International Journal of Computer Engineering
and Technology (IJCET), ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online) Volume 1
Number 2, Sep - Oct (2010), pp. 133- 146
© IAEME, http://www.iaeme.com/ijcet.html

IJCET
©IAEME

A SELF RECOVERY APPROACH USING HALFTONE IMAGES FOR MEDICAL IMAGERY SYSTEM

John Blesswin
Computer Science and Engineering
Karunya University, India
E-Mail: johnblesswin@gmail.com

Rema
Computer Science and Engineering
Karunya University, India

Jenifer Joselin
Computer Science and Engineering
Karunya University, India

ABSTRACT

Security has become an inseparable issue even in the field of medical applications. Communication in medicine and healthcare is very important. The fast growth of the exchange traffic in medical imagery on the Internet justifies the creation of adapted tools guaranteeing the quality and the confidentiality of the information while respecting the legal and ethical constraints, specific to this field. Visual Cryptography is the study of mathematical techniques related aspects of Information Security which allows Visual information 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 represents the secret image by several different shares of binary images. It is hard to perceive any clues about a secret image from individual shares. The secret message is revealed when parts or all of these shares are aligned and stacked together. In this paper we provide an overview of the emerging Visual Cryptography (VC) techniques used in the secure transfer of the medical images over in the internet. The related work is based on the recovering of secret image using a binary logo which is used to represent the ownership of the host image which generates shadows by visual cryptography algorithms.

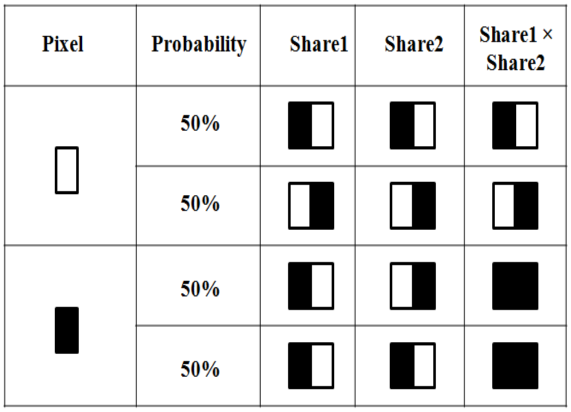
An error correction-coding scheme is also used to create the appropriate shadow. The logo extracted from the half-toned host image identifies the cheating types. Furthermore, the logo recovers the reconstructed image when shadow is being cheated using an image self-verification scheme based on the Rehash technique which rehash the halftone logo for effective self verification of the reconstructed secret image without the need for the trusted third party (TTP).

Index Terms—Visual secret sharing, Medical image, Halftoning, Verifying shares, Cryptography

INTRODUCTION

The rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Nowadays, the transmission of medical information has become very convenient due to the generality of Internet. The current needs in medical imaging security come mainly from the development of the traffic on Internet (tele-expertise, tele-medicine) and to establishment of medical personal file. Various confidential data such as the secure transfer medical images are transmitted over the Internet. Internet has created the biggest benefit to achieve the transmission of patient information efficiently. However, it is easier that the hackers can grab or duplicate the medical information on the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize this weak link over communication network to steal the information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed.

Visual cryptography scheme [4] eliminates complex computation problem in decryption process thus enabling the transfer of medical images in a more convenient, easy and secure way. Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Visual cryptography (VC), proposed by Naor and Shamir [1], is a method for protecting image-based secrets that has a computation-free decryption process.



Pixel	Probability	Share1	Share2	Share1 × Share2
□	50%	◧	◧	◧
	50%	◨	◨	◨
■	50%	◧	◨	■
	50%	◧	◧	■

Figure1 Construction of (2, 2) VC Scheme

If ‘p’ is white, one of the two columns under the white pixel in Figure 1 is selected. If p is black, one of the two columns under the black pixel is selected. In each case, the selection is performed randomly such that each column has 50% probability to be chosen. Then, the first two pairs of sub pixels in the selected column are assigned to share 1 and share 2, respectively. Since, in each share, p is encrypted into a black–white or white–black pair of sub pixels, an individual share gives no clue about the secret image [2].

By stacking the two shares as shown in the last row of Figure 1, if ‘p’ is white it always outputs one black and one white sub pixel, irrespective of which column of the sub pixel pairs is chosen during encryption. If ‘p’ is black, it outputs two black sub pixels. Hence there is a contrast loss in the reconstructed image. However the decrypted image is visible to naked eye since human visual system averages their individual black–white combinations. The important parameters of this scheme are,

a) Pixel expansion ‘m’, which refers to the number of pixels in a share used to encrypt a pixel of the secret image. This implies loss of resolution in the reconstructed image.

b) Contrast ‘α’, which is the relative difference between black and white pixels in the reconstructed image. This implies the quality of the reconstructed image. Generally, smaller the value of m will reduce the loss in resolution and greater the value of ‘α’ will increase the quality [3] of the reconstructed image. As mentioned above if ‘m’ is decreased, the quality of the reconstructed image will be increased but security will be a problem. So research is focused on two paths,

1. To have good quality reconstructed image.
2. To increase security with minimum pixel expansion.

GENERATION OF HALFTONE IMAGES

A. Error Diffusion Technique

Error diffusion is a type of halftoning in which the quantization residual is distributed to neighbouring pixels that have not yet been processed. The simplest form of the algorithm scans the image one row at a time and one pixel at a time. The current pixel is compared to a half-gray value [6]. If it is above the value a white pixel is generated in the resulting image. If the pixel is below the half way brightness, a black pixel is generated. The generated pixel is either full bright, or full black, so there is an error in the image. The error is then added to the next pixel in the image and the process repeats as illustrated in Figure 2. The simple and attractive concept of this technique is the diffusion of errors to neighbouring pixels; thus, image luminance is not lost. The diffused image is generated based on an error diffusion strategy also called an error filter. Each error filter has a set of kernel weights.

The kernel weights of Floyd and Steinberg's error filter are 7/16, 5/16, 3/16, and 1/16, shown in Figure 3. After a quantization procedure, a pixel GI(x,y) at position (x,y) in grayscale image GI(x,y) [6] becomes HI(x,y) and has a value of either 0 or 255.The threshold TH is used to determine HI(x,y) and the quantization error is determined as E(x,y) = GI(x,y) - HI(x,y). A signal consisting of past error values is passed through the error filter to produce a correction factor that is added to future input pixels. If the quantization error is negative, GI(x,y) is quantized as 255 so that the corresponding HI(x,y) is set as 255[16] and its neighbouring pixels values must be decreased. In contrast, the value of GI(x,y) is quantized to zero, and its neighbouring pixels values must be increased.

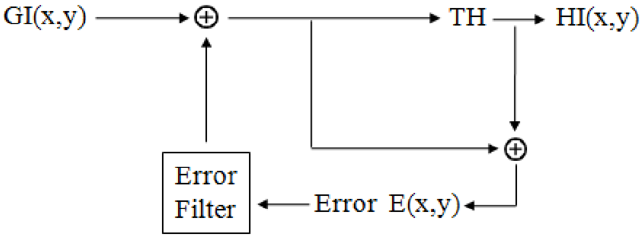


Figure 2 Flowchart of Error Diffusion architecture

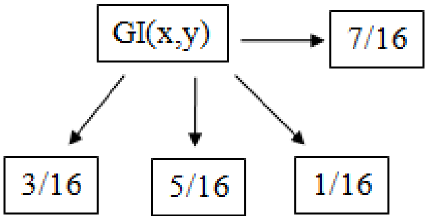


Figure 3 Kernel weight of Floyd and Steinberg's Error Filter

First, Set (x,y) as (1, 1); that is, the first pixel is taken into consideration. Then Compute error value E(x,y) = GI(x,y) - HI(x,y) and corresponding pixel value HI(x,y) in the halftone image [8] for pixel located at coordinates (x,y) in grayscale image GI. Diffuse error E(x,y) over four neighbouring pixels. The four neighbouring pixels altered in this equation are GI (x,y+1) , GI(x+1,y- 1), GI(x+ 1,y), and GI(x+ 1,y+ 1). Their modified values are computed based on the kernel weight of the error filter as shown in Figure 3 demonstrates the kernel weight of Floyd and Steinberg's error filter.

PROPOSED SCHEME

This section presents a detailed description of a novel VSS scheme, called a self recovery approach, proposed for grayscale images [6] that can be applied to the images used in the medical applications. The images used in the medical would be color images [5]. In this case, first, a color image is decomposed into three sub-images: red, green and blue. Secondly, the scheme is applied independently to each sub-image individually. Lastly, the reconstructed secret color is generated by concatenating the three reconstructed grayscale components together [10].

This technique can be used to convert these medical color images [5] to gray scale and apply the VSS scheme. In our proposed scheme, a halftone image HI [8] is created from the grayscale secret image GI (medical image) by using an error diffusion technique.

A half-sampled image of the halftone image HI [8], called a halftone logo HL, is created by using an interpolation technique [12]. In our scheme, the halftone logo HL is used to ascertain the reliability of the reconstructed grayscale secret image [10] GI and the judiciousness of the set of collected shadows as shown in Figure 4. Full details of generating a reconstructed gray scale image and self recovering the grayscale image is presented in four steps as follows.

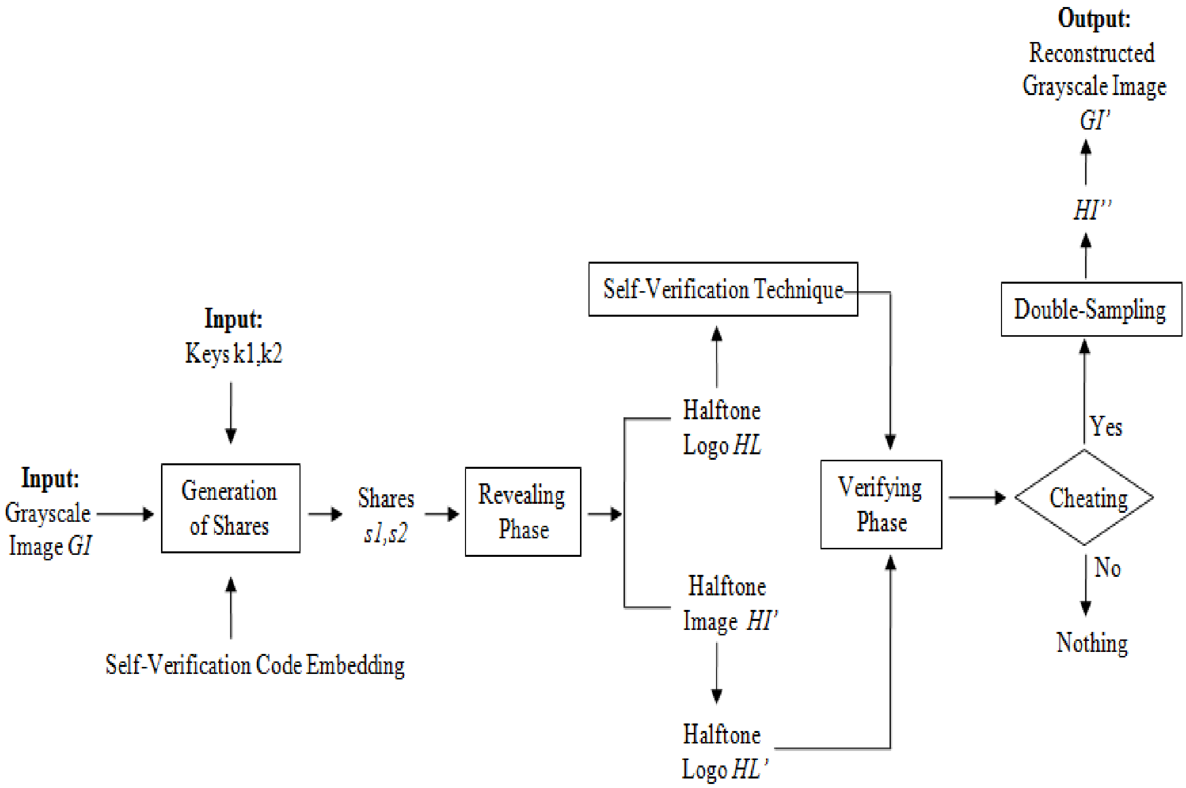


Figure 4 Flowchart of proposed scheme

A. Generation of Shares

Shadows are created for medical-image in the Share construction step. In this step Apply the error diffusion technique to the grayscale image GI to retrieve a halftone image HI, the width and height of HI are W and H. The halftone logo [7], named HL, which is a half-sample of HI, is created by using the interpolation [12] and error diffusion techniques. In this step, the halftone logo HL is shrunk to one-half of halftone image HI in each dimension. Randomly generate two symmetric keys K1 and K2. Encrypt pixels of HL with key K1 and symmetric cryptographic algorithm, such as DES, when pixels are located at even rows of halftone image HL, and then encrypt pixels of halftone image HL with key K2 and symmetric cryptographic algorithm when pixels are located at odd rows of halftone image HL to derive the encrypted halftone logo HL. Then generate the shares using image clustering, interpolation techniques [13] and the key will be embedded into the shares.

B. Self-Verifying code Embedding Phase

A half-sampled image of the halftone image HI [8], called a halftone logo HL, created by using an interpolation technique [13] is rehashed using the first level rehash technique of the Self-verifying code embedding. This technique generates a binary self-verification code for every pixel and inserts the code back into the rightmost two bits of every pixel, and thus a halftone logo with self-verification capabilities can be produced as shown in Figure 5.

For the purpose of explanation, we assume that the size of the halftone logo (HL) [7] is n x n, with 8-bit resolution. The following is the three stages to equip halftone logo with the self verification capabilities:

Step1: Substitution

First, we replace the rightmost two bits of every pixel with 0 to generate a transformed halftone image (HL') based on the simple LSE substitution scheme. From the images we can found 2-bits substitution can make sure images with high quality compared with 4-bits substitution.

Step2: Generating Hit values

We then generate a secure key SK, and use the MHIT procedure of the first level rehash model to treat every pixel value of HL' as the key in the key space. A fad is worth mentioning is that in rehash technique the assumed key values to be non-equal in defining the key space when they built the perfect hash scheme. Pixel values can be identical in a certain halftone logo image, in other words, the keys in the key space could be the same. This scheme generates a self-verification code for the halftone logo, not to locate a unique corresponding position in the address space for them. We follow the definition of keyed hash function to randomly select three keyed hash functions. The values are expressed in binary form.

Step 3: Embedding

The HIT value will then be orderly embedded back into the rightmost two bits of every pixel to generate a halftone logo image (HL) with self-verification capabilities [15]. After the above three steps, every pixel goes through substitution and the modified HIT construction procedure, and then the corresponding HIT values can be derived. If, at a later date, the same HIT values are obtained after the pixels go through the same processes, we can conclude that the pixels have not been tampered. If different HIT values are derived, then the pixels have been tampered. Due to the number of keyed hash functions is related to the number of self-verification codes which are not zero, in other words and then image receivers can identify the illegal tampering from attackers more easily. To increase the effectiveness of self-verification codes, sender and receiver can generate more keyed hash functions. However, it will increase the transmission load. Based on Du et at's original concept of first level rehash scheme, we suggest halftone image senders at least use three keyed hash functions to guarantee the effectiveness of the self-verification codes.

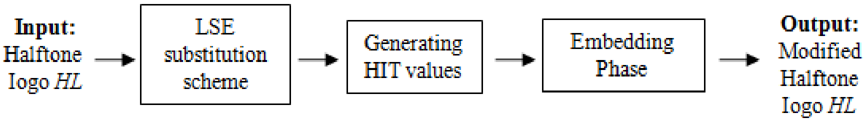


Figure 5 Self-Verification Code Embedding

As to the keys which are used in each keyed hash functions, they can be identical or different. Even all key are same, they still will not decrease the effectiveness of self verification codes. In the previous self verifying scheme the dealer must register his/her issued logo with the trusted third party (TTP) before s/he distributes the shadows to participants during the shares construction phase. After receiving the logo, the TTP checks whether the logo is the same as the half-sampling result of the halftone secret image. If they are the same, the TTP accepts the dealer’s request; otherwise, the TTP rejects the dealer’s request. This paper introduces an image self-verification scheme based on modified Du et al’s first level rehash [14] scheme which rehash the halftone logo for effective self verification of the reconstructed secret image without the need for the trusted third party(TTP).

C. Revealing Phase

This section describes in detail how to extract the halftone logo HL and the reconstructed secret grayscale GI [10] from the set of collected shadows. By using the reversible data hiding scheme [9] , the first key K1 and the intermediate shadow S1 are derived from the shadow SH. Similarly, the second key K2 and the intermediate shadow

S2 are derived from the shadow SH2. Then Divide the first intermediate shadow S1 into non-overlapping 7-pixel blocks. Then, multiply each 7-pixel block by a P (7, 4) Hamming code. Based on X blocks divided from 7×X pixels in the intermediate shadow S1, we obtain a set of X blocks, with each block consisting of 3 bits. By combining these X blocks, reconstruct the encrypted halftone logo eHL'.

Decrypt extracted encrypted halftone image HL by using keys K1 and K2 for pixels located in even rows and odd rows in the encrypted halftone image HL, respectively. After the decryption is completed, the extract halftone image HL' is obtained. Create the halftone image HI by performing the XOR operation on the intermediate shadows S1 and S2. Because the intermediate shadows S1 and S2 are binary images containing 7×X pixels, where X= [(W×H)/7], HI' is a binary image consisting of 7×X pixels. Apply the inverse halftoning technique ELIH to the halftone image HI' to generate the intermediate reconstructed image.

D. Verifying Phase

This phase verifies the reliability of the reconstructed secret image and the set of collected shadows. The halftone image HI, which is generated from in the revealing phase, perform the half-sampling by applying error diffusion and interpolation techniques [13] to retrieve another halftone image, called HI. In this phase the halftone logo HL generated from the halftoned image HI is rehashed using the rehash technique [14] which generates a binary self-verification code for every pixel and insert the code back into the rightmost two bits of every pixel, thus an halftone logo with self-verification capabilities is formed.

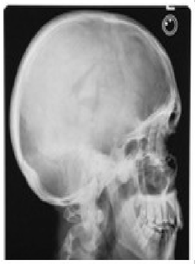
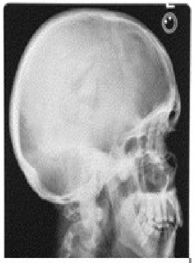
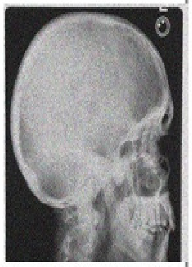
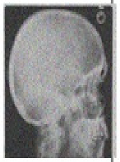
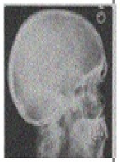
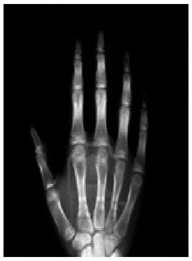
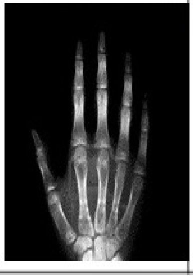
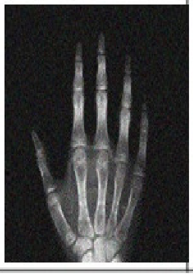
The HL is the extracted halftone image whose original image is the halftone logo HL` and HL is the half sampled image of HI. The reconstructed halftone logo HL depends on the intermediate shadow S1, which is only extracted from shadow SH1. If there is no cheating, the intermediate shadow S1 in the revealing phase is the same as the intermediate shadow S1 in the shares construction phase. In other words, the halftone logo HL` is the same as halftone logo HL when no cheating occurs [11].

E. Image Recovering Phase

This phase recovers the reconstructed secret image when the shadow is being cheated. The cheated image is recovered by applying Double-Sampling and Inverse halftoning [13]. In this first, find the value of d which is the difference between HL` and HI``, d = HL` - HI``. When the value of d is equal to zero, then the reconstructed secret image GI (medical image) is generated completely from HI` by inverse halftoning transformation.

Obviously, when d is not equal to zero, if a fake shadow drops in the first shadow, the reconstructed image GI` is usually a noise-like image and extracted halftone logo HL` is either a noise-like image or a meaning halftone image. If the fake shadow is the second one, a noise-like image GI` is generated in addition to a meaning halftone image HL`[8]. In this case, we not only know that GI` is fake but also can recover GI` by using HL`.

Table 1 Reconstructed image quality and reliability conclusion when no cheating is detected

GI	*GI'*	*PSNR (db)*	*HI'*	*HI''*	*HL'*	*MSE*	*Reliability*
		34.85				0	Sure
		34.54				0	Sure

To recuperate GI from HL`, we first perform double-sampling by applying an interpolating operation into HL` to retrieve HI`.

EXPERIMENTAL RESULTS

Experimental results on medical images demonstrate three objectives. Thus more than 100 medical images have been tested. Sample tested medical images are given in Table 1. The first is the generation of the constructed secret image with high quality, with no computational complexity and no pixel expansion. The second is the reconstruction of images and verification of the reliability of the set of collected shadows as well as the reconstructed secret image. In our scheme, peak signal-to-noise ratio (PSNR) is used to evaluate the quality of the reconstructed original image GI`. Similarly, we use mean square error (MSE) to identify the difference between the extracted halftone logo HL` and halftone image HI``. The reliability of the VSS scheme is guaranteed if MSE is equal to zero. The third objective is the image self-verification code embedding phase for the reliability of HL followed by the recovering of images. Experiments were based two assumptions corresponding to two circumstances. The first circumstance assumes that neither the dealer nor the participants are cheating. If the MSE value of HI and HL is zero, the parameter is "Sure," and vice versa. The quality of the reconstructed secret image is considered by using two points of view. First, under the human visual system, the reconstructed secret image GI is almost indistinguishable from the original image GI. Secondly, the PSNR values of the reconstructed secret images and the original images range from 32 to 34.5 dB. Moreover, all MSEs are equal to zero when no cheating occurs. The reconstructed images can be assumed to be completely believable.

CONCLUSION

In this paper, we propose a novel self-verifying VSS for both grayscale and color images that are used in medical applications. Our scheme not only protects an original medical secret image by dividing it into n shadows but also verifies the reconstructed medical secret image and identifies the cheating types using the self verifiable rehash technique when some of collected shadows are forged during the revealing process. Moreover, the original reconstructed medical secret image is established only when k out of n valid shadows are collected and no one can force the honest participant to reconstruct a wrong secret image. Error diffusion, image clustering, and inverse halftoning are three techniques employed as foundation of this scheme. Based on the Boolean operator XOR, this mechanism can easily recover the reconstructed medical image from the collected shadows without adding computational complexity in the revealing and verifying phase. Thus, it is best to use for images used in the medical applications for transferring images over the Internet.

ACKNOWLEDGMENT

The Authors would like to thank the Innovative Transtar Research Team in Karunya University, for supporting us in our research work.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[2] D. Jena, and S. K. Jena, "A Novel Visual Cryptography Scheme", The 2009 International Conference on Advanced Computer Control, pp- 207-211, 2009.

[3] C. Blundo, P. D'Arco, A. D. Snatis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM Journal on Discrete Mathematics, available at: http://citeseer.nj.nec.com/blundo98contrast.html vol. 16, no. 2, pp. 224–261, April 1998.

[4] Er. Supriya Kinger "Efficient Visual Cryptography," Journal Of Emerging Technologies In Web Intelligence, Vol. 2, No. 2, Page(s): 137-141, 2010.

[5] D.Jin, W.Yan and M.S. Kankanhalli, ''The Progressive color visual cryptography,'' SPIE Journal of Electronic Imaging (JEI/SPIE), Jan 4, 2004.

[6] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recognit. Lett., vol. 24, pp. 349–358, Jan. 2003.

[7] S. H. Kim and J. P. Allebach, "Impact of HVS models on model-based halftoning," IEEE Transactions on Image Processing, vol. 11, pp. 258–269, Mar 2002.

[8] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo "Halftone Visual Cryptography Via Direct Binary Search," 14th European Signal Processing Conference (EUSIPCO 2006), September 4-8, 2006.

[9] Jing-Ming Guo and Jyun-Hao Huang "Data Hiding in Halftone Images with Secret-Shared Dot Diffusion," Proceedings of 2010 IEEE International Symposium, Issue Date: May 30 2010 -June 2 2010 , page(s):1133-1136, 03 August 2010.

[10] Nagaraj V. Dharwadkar1, B.B. Amberker2, Sushil Raj Joshi3 "Visual Cryptography for Gray-Level Image using Adaptive Order Dither Technique," Journal of Applied Computer Science, no. 6 (3) /2009, Suceava.

[11] HU Chih-Ming, TZENG Wen-Guey , " Cheating prevention in visual cryptography", IEEE transactions on image processing, ISSN 1057-7149 ,2007, vol. 16, no1, pp. 36-45.

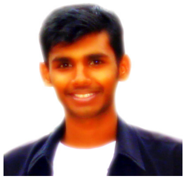
[12] Anthony parker, Robert .V, Kenyon and Donald E. Troxel " Comparison Of Interpolating Methods For Image Resampling," IEEE transaction on medical imaging vol.mi-2,no.1 March 1983.

[13] Miklos .P "Comparison of Convolutional Based Interpolation Techniques in Digital Image Processing," 5th International Symposium, Digital Object Identifier: 10.1109/SISY, 204342630, Pages: 87 – 90, 2007.

[14] M.W Du, T.M Hsieh, K.F. Jea, D.W Shieh, "The Study of a New Perfect Hash Scheme," Software Engineering, IEEE Transactions on Volume: SE-9 , Issue: 3 Digital Object Identifier: 10.1109/TSE.1983.236866 , Page(s): 305 – 313,1983.

[15] Ching-Sheng Hsu, Shu-Fen Tu "Finding Optimal LSB Substitution Using Ant Colony Optimization Algorithm," . ICCSN '10 Second International Conference on Communication Software and Networks, 2010, Digital Object Identifier : 10.1109/ICCSN.2010.61 ,Page(s): 293 – 297, 2010.

[16] N. D. Venkata and B. L. Evans, "Adaptive threshold modulation for error diffusion halftoning," IEEE Trans. Image Process., vol. 10, no. 1,pp. 104–116, Jan. 2001.



John Blesswin received the B.Tech degree in Information Technology from Karunya University, Coimbatore, India, in 2009. He passed B.Tech examination with gold medal. He has been doing M.Tech Computer Science and Engineering at Karunya University. His research interests include visual cryptography, visual secret sharing schemes, image hiding and information retrieval.

Rema received the B.E degree in Computer Science and Engineering from Vins Christian College of engineering, Nagercoil, Kanyakumari district in 2009. She has been doing M.Tech Computer Science and Engineering at Karunya University. Her research interests visual cryptography scheme and visual secret sharing scheme.

J. Jenfier Joselin received the M.Tech degree in Computer Science and Engineering from Karunya University, Coimbatore, India, in 2008. She is working as a lecturer in CSE dept in Karunya University since May 2008. Her research interests include image compression, software architecture and visual cryptography schemes.