© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Image Encryption using Visual Cryptography and Watermarking Techniques

Sarita*, Sudesh Nandal, Sandeep Dahiya

Department of Electronics and Communication Engineering, B.P.S.M.V, Khanpur Kalan, Sonipat, Haryana, India

ABSTRACT

The present study discusses a novel two layer technique for securing digital images. The two techniques used are visual cryptography (VC) scheme and int-to-int wavelet transforms (IWT). (2, 2) –VC scheme is used to split the secret image into two shares. 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. Invisibly embedding image shares generated by the visual cryptography in the host image to provide authentication to the shares. The proposed scheme is compared with the traditional discrete cosine transform (DCT) for watermarking. The performance is measured by computing peak signal to noise ratio, mean square error and cross-correlation coefficient.

Keywords: Image Encryption, Decryption, Visual Cryptography, Watermarking, DCT, DWT

I. INTRODUCTION

Due to the technology advancement in modern scenario, all works are digitized and the information is transferred through the internet from one end to another to reduce time consumption. With the progress of technology, no doubt time reduces but at the same junction security issue arises. Image data is commonly used all over the world. Image may enclose top secret message which can be misused by the hackers and unauthorized people.

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 technique is compared with DCT based watermarking technique. Moni Naor and Shamir extended (n,n) VCS for (k,n) in 1995 [1]. In 1996 Naor and Shamir proposed an idea to improve contrast [2]. Ateniese et al. presented (2,n) visual cryptography scheme in which 2 shares were needed for decryption [3]. Blundo et al. give (3,n) VC scheme, number of shares needed for decryption are 3 [4]. Hou presented an idea to share color images using digital halftoning [5]. Andrew Tirkel et al. utilized digital watermarking in 1992 [6] . Radhika V. Totla et al. presented algorithm based DWT and DCT for digital image watermark [7]. Bhupendra Ram proposed the addition of watermark into select coefficient with significant energy of the image in the transform domain that ensures the non erasability of the watermark [8]. The details of visual cryptography and watermarking using IWT are discussed in the Section II. Section III discusses methodology. Section IV outlines the results and performance measures. Section V concludes this paper.

II. METHODS AND MATERIAL

1. Existing Techniques

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

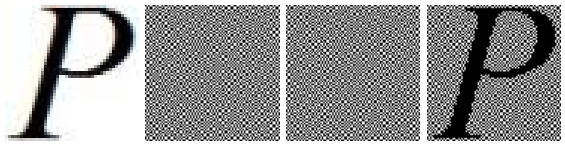
A. (2,2) Visual Cryptography Scheme

It was introduced by the Moni Naor and Shamir in 1994 [1]. Visual cryptography (VC) is a technique in

which encryption is performed by breaking the secret image into the parts and printed on to transparent sheet and the decryption is performed by human visual system by stacking the sufficient number of parts.

In VC original image pixels are divided into sub pixels and the numbers of sub pixels are decided by the visual encryption technique [9]. The secret/recovered image which generates by the visual encryption is not more than the collection of black and white pixels.

In (2, 2) VC Scheme, the original image, which is to be protect is divided into two shares such that every pixel in the original image is replaced by a non-overlapping block of two or four sub-pixels as shown in Fig.1. It is pertinent that without sharing the information, secret codes cannot be identified. To recover the image, each of these shares is XORed onto a transparency [10]. Stacking both these transparencies will allow decryption of the secret as shown in Fig. 1.



Secret Image Share 1 Share 2 Stacked Result

Figure 1: Working of visual cryptography scheme

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

B. Digital Watermarking based on DCT

It is a mathematical function that translates spatial domain digital image data to the frequency domain [11]. In DCT, after converting the image in frequency domain, the data is embed in the LSB of the medium frequency components and is particular for lossy compression [12]. JPEG compression is performing by DCT coefficients. It divides the image into parts of separate significance. It change a signal or image from the spatial to the frequency domain. It divides the image into different frequency component [13]. In low frequency sub-band, a large amount of the signal energy is in low frequencies which have most significant visual parts of the image. Through compression and noise attacks high frequency sub-band, high frequency components of the image are usually removed. So the secret message is embedded by amend the coefficients of the sub-band of middle frequency, so that the visibility of the image will remain unaffected. The expression for 2D DCT is given below where symbols have their usual meaning [14].

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j) \quad (1)$$

The DCT of the cover image is computed block by block where each block is of 8x8 pixels. The shares are embedded into the DCT transformed image at specific positions.

C. Digital Watermarking using IWT

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

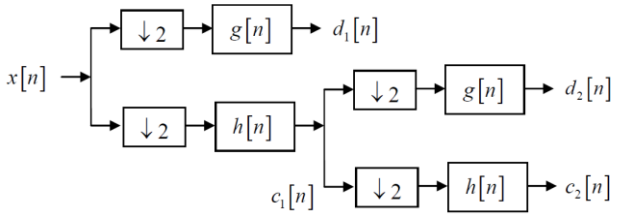


Figure 2: DWT Forward Transform Filter Bank

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. To find high frequency values basic polynomial interpolation is used. Scaling functions also constructed by this method, in order to find out low frequency values [15]. Lifting scheme for Integer Wavelet Transform consist of three steps as shown in Fig. 3.

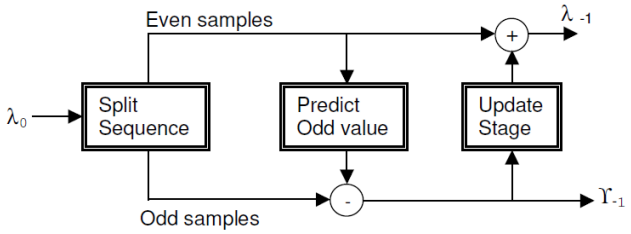


Figure 3: IWT Forward Transform

- Split (Lazy wavelet transform)
- Predict (Dual lifting)
- Update (Primal lifting)

To attain an efficient performance of the discrete wavelet transform, it is of enormous realistic

importance that the wavelet transform is characterized by a set of integers. Because wavelet coefficients as a floating point values requires 32 bits per coefficients to store. For efficient encoding and storage wavelet coefficients are rounded to convert it into integer number. Due to rounding process, the original signal cannot be recreated from its altered without an error [16]. In lifting scheme of wavelet transform, inverse transform will cancel the rounding error. Hence, it is likely to achieve perfect reconstruction [17].

2. METHODOLOGY

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

D. *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

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

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.

E. 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.

III. RESULTS AND DISCUSSION

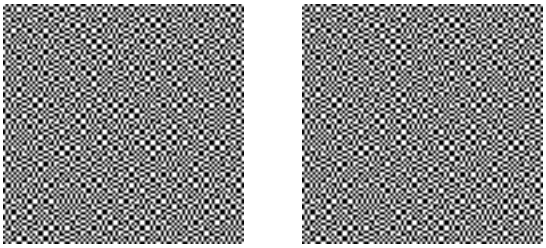
The visual cryptography and digital watermarking of the images are simulated in MATLAB. The secret image which is used for simulation is shown in Fig 4.

Figure 4: Secret Image

The cover image which is used in the cryptography phase shown in Fig 5.

Figure 5: Cover Image

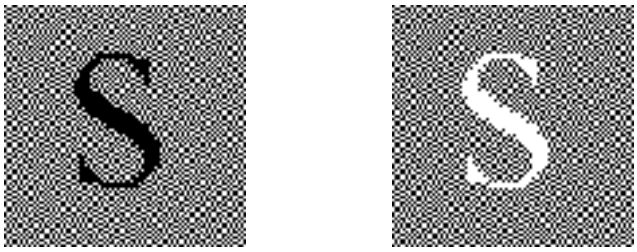
The image shown in Fig. 4 is split into two shares using (2,2)-VCS scheme discussed in the previous section. The shares are shown in Fig. 6.



Share 1 Share 2

Figure 6: Shares

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.



(a) (b)

Figure 7: Stacking using (a) AND operation (b) OR operation

The shares are concatenated as shown in Fig. 9.

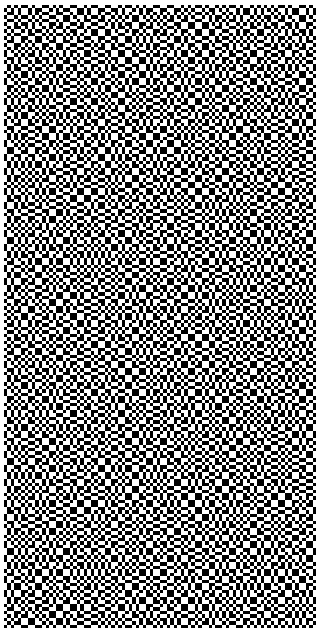
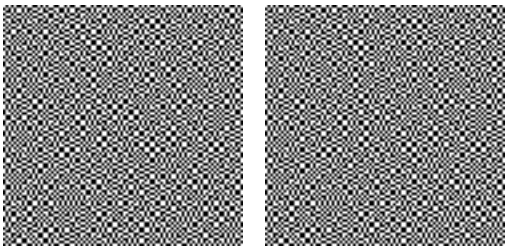


Figure 8: Combined Share Images

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 is shown in Fig. 10.

Figure 9: Watermarked Image (IWT)

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.



Share 1 Share 2

Figure 10: Shares extracted using IWT

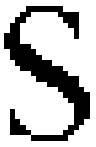
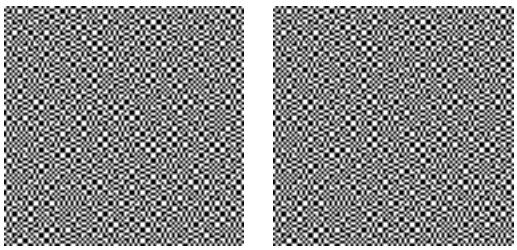


Figure 11: Extracted result using proposed algorithm

The results obtained using the DCT algorithm is shown in Fig. 13, 14 and 15.

Figure 12: Watermarked image (DCT)



Share 1 Share 2

Figure 13: Shares extracted using DCT

The performance parameters used are Peak Signal to Noise Ratio (PSNR), Cross-Correlation Coefficient (R_{xy}), Mean Square Error (MSE) and. A comparison of the both the algorithms for the image is outlined in Table II. **A1** refers to the algorithm which uses DCT and **A2** refers to the proposed algorithm.

Figure 14: Extracted result using DCT

TABLE I
COMPARISON RESULTS

Parameter	Image			
	Secret Image		Watermarked Image	
	A1	A2	A1	A2
PSNR	63.5608	Inf	0.2172	0.0279
MSE	0.0286	0.0000	54.7622	63.6824
$\mathbf{R_{xy}}$	0.8197	1.0000	0.9999	1.0000

IV. CONCLUSION

This work presented two step techniques for securing digital images. First, random-grid-based (2, 2) Visual Cryptography scheme has been used to split an image into two meaningless shares. Then, the int-to-int DWT has used to decompose a cover image and the shares have embedded into Diagonal Detail component to the decomposition to give watermarked image. The technique has been compared with DCT based watermarking technique. The analysis of the differences between the int-to-int DWT or IWT and infinite precision DCT has reported using Mean Square Error (MSE), Cross-correlation Coefficient and PSNR to provide excellent results.

In this work, random-grid-based (2, 2) visual cryptography scheme has been used to split an image into two meaningless shares. Recent developments in the field of Visual cryptography have enabled the splitting of an image into multiple shares. Various other watermarking algorithms are available apart from wavelet domain which can be used in this work which may provide better results.

V. REFERENCES

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

[2] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary version appears in "Security Protocols", M. Lomas ed. Vol. 1189 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp.197-202, 1997.

[3] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, , pp. 416–428, 1996.

[4] C. Blundo, P. D'Arco, A. D. Snatis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM Journal vol. 16, no. 2, pp. 224– 261, April 1998.

[5] Y. C. Hou, C. Y. Chang, and S. F. Tu, "Visual cryptography for color images based on halftone technology," in International Conference on Information Systems, Analysis and Synthesis. World Multiconference on Systemics, Cybernetics and Informatics. Image, Acoustic, Speech And Signal Processing: Part II, 2001.

[6] R.G. Schyndel, A. Tirkel, and C.F Osborne, "A Digital Watermark" , Proceedings of IEEE International conference on Image Processing, pp. 86-90, 1994

[7] Radhika V. Totla, K.S. Bapat."Comparitive Analaysis Of Watermarking In Digital Image Using DCT And DWT", International Journal Of Scientific And Research Publication, Vol. 3, Issue 2, Feb 2013

[8] Bhupendra Ram, "Digital Image Watermarking Techniques Using Discrete Wavelet And

Discrete Cosine Transform", International Journal Of Advancements In Research And Technology, Vol.2, Issue 4, April 2013

[9] 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.

[10] Jagdeep Verma, Vineeta Khemchandani "A Visual Cryptographic Technique To Secure Image Shares," International Journal Of Engineering Research And Applications (IJERA), Vol. 2, No. 1, , pp.1121-1125, Jan-Feb 2012.

[11] Preeti Parashar and Rajeev Kumar Singh "A Survey: Digital Image Watermarking Techniques," International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 7, No. 6 , pp. 111-124, 2014.

[12] 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.

[13] Bhupendra Ram, "Digital Image Watermarking Techniques Using Discrete Wavelet and Discrete Cosine Transform," International Journal of Advancements in Research and technology, Vol.2, No. 4, April 2013.

[14] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum," International Journal of Electrical, Electronics and Data Communication, Vol. 1, No. 2, pp 111-124, 2013.

[15] Ankita A. Hooda, N. J. Janve,"A Hybrid and Robust Wavelet Based Video Watermarking Scheme for Copyright Protection Using Principle Component Analysis," International Journal of Computer Trends and Technology, Vol. 4, No. 6, pp. 1727-1732, 2013.

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

[17] 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,pp. 1165-1168, , 2008.