iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** X **Month of publication:** October 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Secret Image Sharing Using Discrete Wavelet Transform Watermarking Technique

Miss. Shabana M. Y.Sheikh[1], Dr. Varsha Namdeo[2]
[1]*M.Tech (CSE), Final Year, Department of CSE, RKDF IST*
[2]*Associate Professor, Department of CSE, RKDF IST*

Abstract- Patent safety and verification have become increasingly more important in regular life. The digital watermark is one of the method invented to handle this problem. In this paper, a digitally invisible watermark is inserted in a quick response code image by means of wavelet transform. In the embedding process, a binary image, logo, is converted into a corresponding watermark and then inserted into a selected sub band. The experimental results explained that, for all the cases considered in this paper is more strong to attacks and as such it can serve as a viable patent safety and verification tool.
Keywords- QR Code, Watermark, Video, Wavelet Transform

I. INTRODUCTION

Digital watermark is a motif of bits included into a digital image, audio or video that identifies the patent and verification information. The aim of watermark method is to inserting the secret information seamlessly hidden within into original message, which is healthy against attacks. In recent years, some developers have proposed the adoption of watermark method. The watermark can also be inserted in the primary spatial domain of the image.In the main drawback of spatial domain was that it easy to be hacked and assault.

In the proposed method inserted the patent image into the primary image using (N,N) secret sharing scheme. This technic could resist impurities such as JPEG compression, resize and noise addition. There are many method to insert the watermark into frequency domain of the primary image. The techniques operating on a frequency domain use transformations such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). In, a watermark technique of multispectral image is performed in the wavelet transform. In the proposed a scheme for color images using wavelet transform based on texture characteristic and secret sharing.

In this paper, we will propose the blind watermarking algorithm by means of two-level discrete wavelet transform (DWT) embedded in a QR code image. This paper is arranged as follows. A barcode is an optically machine-readable label that is attached to an item and that records relevant knowledge. The knowledge encoded by a QR code may be done up of four standardized types ("modes") of data (numeric, alphanumeric, byte / binary, Kanji) or, through supported extensions, virtually any type of knowledge. The QR Code system has become common outside the automotive industry due to its fast readability and larger storage capacity compared to common UPC barcodes. Applications contain product tracking, item identification, time tracking, document management, general marketing, and much more.

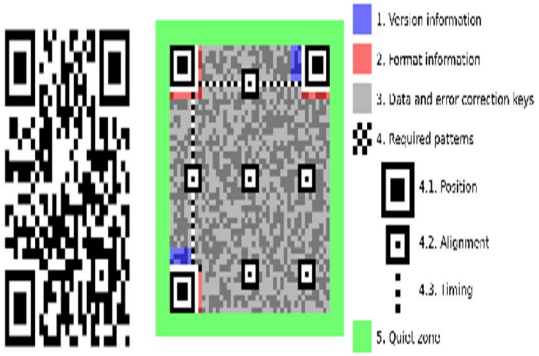


Fig. 1. (a) QR code (b) QR code Structure

A quick response code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging apparatus, such as a camera or mobile, and 13th International Symposium on Communications and Information Technologies (ISCIT) 791 processed using Reed-Solomon error correction up to that the image can be appropriately changed. knowledge is then extracted from the motif present in both horizontal and vertical components of the image. Fig. 1(a) shown the example of QR code and the structure of QR code shown in Fig. 1(b)

II. PROPOSED METHOD

A. *Process of Watermarking*

A binary image of Burapha University logo, is a selected as the watermark. The process of inserting this watermark was performed on a QR code image on its frequency domain. The QR code image was first decomposed by a two-level two-dimensional wavelet transform as shown inFig.2. The following watermark extraction, are bided in a sense that it did not want the primary QR code image in order to get the embedding watermark. There were two steps in our algorithm: watermark embedding and watermark extraction.

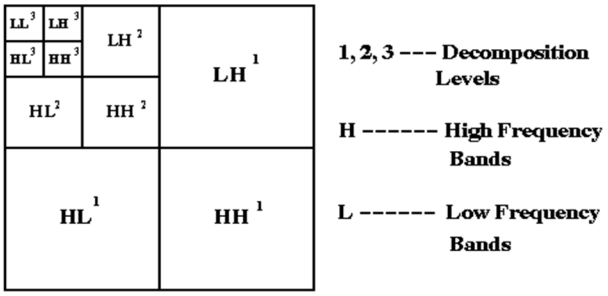


Fig.2. 2-Level 2-Dimensional Wavelet Transform

The step of embedding process are outlined as follows Step of watermark image with secret key I The watermark image was produced as a bit sequence of watermark S. The information and background contains were set to 1 and –1, respectively.

S={si,1<=i<=N}.si ε{-1,1} (1)

where *N* is the total number of pictures-cells in the watermark image The pseudo-random sequence **(P)** whose each digit can take a value either 1 or –1 was randomly generated with a secret key for embedding and extracting of the watermark.

P={pi,1<=i<=M},pi ε {-1,1} (2)

Step of QR code image

I. The two-level DWT of *M* x *M* image ( ) *ti* was computed for quick response code image.
II. A watermark was then embedded in sub band LH2 orHL2 or HH2. According to the rule

ti = ti + α.pi.si,I = 1,2,3……..N

Where t_i is input image. $'t_i$ is output image with watermark. α is a magnitude factor which is a unchanged determining the watermark power.

III. After that, the inverse DWT (IDWT) was then applied to obtain the watermarked image.

IV. Compute PSNR

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

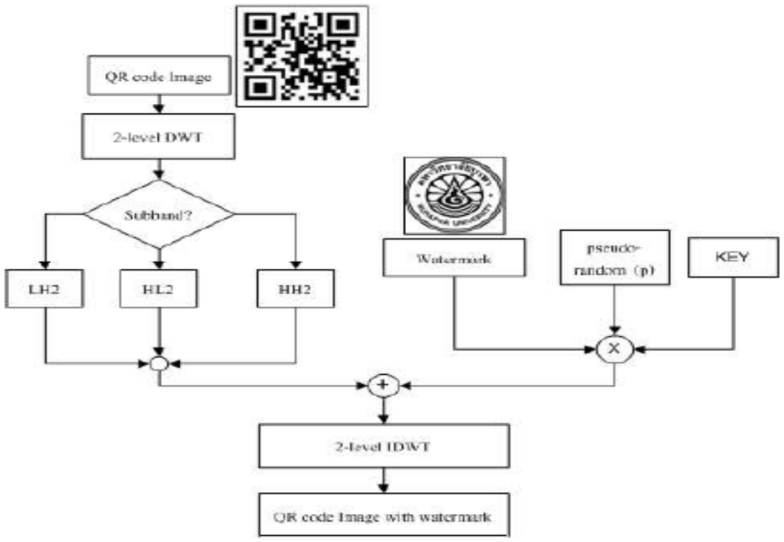


Fig.3. Watermark embedding process

The watermark extraction algorithm didn't used the primary QR code image. A assumption of the original value of the picture-cell is however required. Thus, a assumption of the primary value of the pixels was performed using noise reduction technique. In this paper, we use an averaging3×3mask whose elements were fixed to 1/9. The extraction process are outlined as follows (Fig.4).The predicted image t_i could be gained by smoothing the input image t_i^* with a spatial convolution mask. The prediction of the primary value can be defined as:

where *c* is the size of the convolution cover. The watermarked image and the predicted image were DWT converted independently.

II. The estimate of the Sî is indicated by the difference between t* and ˜ti

$\delta = t^*i - t\hat{i} = \alpha.pi.si$ *(5)*

III. The sign of the difference between the assumption and the actual value is the value of the embedded bit:

$Sgn(\delta_i) = pi.si$ *(6)*

IV. Compute NC

The watermark was then appraise by multiplying pseudo- random number to the embedded bit. If wrong pseudo random series was to be used, the scheme should not work.

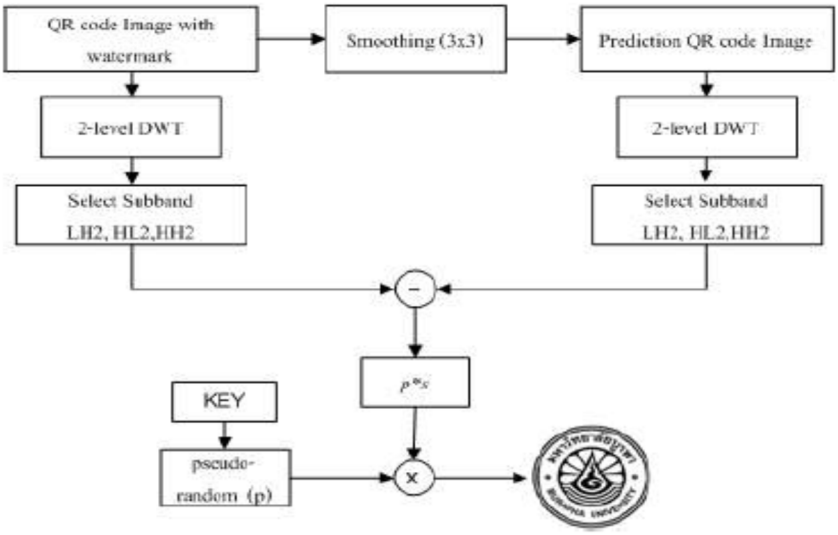


Fig.4. Watermark Extraction Process

III. PREVIOUS WORK

A. Digital Watermarking Techniques

The most important characteristic of any digital watermarking method are strength, sefety, imperceptibility, complexity, and conformation. Robustness is defined as if the watermark can be discover after media (normal) procedure such as filtering, lossy compression, color correction, or geometric modifications. Security means the embedded watermark cannot be avoid beyond reliable detection by set attacks. Imperceptibility means the watermark is not seen by the human visual system.

Intricacy is explained as the effort and time required for watermark embedding and obtained.finally, conformation is a operation whereby there is private key or public method (Dittmann, Mukherjee & Steinebach, 2000).Each of these properties must be taken into consideration when inserting a certain digital watermarking method. The following part describe a few of the most appearing digital watermarking methods.

B. Spatial and Frequency Domain

Spatial and frequency domain watermarking are refer to graphic images and character. Spatial domain watermarking little change the pixels of one or two randomly refer subsets of an image. Changes might include flipping the low-order bit of each pixel. However, this methods is not good when set to normal media procedure such as filtering or lossy compression (Berghel,1998). Some of its main algorithms are given below:

1) *Additive watermarking:* The most simple method for embedding the watermark in spatial domain is to insert pseudo random noise motif to the intensity of image pixels. The noise signal is popularly integers like (-1,0,1) or sometimes floating point numbers.
2) *Least Significant Bit Modification:* A digital image version of this analogue image contains sampled values of the method at discrete place or pixels. These values are said to be the presentation of the image in the spatial domain or often refer to as the pixel domain. Spatial embedding include message into image pixels.
3) *Texture mapping coding Technique:* This method is refer only in those images which have some structure part in it. This process hides the watermark in the structure part of the image. This algorithm is only suitable for those areas with large number of arbitrary structure images and cannot be done automatically. This method hides data within the stay random structure patterns of a picture. carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened.
4) *Patchwork Algorithm:* Patchwork is a data hiding method developed by Bender et al and published on IBM Systems Journal, 1996[6]. It is depend on a pseudorandom, statistical model. Patchwork imperceptibly include a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is the more usefull characteristic of any digital watermarking methods are strength, security, imperceptibility, complexity, and conformation.strongness is defined as if the watermark can be discover after media (normal) procedure such as filtering, lossy compression, color correction, or geometric modifications. Sefety means the inserted watermark cannot be avoid beyond reliable detection by is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened.
5) *Correlation-Based Method:* In this methods, a pseudorandom noise (PN) motif says W(x, y) is added to cover image I(x, y) Iw(x, y) = I(x, y) + k*W(x, y) where K present the gain factor, Iw present watermarked image ant location x, y and I represent cover image. Here, if we enhanced the gain factor then although it enhanced the strength of watermark but the quality of the watermarked image will reduced. Frequency domain watermarking method is also called transform domain. Values of certain frequencies are altered from their original. Typically, these frequency alterations are done in the lower frequency levels, since alterations at the higher frequencies are lost during compression. The watermark is applied to the complete image so as not to be reduced during a cropping process. However, there is a trade-off with the frequency domain method. Conformation can be hard since this watermark is refered indiscriminately across the complete image (Berghel,1998). Some of its important algorithms are given below:

a) *Discrete Fourier Transform:* Fourier Transform (FT) is an process that convert a continuous function into its frequency components. The equivalent convert for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the even methods that are un-periodic can be presented as the integral of sine and/or cosine multiplied by a weighing methods. This weighing function made up the coefficients of the Fourier Transform of the signal. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and translate these coefficients.
b) *Discrete Cosine Transform:* Discrete Cosine Transform is related to DFT in a term that it convert a time domain signal into its

frequency components. The DCT however only refer the real parts of the DFT coefficients. In terms of characteristic, the DCT has a healthy energy compaction characteristic and most of the signal data tends to be concentrated in a little low-frequency components of the DCT. The JPEG compression method utilizes this characteristic to separate and reduce insignificant high frequency components in images

c) *Discrete Wavelet Transform* Wavelet Transform is a modern method frequently used in digital image processing, compression, watermarking etc. The transforms are depend on little waves, called wavelet, of varying frequency and limited time. A wavelet series is a representation of a square-integral function by a certain ortho-normal series produced by a wavelet. The properties of wavelet should break primary signal into wavelet transform coefficients which consist the position data. The primary signal can be completely reconstructed by performing Inverse Wavelet Translation on these coefficients. Watermarking in the wavelet transform domain is generally a difficulty of embedding watermark in the sub bands of the cover image.

IV. CONCLUSION AND FUTURE SCOPE

In the proposed Digital watermarking method, a binary image is watermarked into a quick response Code image. The inserting process is in LH, HL and HH sub bands based on wavelet transform. The algorithm explain that the watermark with an acceptable visual quality can be get easily. In future we try to find more efficient ways for more series attacks such as stronger noise, high compression and geometric distortion etc.

In future work we focus on enhanced the proposed method for more inserting capacity and also for embedding secret data in audio or video file. In future there is a scope to build a better method for QR Code image depending on the above theoretical knowledge and the current method available and also reduce the degradation of image quality.

REFERENCES

[1] R. Z. Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, “Incrementing visual cryptography using random grids,” Opt. Commun., vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[2] P. L. Chiu and K. H. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[3] I. Kang, G. R. Arce, and H. K. Lee, “Color extended visual cryptography using error diffusion,” IEEE Trans. Image Process., vol. 20, no. 1, 132–145, Jan. 2011.

[4] M. Kim, D. Li, and S. Hong, A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents :Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I WCECS 2013, 23-25 October, 2013, San Francisco, USA.

[5] C. Guo, C. C. Chang, and C. Qin, “A multi-threshold secret image sharing scheme based on MSP,” Pattern Recognit. Lett., vol. 33, no. 12, pp. 1594–1600, Sep. 2012

[6] K. H. Lee and P. L. Chiu, “An extended visual cryptography algorithm for general access structures,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[7] Frank Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA, 2008

[8] Jun-Chou Chuang, Yu-Chen Hu & Hsien-Ju Ko. A Novel Secret Sharing Technique using QR Code, International Journal of Image Processing (IJIP), Volume : Issue (5),pp. 468-475, 2010.

[9] J. Fridrich, M. Goljan, and D. Soukal, “Perturbed quantization steganog-raphy with wet paper codes,” in Proc. Workshop Multimedia Sec., Magdeburg, Germany, Sep. 2004, pp. 4–15.

[10] Sushma Yalamanchili, M. Kameswara Rao, “Copyright Protection of Gray Scale Images by Watermarking Technique using (N,N) Secret Sharing Scheme,” Journal of Emerging Technologies in Web Intelligence, Vol 2, No 2, pp.101-105, May 2010.

[11] Y. Rangsanseri, J. Panyaveraporn and P. Thitimajshima, “PCA/Wavelet Based Watermarking of Multispectral Images,” 2005 International Symposium on Remote Sensing (ISRS2005), Korea, 12-14 Oct. 2005.

[12] Nagaraj V. Dharwadkar and B.B.Amberker, “Watermarking Scheme for Color Images using Wavelet Transform based Texture Properties and Secret Sharing,” International Journal of Information and Communication Engineering,Vol 6, No 2,pp 94-101, 2010.

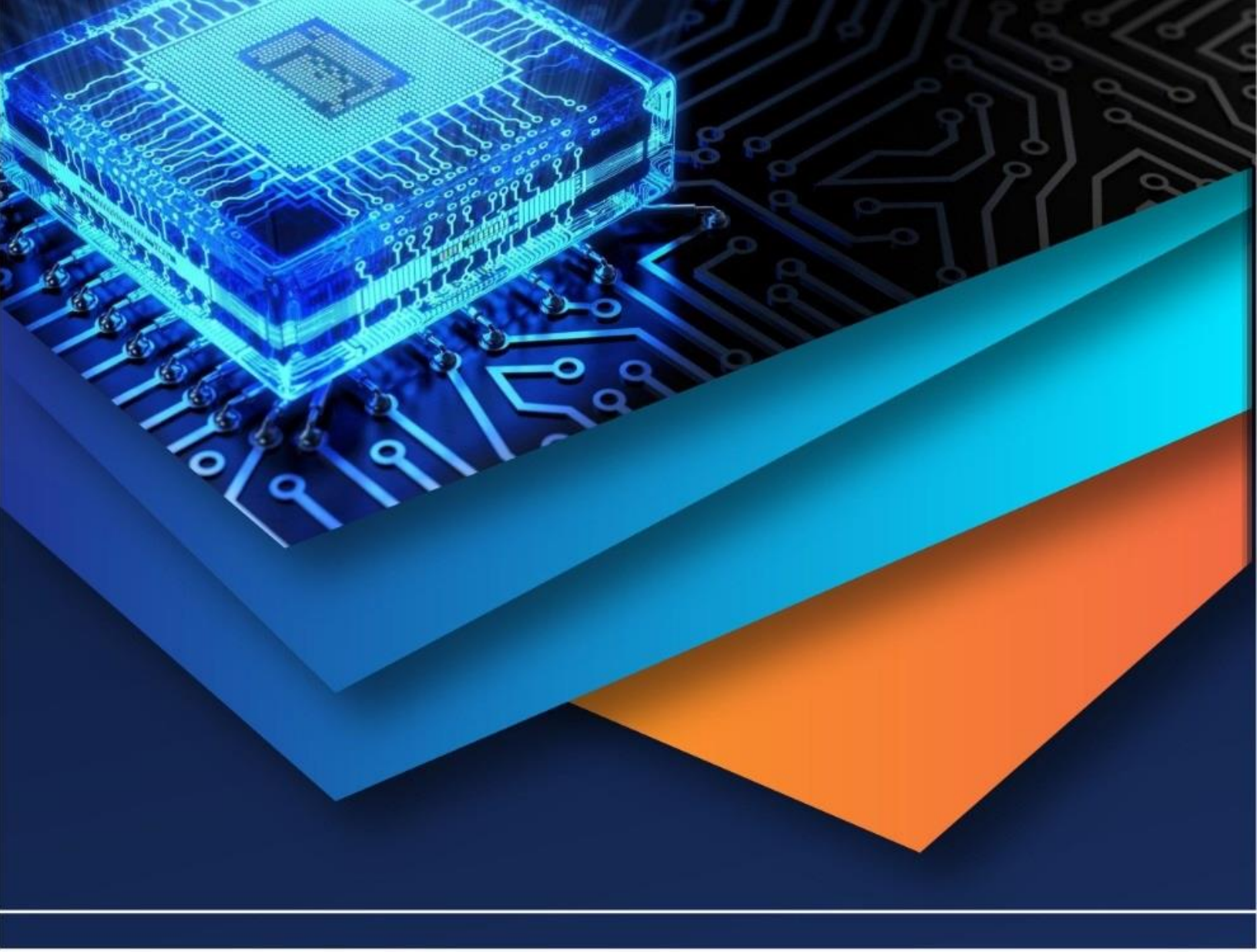
[13] R.Z.Wang,Y.C.Lan,Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, “Incrementing visual cryptography using random grids,” Opt. Commun., vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[14] P. L. Chiu and K. H. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[15] Y. Rangsanseri, J. Panyaveraporn and P. Thitimajshima, “PCA/Wavelet Based Watermarking of Multispectral Images,” 2005 International Symposium on Remote Sensing (ISRS2005), Korea, 12-14 Oct. 2005.

[16] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[17] F. Hartung, J.K. Su, and B. Girod, Spread Spectrum Watermarking: Malicious Attacks and Counter-Attacks, Proc. of SPIE Vol. 3657: Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 1999.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY