International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

VCS & Lifting Wavelet Scheme Based Digital Image Security Technique

Amit Kumar Sharma[1], Aman Kumar[2]

[1,2]Department of Computer Science and Engineering,
L.R. Institute of Engineering and Technology
Solan, Himachal Pradesh (India)

ABSTRACT

In this paper, a two layer technique for securing digital images is proposed. The two techniques used are visual cryptography (VC) scheme and int-to-int wavelet transform (IWT). (2,2) –VC scheme is used to split the secret image into two shares. Next, the IWT is used to decompose the image into its sub bands and the secret image shares are stored in the HH band of the decomposition. The performance is measured by computing peak signal to noise ratio, mean square error and cross-correlation coefficient.

***Keywords*— Image Encryption, Visual Cryptography, Watermarking.**

I.INTRODUCTION

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, such as document, image, audio, and video. Therefore, the protection of rightful ownership of digital data has become an important issue in recent years. Nowadays, researchers have proposed many techniques to protect the intellectual property rights for digital images. Digital watermarking, a kind of such techniques, is a method that hides a meaningful signature, or the so-called digital watermark, in an host image for the purpose of copyright protection, integrity checking, and captioning. When the rightful ownership of the image needs to be identified, the hidden watermark can be extracted for the ownership verification.

Over the years various researchers have proposed numerous methods for securing digital images for transmission. Naor et. al. [1] proposed a visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into n noise-like shares. The secret image can be decrypted by the human eye when any k or more shares are stacked together. The greatest advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is a simple and safe secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the share-images are larger than the original secret image. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry. Since the concept of visual cryptography was first proposed, there have been several studies making efforts to

deal with the pixel expansion problem [2-11]. Most of these have fallen into the category of probability visual cryptography schemes.

Ito et al. [2] and Yang [5] used the concept of probability to interpret the meaning of the Boolean matrices proposed by the conventional VC and proposed a pixel non-expansion method suitable for binary images. However, the random nature of probability means that the shares have poor display quality. Tu and Hou [4] adopted Ito's method [2] but utilized multiple successive pixels in the secret image as the unit of encryption. They generated smooth-looking shares of invariant size for gray-level secret images.

In 1987, Kafri and Keren [6] proposed a random grid visual secret sharing (RGVSS) method, which has gained more attention over the years. In their method, each pixel of the image is treated as a grid, with a random variable used to encrypt the secret image. The biggest benefit of the RGVSS method for encryption is that it generates unexpanded share-images. In 2007 Shyu [7] extended Kafri and Keren's RGVSS model, proposing three different models utilizing a (2,2)-threshold scheme. Shyu [8] and Chen and Tsao [9] also presented (2, n)- and (n, n)-threshold RGVSS schemes, so this method is no longer limited to the (2, 2)-threshold scheme. Both traditional VC and RGVSS produced meaningless share-images, which can create some management problems for those participating in many secret sharing projects because they have to keep track of many different share-images.

Moreover, transmission of a meaningless image can arouse the suspicion of an outsider, who may realize that this image may carry some type of secret message. This attracts attention and could strengthen their desire to uncover the secret image, thus reducing the security of the share-image. Ateniese et al. [13] first applied the strategy of steganography to generate meaningful share-images in VC. Following Ateniese, Hou and Wu [14] proposed a method which uses the halftone and color composition/decomposition techniques to generate meaningful grey or color share-images. Zhou et al. [15] and Wang et al. [16] also improved upon Ateniese's method by developing VC algorithms for dealing with halftone images designed to make the recovered stack-image less unclear. Chang et al. [17] found a way to hide a color secret image in two color cover images.

Nakajima and Yamaguchi [18] presented a scheme for encrypting a natural image. All of above methods used pixel expansion method to generate meaningful color share-images. For example, with the methods of Chang et al. [17] and Nakajima and Yamaguchi [18], pixel expansion made the share images nine times larger than the original image. Fang [19] proposed a progressive VC scheme which could also produce meaningful share-images, but pixel expansion meant that they were still four times larger than the original image. Thien and Lin [20] proposed a pixel non-expansion method that could produce a meaningful share-image but a computer was needed to decrypt the secret image, losing the advantage of visual cryptography which is decryption directly by the human eye.

Chen and Tsao [10] first proposed a user-friendly random grid visual secret sharing (Friendly RGVSS) method which achieved the goal of producing meaningful share-images and pixel non-expansion, but their method still had many restrictions. In that method, pixels are taken from the secret image and the cover image to generate the needed share-images. The result is that the contrast in the stack-image and share-images is not as good as that obtained with methods that use all the pixels to display the secret image or the cover image (e.g., Ateniese et al.'s EVCS). In extreme situations, when an insufficient number of black pixels are taken from the secret image,

it may be impossible to display the content of the secret-image in the stack-image. In addition, with this method, only one picture can be used as the cover image, and the colors of the two share-images must be complementary to each other.

Lou et al. [11] proposed a visual secret sharing scheme capable of hiding a secret image and an extra confidential image within two meaningful cover images. The two share-images could be stacked to obtain the secret image without any complex computation. The shifting of one of the share-images by a certain unit could allow the receiver to obtain an extra confidential image with which to check the validity of the revealed secret image. However, with this system the visual quality is poor, because of the extra image hidden in the share-images, and the cover image cannot be concealed when the share-images are stacked. All these disadvantages reduce the visual quality of the share-images and the stack-image. Lee and Chiu [12] proposed an extended visual cryptography algorithm for general access structures to create unexpanded meaningful shares to hide a secret image. It operates in two phases. In the first phase, based on a given access structure and conventional VC schemes, meaningless shares are constructed by using an optimization strategy. In the second phase, cover images are directly added to each share by a stamping algorithm to generate meaningful shares. However, the ratio of incremental pixel density of the cover image to be stamped on the shares will heavily influence the contrast in the share-images and the stack-image. Increasing the contrast of the share-image will always decrease the contrast of the stack-image, and vice versa.

Apart from cryptographic encryption schemes as discussed above, watermarking is another method to secure image. Many researchers have used this technique for security purposes. Digital watermark is a kind of technology that embeds copyright information into multimedia data. According to watermark embedding position, digital watermark could be divided into two main kinds of spatial domain and frequency domain. Spatial domain digital watermark has more data quantity and more frangible than frequency domain digital watermark so that the research of digital watermark is centralized in frequency domain. Wavelet transform is a new time-frequency analyzing method to localize spatial and frequency domain. Many watermark algorithms are implemented in discrete wavelet transform (DWT) domain.

Peyman et. al. [21] proposed a technique to protect digital identity documents against a Print Scan attack for a secured ID card authentication system. The existing PS operation imposes several distortions, such as geometric rotation & histogram distortion on the watermark location which may cause the loss of information. The proposed system removes distortion of the PS operation: filtering, localization, binarizitation, rotation and cropping. The proposed authentication system extracts the watermarks inside the ID card‘s holder photo, place in the decoder and then checks it out with the ID card personal number. If the extracted watermark and the ID card personal number are the same, the identity of the user / customer will be verified otherwise identity will be denied.

Swathi etl al. [22] proposed a technique in which binary image was the watermark. In the frequency domain, the embedding process on QR code image using watermark is performed. The QR code image is decomposed by one level using one dimensional wavelet transformation.

Suhail et. al. [23] proposed a watermarking algorithm based on the discrete cosine transform (DCT) and image segmentation. The image was first segmented in different portions based on the Voronoi diagram and features

extraction points. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment.

Tianming et. al. [24] presented a digital watermarking algorithm based on the DWT coefficients. This algorithm does not change any information of the original image, but combines the information of low frequency DWT coefficients and the watermark image. The combination is the key, which is used to extract the watermark. When we need to extract the watermark, we can obtain it by divide the key.

Yang et. al. [25] proposed a watermarking algorithm based on integer wavelet transform (IWT). Instead of hiding data bits directly to the blocks, authors employed adaptive bit-labeling scheme to a block so that it can be used to carry a data bit 0 or 1.

In this work, random-grid-based (2,2) Visual Cryptography scheme is used to split an image into two meaningless shares. Then, the int-to-int DWT is used to decompose a cover image and the shares are embedded into Diagonal Detail component to the decomposition to give watermarked image. The details of Visual cryptography and watermarking using IWT is discussed in the Section II. Section III discusses methodology. Section IV outlines the results and performance measures. Section V concludes this paper.

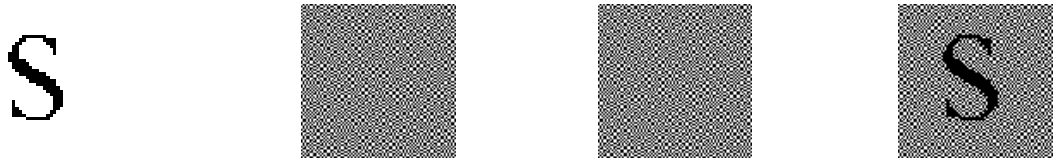
II.TECHNIQUES

In this section, (2,2) Visual Cryptography scheme and watermarking using int-to-int DWT are discussed. Along with these, watermarking using DCT for comparison is also explained.

A. (2,2) Visual Cryptography Scheme

Visual Cryptography (VC) is a method of encrypting a Secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to simply stack shares and view the Secret image that appears on the stacked shares.

To encode a secret employing a (2, 2) VC Scheme, the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two or four sub-pixels as shown in Fig.1. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is Xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret as shown in Fig. 1.



(a) (b) (c) (d)

Fig. 1 An illustration visual cryptography scheme

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

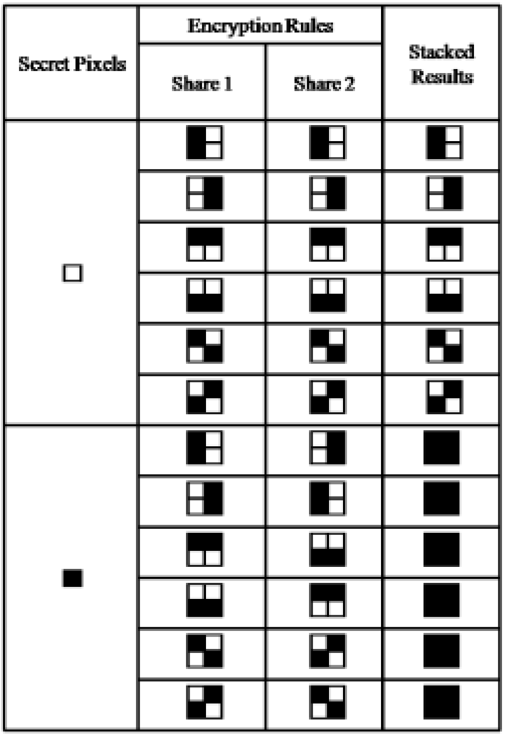
4: (k, n) – Threshold VCS:

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.

A VSS scheme is constructed for an access structure, (Qual, Forb), which specifies how the secret is shared among the n participants. Qual denotes the family of qualified sets, and Forb denotes the family of forbidden sets. Participants belonging to a qualified set can see the secret through stacking their transparencies together, and those belonging to a forbidden set cannot perceive any information from the stacked image. Take a 2-out-of-2 VSS scheme for example. There are two participants {1, 2}, and Qual = {{1, 2}} and Forb = {{1}, {2}}. Table 1 is an illustration of a 2-out-of-2 VSS scheme.

TABLE I

ENCRYPTION RULES



There are six encryption rules for a white (resp. black) pixel. For each time of encoding a white (respblack) pixel, we randomly choose one of the encryption rules and split the pixel into two shares according to the selected rule. To decode the secret, we just stack the two shares to see the secret on the stacked result. Generally speaking, the encryption rules must satisfy the contrast and security condition. The contrast condition means that there must be a contrast between the stacked result of a white pixel and that of a black pixel if the shares come from a qualified set, while the security condition means that there must be no difference between the stacked result of a white pixel and that of a black pixel if the shares come from a forbidden set.

In this work, (2,2) – VCS scheme is used with four sub pixels for each pixel in original binary image.

B. Digital Watermarking using IWT

Discrete wavelet transform performs multi-stage signal decomposition. Discrete wavelet transform using filter bank is shown in Fig. 2.

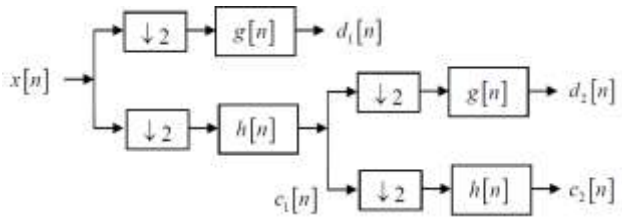


Fig. 2 DWT Forward Transform Filter Bank

In this section, fast and efficient way of finding discrete wavelet transform using lifting scheme is discussed. It de-correlates the signal at different resolution level. Basic polynomial interpolation is used to find high frequency values. It is also used to construct scaling functions in order to find out low frequency values. Lifting scheme for Integer Wavelet Transform consist of three steps as shown in Fig. 3.

- Split (Lazy wavelet transform): This stage splits entire set of signal into two frames. One frame consists of even index samples and the other frame consists of odd samples
- Predict (Dual lifting): The even and odd samples are interleaved. If the signal is having locally correlated structure, then even and odd samples are highly correlated. In that case, it is very easy to predict odd samples from even samples.
- Update (Primal lifting): The coarser signal must have same average value that of original signal. To do this, we require lifting with help of wavelet coefficients. In order to maintain same properties among all the coefficients throughout all the levels, we require to find out some scaling function. In update phase, scaling function is calculated from previous value of wavelet coefficients.

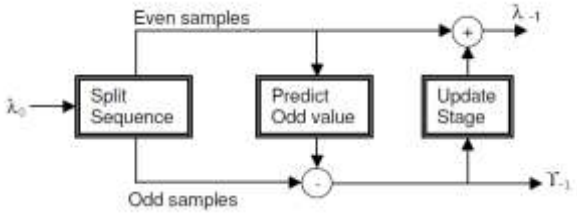


Fig. 3 IWT Forward Transform

To obtain an efficient implementation of the discrete wavelet transform, it is of great practical importance that the wavelet transform is represented by a set of integers. Because if we store wavelet coefficients as a floating point values it requires 32 bits per coefficients. Hence, wavelet coefficients are rounded to convert it into integer number for efficient encoding and storage. Because of this rounding process, the original signal cannot be reconstructed from its transform without an error. Using lifting scheme of wavelet transform, rounding error is cancelled during the inverse transform. Hence, it is possible to achieve perfect reconstruction.

III.METHODOLOGY

The proposed algorithm involved two parts. First, (2,2) - Visual Cryptography Scheme for encryption and second, cryptography using Integer to Integer DWT (Lifting Scheme). Algorithm of both the steps are discussed as follows:

A. Steps for Visual Cryptography

1) Read the secret image (black & white).

2) Initialize two primary blocks which are complement to each other for creating shares. An example is

$$block\ 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$block\ 2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (1)$$

If these blocks are used, the shares will be twice the size of the secret image i.e., for each pixel in the secret image, there will be four pixels in each share.

3) Repeat the following for each pixel in the secret image,

a. If the pixel in secret image is 1, assign the corresponding four pixels in both the shares as block 1 or block 2 with equal probability.

b. If the pixel in secret image is 0, assign the corresponding four pixels
in share 1 as block 1 or block 2 with equal probability.
and in share 2 as block 2 or block 1 with equal probability.

4) Combine both the shares by concatenating the shares vertically.

B. Steps for Encryption using Integer to Integer DWT (Lifting Scheme

1) Read the watermark image.

2) Compute the int-to-int DWT of the watermark image.
Parameters of Lifting Scheme:
Type : int2int

Wavelet : haar

Primal elementary lifting step: -0.125 , 0.125

3) Embed the combined share data in the Diagonal Detail component (HH component).

4) Now, reconstruct the image using the new Diagonal Detail component.

IV. RESULTS

Fig. 4. shows the secret image which is used for simulation. Fig.5 shows the cover image which is used in the cryptography phase. The image shown in Fig. 4 is split into two shares using (2,2)-VCS scheme discussed in the previous section. The shares are shown in Fig. 6. The original data can be obtained by stacking the shares using "and"/"or" operations. The results of both the operations are shown in Fig. 7 and 8 respectively. The shares are concatenated as shown in Fig. 9.

In the second phase, the cover image is decomposed into 4 sub-bands and the share images are embedded into the HH band. Then, the inverse IWT is computed to generate watermarked image. The result of inverse IWT is shown in Fig. 10.

Similar process is used to extract the original data from the watermarked image. The extracted shares are shown in Fig. 11. Fig. 12. shows the required result.

Fig. 4 Secret Image

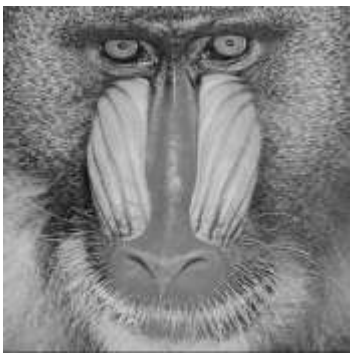
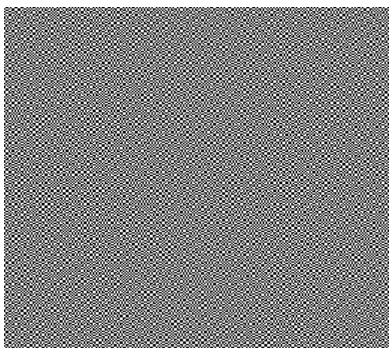
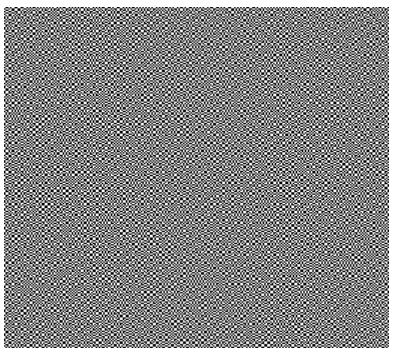


Fig. 5 Cover Image



Share 1



Share 2

Fig. 6 Shares

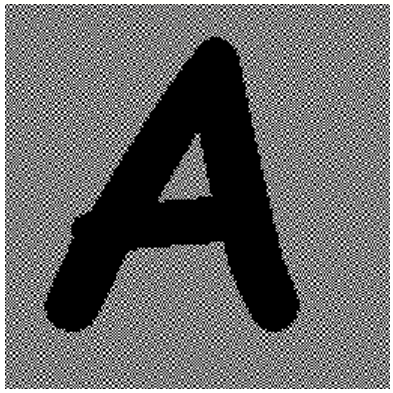


Fig. 7 Stacking using AND operation **Fig. 8 Stacking using OR operation**

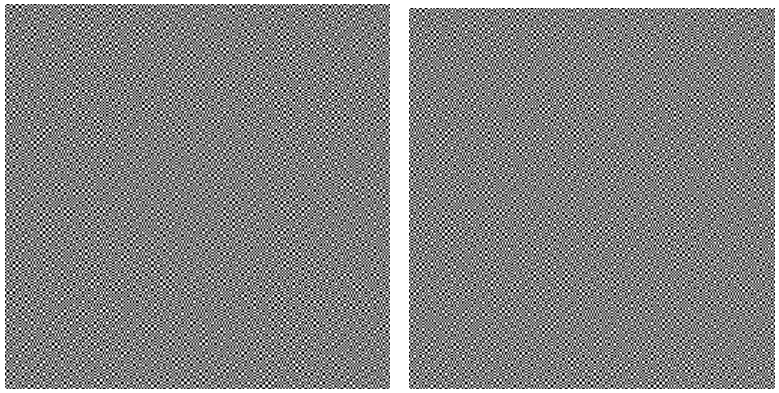


Fig. 9 Combined Share Images

The performance parameters used are peak signal to noise ratio (PSNR), mean square error (MSE) and cross-correlation coefficient (R_{xy}). The computed parameters for the image are outlined in Table II.

TABLE II
RESULTS

Parameter	Image	
	Secret Image	Watermarked Image
PSNR	Inf	49.7777
MSE	0.0000	0.6844
R_{xy}	1.0000	0.9997

V. CONCLUSIONS

In this paper, a new technique for securing digital images is presented. In the proposed algorithm, a random-grid-based (2,2) Visual Cryptography scheme is used to split an image into two meaningless shares. Then, the int-to-int DWT is used to decompose a cover image and the shares are embedded into HH band of the decomposition to give watermarked image. The analysis of proposed technique has been presented using Mean

Square Error (MSE), PSNR and Cross-correlation Coefficient. From the Fig. 12 and 15 and Table II, it can be concluded that the proposed technique performs better in all respects. While the technique provides excellent results, still there is scope for improvement.

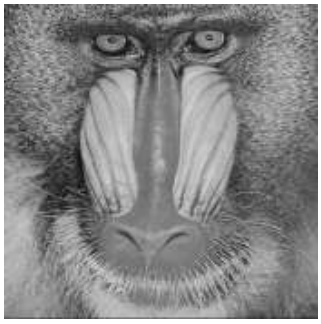
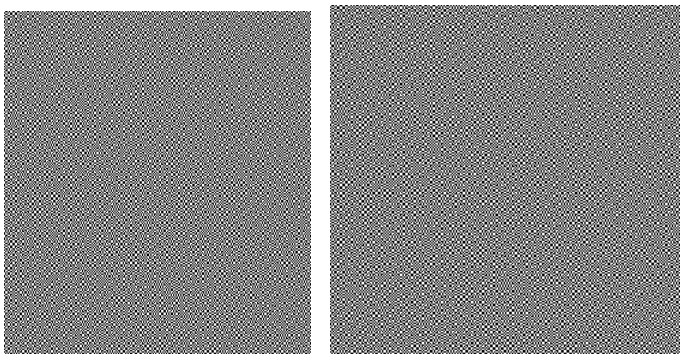


Fig. 10 Watermarked Image



Share 1 Share 2

Fig. 11 Extracted shares

Fig. 12 Extracted result

In this work, random-grid-based (2,2) Visual Cryptography scheme is used to split an image into two meaningless shares. Recent developments in the field of Visual Cryptography has enabled the splitting of an image into multiple shares. Along with it, various authors have proposed schemes with meaningful shares. Such techniques may be used for improving the security of the secret image. Along with this, much research is being

done in the field of watermarking schemes. This work proposes int-to-int DWT for invisible watermarking of the shares. Impact of different wavelets and decomposition level can be studied for comparison proposes. Along with it, various other watermarking algorithms are available apart from wavelet domain which can be used in this work which may provide better results.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, pp. 1-12, 1995.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A, no. 10, pp. 2172-2177, 1999.

[3] T. L. Lin, S. J. Horng, K. H. Lee, P. L. Chiu, T. W. Kao, Y. H. Chen, R. S. Run, J. L. Lai, and R. J. Chen, "A novel visual secret sharing scheme for multiple secrets without pixel expansion," Expert Systems with Applications, vol. 37, no. 12, pp. 7858-7869, 2010.

[4] S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," Imaging Science Journal, vol. 55, no. 2, pp. 90–101, 2007.

[5] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, vol. 25, no. 4, pp. 481-494, 2004.

[6] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, vol. 12, no. 6, pp. 377-379, June 1987.

[7] S. J. Shyu, "Image encryption by random grids," Pattern Recognition, vol. 40, no. 3, pp. 1014-1031, 2007.

[8] S. J. Shyu, "Image encryption by multiple random grids," Pattern Recognition, vol. 42, no. 7, pp. 1582–1596, 2009.

[9] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," Pattern Recognition, vol. 42, no. 9, pp. 2203-2217, 2009.

[10] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 11, pp. 1693-1703, 2011.

[11] D. C. Lou, H. H. Chen, H. C. Wu, and C. S. Tsai, "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares," Displays, vol. 32, no. 3, pp. 118-134, 2011.

[12] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1 part 2, pp. 219-229, 2012.

[13] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," Theoretical Computer Science, vol. 250, pp. 143-161, 2001.

[14] Y. C. Hou and J. H. Wu, "An extended visual cryptography scheme for concealing color images," in Proceeding of The 5th Conference on Information Management and Police Administrative Practice, Taoyuan, Taiwan, pp. 62-69, (in Chinese) 2001.

[15] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2453, 2006.

[16] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 383–396, 2009.

[17] C. C. Chang, W. L. Tai, and C. C. Lin, "Hiding a secret color image in two color images," Imaging Science Journal, vol. 53, no. 4, pp. 229–240, 2005.

[18] M. Nakajima and Y. Yamaguchi, "Enhancing registration tolerance of extended visual cryptography for natural images," Journal of Electronic Imaging, vol. 13, no. 3, pp. 654–662, 2004.

[19] W. P. Fang, "Friendly progressive visual secret sharing," Pattern Recognition, vol. 41, pp. 1410-1414, 2008.

[20] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 12, pp. 1161–1169, 2003.

[21] Peyman Rahmati, and Andy Adler, and Thomas Tran. ―Watermarking in E-commerc, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013

[22] Swathi.K, Ramudu.K, Robust Invisible QR Code Image Watermarking Algorithm in SWT Domai, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2

[23] M. A. Suhail and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model," in IEEE Transactions on Instrumentation and Measurement, vol. 52, no. 5, pp. 1640-1647, Oct. 2003.

[24] Gu Tianming and Wang Yanjie, "DWT-based digital image watermarking algorithm," Electronic Measurement & Instruments (ICEMI), 2011 10th International Conference on, Chengdu, 2011, pp. 163-166.

[25] C. Y. Yang, W. Y. Hwang and Y. F. Cheng, "IWT-Based Watermarking By Adaptive Bit-Labeling Scheme," Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, Harbin, 2008, pp. 1165-1168.