixel Si j.

Step9: Apply pixel reversal i.e. Si j´´´ = 255 - Si j´.

Step10: Store Si j´´´ in matrix as image called share 2

Step11: Repeat point 1 to 10 for all pixels from original image (i.e. matrix of original image).

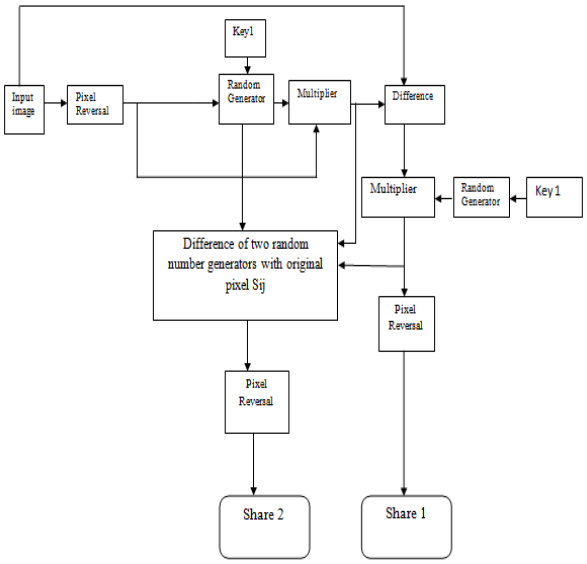


Figure 2: Block diagram of Encryption

B. Decryption

During decryption the key2 which is same as key1 is used to generate the same random numbers, by combining the two shares the image is retrieved back.

$$S= (510-S1-S2+255*r1)/ (1+r1);$$

Where S is the reconstructed image, S1 S2 are share 1 and share 2 and r1 is the random number.

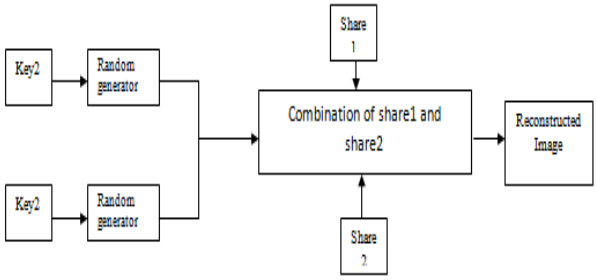
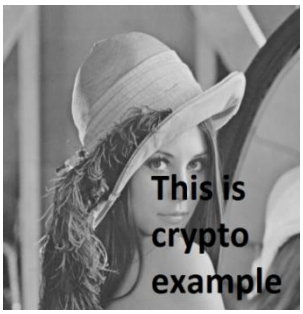


Figure 3: Block diagram of Decryption

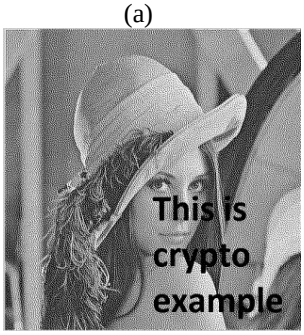
In the proposed scheme the size of the reconstructed image is same as the size of input secret image. There is no pixel expansion. The keys are introduced during encryption and decryption which boosts the security which is additional block compared to paper [7]. Only when the both key1 and key 2 values are same then the image is retrieved back, when both the key values are different the retrieved image is unable to visualize .Thus the proposed scheme is highly secured, and the quality of the reconstructed image is good. In (2, 2) visual cryptography by Naor &Shamir was implemented in [7], Where the decoded image is twice that of original secret image because the pixel p expanded into two sub pixels this effect is called pixel expansion. That affects the contrast of the resulting image. The previous work on pixel expansion and contrast optimization shows that researcher did efforts to reduce the expansion and optimize the contrast of the secret picture [8], [9]. Further they portrait the process of creating the shares using mathematical representations and mainly they focus the security and contrast condition [11]

IV RESULT ANALYSIS

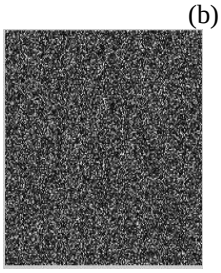
The input grayscale image is converted to halftone image by using Jarvis Halftone method. The halftone image is applied as input to the encryption algorithm.



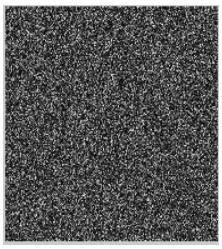
(a)



(b)



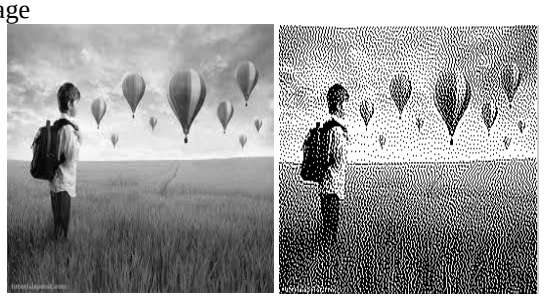
(c)



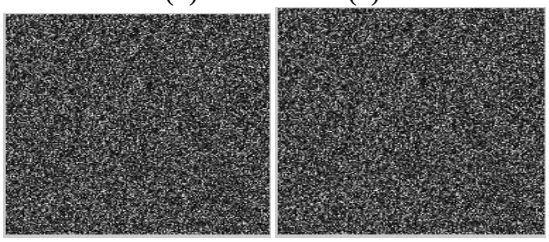
(d)

(e)

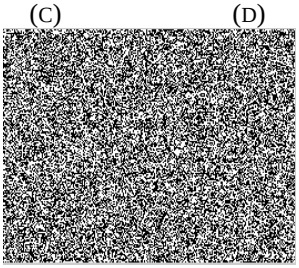
Figure 6: Results of Encryption and Decryption algorithm (a) original grayscale image (b) grayscale halftone image (c share 1 (d) share 2 (e) reconstructed image



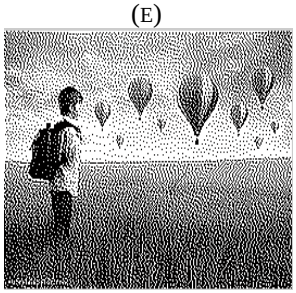
(A) (B)



(C) (D)



(E)



(F)

Figure 7: Results of Encryption and Decryption algorithm (A) Original grayscale image (B) grayscale halftone image (C) Share 1 (D) Share 2 (E) Reconstructed image with different key (F) Reconstructed image with correct key.

The algorithm was implemented in MATLAB. The simulation results of the algorithm on different secret images are seen in Figure 6 and Figure 7. Figure 6 where a secret halftone image is encrypted into high-quality halftone shares. The quality of the reconstructed image is good. The Key value must be same during Encryption and Decryption so as to generate the same random numbers at the decryption to visualize the reconstructed image. If the key value is not same we cannot reconstruct the input secret image which can be seen in Figure7 (E).Figure 7(F) shows the retrieved image when key value are same during encryption and decryption. The size of the shares and the reconstructed image is same as that the size of input secret image.

Table1: SNR for different key values

Encryption correct secret key=323	
Key value	SNR
315	0.9983
317	0.9983
321	0.9982
325	0.9983
327	0.9983
329	0.9982
323	Infinity
331	0.9982
100	0.9983
300	0.9982
500	0.9982
600	0.9982

Table 1 Lists SNR for decryption keys which are not same as encryption key. It is observed that SNR value does not give any hint about the correct key value. Hence it is difficult to break the key.

V. CONCLUSION AND FUTURE WORK

In this paper, a novel Encryption method for Grayscale Halftone Images using Random numbers is proposed. Proposed work does not alter the size of the retrieved image. Applying input halftone grayscale image to the encryption algorithm generated the shares which perfectly hides the visual information. The key introduced during encryption and decryption boosts the security. Since same key is used at the decryption, image quality remains the same.

This method can be widely used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, military etc. Further proposals include extending this method to the colour images.

ACKNOWLEDGEMENTS

We thank immensely our college management, Principal, Prof.Dr.S.Mohan Kumar, HOD, Prof. Savitri Raju,Dept of ECE for extending their support in providing us infrastructure and allowing us to utilize them in the successful completion of our research paper.

REFERENCES

[1] Rafael C.Gonzalez and Richard E. woods, "Digital Image Processing", Pearson Education, Second Edition,2005

[2] M. Naor and B. Pinkas, "Visual authentication and identification," Crypto, Lecture Notes Comput. Sci., vol. 1294, pp. 322–340, 1997.

[3] C. Chang and H.Wu, "A copyright protection scheme of images based on visual cryptography," Imag. Sci. J., vol. 49, no. 3, pp. 141–150, 2001.

[4] C.Wang, S. Tai, and C. Yu, "Repeating image watermarking technique by the visual cryptography," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol. E83A, no. 8, pp. 1589–1598, Aug. 2000.

[5] ZHQM ZMGM ZMFM. —G. JULIUS CAESAR. XYAWO GAOOA GPEMO HPQCW IPNLG RPIXL TXLOA NNYCS YXBOY MNBIN YOBTY. QYNAI.— JOHF. KENNEDY. "Cryptography", www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf

[6] Adi Shamir, How to Share a Secret, published in ACM, Laboratory for Computer science, Massachusetts Institute of Technology, 1979.

[7] Ch.Ratna Babu, M.Sridhar, Dr. B.Raveendra Babu, "Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security" 978-1-4673-5986-3/13/$31.00 ©2013 IEEE

[8] C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson, Contrast optimal threshold visual cryptography schemes, SIAM J. on Discrete Math. 16, 2003, 224-261.

[9] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, On the Contrast in Visual Cryptography Schemes, Journal of Cryptology: the journal of the International Association for Cryptologic Research, 1996

[10] Stelvio Cimato, Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci, Ideal contrast visual cryptography

[11] Jim Cai, A Short Survey On Visual Cryptography Schemes,2004,http://www.cs.toronto.edu/~jcai/paper.

[12] M.Naor and A.Shamir.Visual cryptography, advances in cryptology. Eurocrypt 94 Proceeding LNCS, 950: 1–12, 1995.

◈◈◈