ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Steganographic Technique in Z-Domain for Image Authentication (STZ-DIA)

Nabin Ghoshal
Department of Engineering and Technological Studies
University of Kalyani Kalyani, Nadia,
Pin. 741235, West Bengal, India
nabin_ghoshal@yahoo.co.in

*Abstract***:** This paper deals with a novel technique for image authentication in Z-domain based on the Discrete two dimensional Z-Transform. The Z-Transform is exploits on sub-image block called mask of size 2 x 2 for frequency components of the corresponding spatial component in row major order. Multimedia Image authentication is done by hiding secret message/image into the real part of the component obtained by discrete two dimensional Z-Transform of the carrier image. A single bit from the authenticating image/message is embedded in middle and low quantum value of carrier image mask. Robustness is achieved through embedding bits in variable positions of carrier image determined by the decimal value of sum of higher three bits of frequency values (i.e. b_7+b_6+b_5). After embedding, a delicate re-adjust phase is incorporated in all frequency components of each mask, to keep the pixel values positive and non-fractional in the spatial domain. The invisibility is conformed by using delicate re-adjust phase. This technique is also applicable for secrete data transmission through carrier color image by hiding secrete data. Experimental results show the robustness and performance of the proposed watermarking technique.

Keywords: Z-Transform, Inverse Z-Transform, DFT, QFT, DCT

I. INTRODAUCTION

The driving forces behind the increased use of copyright [1, 2, 3] marking is the growth of the Internet which has allowed images, audio, video, etc to become available in digital form. Copyright abuse is the motivating factor in developing new encryption technologies. Steganography is the art of hiding information into picture or other media in such a way that no one apart from the sender and intended recipient even realizes that there is hidden information. Image transmission via the internet has some problem such as information security, copyright protection, Originality etc. Secured communication is possible with the help of encryption technique which is a disordered and confusing message that makes suspicious enough to attack eavesdroppers. Without creating any special attention of attackers steganographic methods overcome the problem by hiding the secrete information behind the source image. Image trafficking across the network is increasing day by day duo to the proliferation of internetworking. Image authentication is needed to prevent unauthorized access in various e-commerce application areas. This security can be achieved by hiding data within the image. Data hiding [4, 5, 6, 7, 10] in the image has become an important technique for image authentication and identification. Therefore, military, medical and quality control images must be protected against attempts to manipulations. Generally digital image authentication schemes mainly falls into two categories-spatial-domain and frequency-domain techniques. So, digital image authentication [12, 13] technique has become a challenging research area focused on battling to prevent the unauthorized or illegal access and sharing.

So many works has been done in spatial-domain for digital image authentication. Among these the most common methods Chandramouli et al. [8] developed a useful method by masking, filtering and transformations of the least significant bit (LSB) on the source image. Dumitrescu et al. [9] construct an algorithm for detecting LSB steganography. Pavan et al. [11] and N. N. EL-Emam [5] used entropy based technique for detecting the suitable areas in the image where data can be embedded with minimum distortion. Ker [14] and C. Yang [15] presented general structural steganalysis framework for embedding in two LSBs and Multiple LSBs. H.C. Wu [16] and C-H Yang [17] constructed LSB replacement method into the edge areas using pixel value differencing (PVD).

Several works has been done in frequency domain for digital image authentication. In this area most common transformations are the discrete cosine transformation (DCT), quaternion Fourier transformation (QFT), discrete Fourier transformation (DFT), discrete wavelet transformation (DWT), and the discrete Hadamard transformation (DHT). Frequency-domain methods are widely applied than the spatial-domain methods. Here embedding is done in the frequency component of the image pixel in frequency-domain the human visual system is more sensitive to low frequency components than the high frequency component. To avoid severe distortion of the original image the midrange frequencies are best suitable for embedding to obtain a balance between imperceptibility and robustness. I. J. Cox et al. [18] developed an algorithm to inserts watermarks into the frequency components and spread over all the pixels. DCT-based image authentication is developed by N. Ahmidi et al. [19] using just noticeable difference profile [20] to determine maximum amount of watermark signal that can be tolerated at each region in the image without degrading visual quality. P. Bas et al. [21] proposed a color image watermarking scheme using the hypercomplex numbers representation and the quaternion Fourier transformation. Vector watermarking schemes is developed by T. K. Tsui [22] using complex and quaternion Fourier transformation.

This paper proposed a watermarking technique with the help of Z-Transform using the decimal value of sum of higher order three bits of each byte which satisfies all the necessary criteria like imperceptibility [16, 17], robustness [20, 21] and security [18, 19] that watermarking should satisfy and also provides a good security from all possible attacks. The embedded images are provides less noise insertion and more robust. In this paper two-Dimensional Discrete Z-Transform has been presented with expression evaluated and simplified. The insertion and extraction technique in the carrier image has also been introduced with suitable algorithm and example. The results of the proposed STZ-DIA have compared with the existing DCT-based, QFT-based and Spatio Chromatic DFT-based watermarking method in terms of visual interpretation, MSE, PSNR in dB and Image Fidelity (IF) [23]. Figure 1 shows the flow diagram of STZ-DIA.

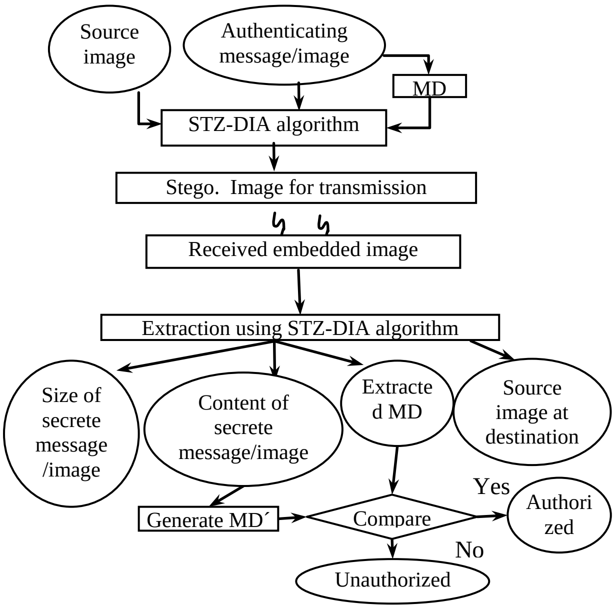
Source image
Authenticating message/image
MD
STZ-DIA algorithm
Stego. Image for transmission
Received embedded image
Extraction using STZ-DIA algorithm
Size of secrete message /image
Content of secrete message/image
Extracte d MD
Source image at destination
Yes
Authori zed
Generate MD´
Compare
No
Unauthorized

Figure 1. Schematic diagram of STD-DIA technique

II. EVALUATED AND SIMPLIFIED Z-TRANSFORM

The techniques used in this paper is two dimensional discrete Z-Transform and two dimensional discrete inverse Z-Transform represented as follows

A. *One Dimensional Z-Transform:*

A function f(n) can be represented in Z-Transform as

$$f(z) = \sum_{n=-\infty}^{\infty} f(n)z^{-n}$$

z is a complex number consisting of a real part and an imaginary part.

B. *Two Dimensional Z-Transform:*

A function f(n1,n2) can be represented in Z-Transform as

$$f(z1, z2) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1, n2)z1^{-n1}z2^{-n2} \quad …….(I)$$

z1 and z2 are both complex numbers consisting of a real part and an imaginary part.

C. *A Discrete Form of Z-Transform (Two Dimensional):*

Since z1 and z2 are complex numbers, Let z1=$e^{j\omega 1\pi}$ and z2=$e^{j\omega 2\pi}$

where $e^{j\theta} = \cos\theta + j\sin\theta$ is a complex number.

Substituting the values of z1 and z2 in equation (I), We have,

$$f(e^{j\omega 1\pi}, e^{j\omega 2\pi}) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1. n2){e^{j\omega 1\pi}}^{-n1}{e^{j\omega 2\pi}}^{-n2}$$

Or,

$$f(\omega 1, \omega 2) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1, n2)e^{-j\pi(n1\omega 1+n2\omega 2)} \quad (II)$$

This equation is the discrete form of Two Dimensional Z-Transform.

D. *Two Dimensional Inverse Z-Transform:*

The Inverse Z-Transform of a function f(n1,n2) is represented as

$$f(n1, n2) = \left(\frac{1}{2\pi j}\right)^2 \oint\!\!\oint f(z1, z2)z1^{n1-1}z2^{n2-1}\, dz1dz2…(III)$$

Where f(n1,n2) be a function and f(z1,z2) be the Z-Transform of the function f(n1,n2).

E. *Discrete Form of Inverse Z-Transform (Two Dimensional):*

Since z1 and z2 are complex numbers, Let z1=$e^{j\omega 1\pi}$ and z2=$e^{j\omega 2\pi}$

where $e^{j\theta} = \cos\theta + j\sin\theta$ is a complex number.

Substituting the values of z1 and z2 in equation (III), We have a discrete form of Inverse Z-Transform (Two Dimensional). z1=$e^{j\omega 1\pi}$

So, $\frac{dz1}{d\omega 1} = e^{j\omega 1\pi}j\pi$ or, $dz1 = e^{j\omega 1\pi}j\pi\, d\omega 1$

And z2=$e^{j\omega 2\pi}$

So, $\frac{dz2}{d\omega 2} = e^{j\omega 2\pi}j\pi$ or, $dz2 = e^{j\omega 2\pi}j\pi\, d\omega 2$

We can now conclude,

$$f(n1, n2) = \left(\frac{1}{2\pi j}\right)^2 \oint\!\!\oint f(e^{j\omega 1\pi}, e^{j\omega 2\pi}){e^{j\omega 1\pi}}^{n1-1}{e^{j\omega 2\pi}}^{n2-1}e^{j\omega 1\pi}j\pi\, d\omega 1\, e^{j\omega 2\pi}j\pi\, d\omega 2$$

Finally,

$$f(n1, n2) = \frac{1}{4}\sum_{\omega 1=-1}^{1} \sum_{\omega 2=-1}^{1} f(\omega 1, \omega 2)e^{j\pi(n1\omega 1+n2\omega 2)} \quad (IV)$$

This equation is the discrete form of Two Dimensional Inverse Z-Transform.

This paper presents a technique for image protection by inserting single bit of message/image along with message digest MD into the source image for image identification and also for secure message transmission. In STZ-DIA using 24 bits color image, single bits of secrete data are inserted in middle and low frequency value of the red, green and blue components from LSB. STZ-DIA embeds large amount of authenticating message/image with a bare minimum change of visual pattern with better security against statistical attacks.

Section III of the paper deals with the proposed technique. Results, comparison and analysis are given in section IV. Conclusions are drawn in section V and references are given in section VI.

III. THE TECHNIQUE

STZ-DIA used 24 bit colour image in which each pixel is the composition of red (R), green (G) and blue (B) of each 8-bit image. The proposed STZ-DIA embeds authenticating message/image *AIp*$_{,q}$ of size .75*(m x n) bits embedding capacity along with 128 bits MD and dimension of authenticating message/image (32 bits) to authenticate the source image SI$_{m,n}$ of size m x n bytes. 2 x 2 image block called mask is chosen from the source image matrix in row major order and transform it into frequency domain using (II). Depending on colour composition of source images single bit of authenticating message/image is inserted from LSB in each real part of each frequency component of source image block excluding the first frequency component of each image block. First component is used to maintain the imperceptibility and robustness. After embedding the authenticating data in frequency domain then the inverse Z-Transform is applied using (IV) to transform from frequency to spatial domain. Then each time re-adjusting phase is applied to overcome the negativity and fractional value in spatial domain. Finally a control technique is used to reduce the noise. In this technique just after the maximum embedding position are consider here and adjust them in such a manner that the changes remain optimal before and after embedding. The reverse operation is performed at the receiving end to extract bits of authenticating message/image and message digest MD for authentication at destination.

The Insertion of the authenticating image is performed in the Z-Domain. Hence, in order to perform the insertion operation of the authenticating image into the original image, the original image is converted to its corresponding frequency components using Z-Transform. Insertion position is calculated by the value of higher order three bits of each image byte. Let M x N be the size of the original digital color image. Evidently, M x N bits are to be embedded in the original digital color image. Hence, total number of bits embedded is equal to M x N.

A. *Algorithm for Insertion:*

Input: A carrier image and authenticating message/image.
Output: An authenticated image.
Method: Insert one bit in middle and low frequency values recursively

a. Obtain MD from source image and dimension of secrete data.
b. Read image type, dimensions and maximum intensity from source image and write in the output image.
c. Repeat until all pixels have been read from the source image.
    i. Repeatedly take 2 x 2 blocks of pixels from the image matrix and perform Z-Transform of the block of pixels until all pixels in the matrix have been taken.
    ii. Read the authenticating image.
    iii. Embed dimension of secrete data and MD.
    iv. Embed the watermark bits in the source image byte at the position based on the value of b_7+b_6+b_5 of source image byte.
    v. Compute the Inverse Z-Transform of the 2 x 2 block of pixels.
    vi. If any pixel is found to be of negative value, the maximum negative number is stored and added in the watermarked pixel values such that there is no effect on the bit position where the watermark bit is embedded.
    vii. Compute the Inverse Z-Transform of the block of pixels and the numbers obtained is guaranteed to be of positive values.
    viii. Read next two rows of pixels i.e. next 2*M no. of pixels where M is the no. of columns in the source image and repeat the steps from 3.1 to 3.8 until all pixels have been transformed.
d. Write the block of pixels back affter reading 2 rows of pixels and performing Z-Transform followed by watermarking and inverse Z-Transform
e. Stop.

B. *Algorithm for Extraction:*

Input: Authenticated image.
Output: The original image, authenticating message/image.
Method: Extract one bit from middle and low frequency values recursively

a. Read image embedded image..
b. Repeat until all pixels have been read from the embedded image file.
    i. Read two rows of pixels i.e. 2*M no. of pixels where M is number of columns in the embedded image and store the pixels in a 2 x M matrix.
    ii. Repeatedly take 2 x 2 blocks of pixels from the matrix at the left and perform Z-Transform of the block of pixels until all pixels in the matrix have been taken.
    iii. Calculate the position of the embedded bit from the embedded image byte using the decimal value of b_7+b_6+b_5.
    iv. Convert each 8 bits of 0's and 1's into decimal value and write the value in the output image.
    v. Read next two rows of pixels i.e. next 2*M no. of pixels where M is the no. of columns in the embedded image and repeat the steps from 2.1 to 2.5 until all pixels have been transformed and embedded bits have been calculated.
c. Close the files.

The proposed STZ-DIA technique embeds authenticating data into the middle and low frequency component of source image for any changes of frequency component it can affect the spectrum value which may change the quantum value in spatial domain. To maintain the balance in each mask first frequency component is used as re-adjust phase and remaining three of each mask is used to embed authenticating data.

In the proposed algorithm after embedding we have used inverse Z-transform to get the embedded image in spatial domain. Applying inverse Z-transform on identical mask with embedded data the quantum values may changes it can generate the following situation:

The converted value may by negative (-ve).

The converted value in spatial domain may be a number with non zero fractional value i.e. pure non integer number.

The converted value of each image byte may be greater the maximum value (i.e. 255).

The concept of re-adjust phase is to handle the above three serious problem by using the first frequency component of each mask. In this phase if the converted value is -ve or with fractional value then add 1 with the first frequency component in the mask and then apply inverse Z. This repeating process continue until all are not will be non negative and non fractional. For case (iii) if the number is greater than the maximum value then subtract 2 from the first frequency component and then apply inverse Z. This process is continuing until any value of the mask is greater than 255. Since the insertion and successive extraction follows the inverse z-transform and thereafter the z-transform of the image after the insertion operation, the image value obtained after performing the inverse z-transform should be an integer value as this value will be written into a file as the embedded image. So, if this value is not found to integer and is fractional, then some information may be lost. Hence, it is very important to ensure that the value obtained after the inverse z-transform must have the fractional part as .00 and to ensure this, we must look at the z-transform equation very closely. After performing the inverse z transform of the embedded block of pixels, some pixels may be found to have the negative values. This negativity error has been overcome by taking the maximum negative value form the 2x2 block of pixels and adding this maximum value to data obtained after performing the watermarking operation without affecting the bits where the authenticating bits have been embedded in the source image. After that, the 2x2 block of pixels are converted back to spatial domain using the inverse z transform.

IV. RESULT. COMPARISON AND ANALYSIS

This section represents the results, discussion and a comparative study of the proposed technique STZ-DIA with the DCT-based watermarking method and QFT based watermarking method in terms of visual interpretation, image fidelity (IF [23]), and peak signal-to noise ratio (PSNR [23]) analysis and mean square error (MSE [23]) . In order to test the robustness of the scheme STZ-DIA, the technique is applied on more than 50 PPM gray images from which it may be reveille that the algorithm may overcome any type of attack like visual attack and statistical attack. The distinguishing of source and embedded image from human visual system is quite difficult. In this section some statistical and mathematical analysis is given. The original source images ‘Peppers’, ‘Airplane’, ‘Lenna’, and ‘Fruits’ are shown in Fig. 2a, 2b, 2c and 2d and 71708 bytes of information are embedded. The dimension of each source colour images is 512 x 512 and the dimension of authenticating colour image is 180 x 180 showing in Fig. 2e. Fig. 2f, 2g, 2h, and 2i are embedded images using STZ-DIA. Magnified version of embedded images are 2j, 2k, 2l and 2m for checking visual distortion. But here distortion is negligible. We use the peak-to-signal noise ratio (PSNR) to evaluate qualities of the stegoimages. Table I shows the 71708 bytes of secrete data embedding is done with higher PSNR values for different source images. Here single bit of secrete data are embedded in middle and low frequency component. Table II shows the PSNR values for Lenna image in existing methods [22] like SCDFT, QFT and DCT. In all the techniques the dimension of Lenna JPEG image is 512 x 512. In all the existing technique the PSNRs are low, means bit-error rate are high but in the proposed scheme more bytes of authenticating data can be embedded and the PSNR values are significantly high, means bit-error rate is low. In DCT based watermarking scheme do not embed watermarks in every single block of image. Here selectively pick the regions that do not generate visible distortion for embedding, thus decreasing the authenticating data size. In QFT based watermarking compensation mark allows the watermark to be undetected even if the strength of it is high. For low compression factor it can not completely recover the embedded message. In STZ-DIA the average embedding capacity is 71708 bytes with higher average PSNR values 47.66 and completely recoverable the authenticating message/image. The proposed algorithm is capable to embed huge amount of data without visual distortion. Using STZ-DIA technique the average PSNR enhancements are 17.56, 16.74 and 17.26 dB than SCDFT, QFT and DCT respectively with 67864 bytes of more embedding capacity.

Fig.ure 2a. Source image ‘Peppers’

Figure 2b. Source image ‘Airplane’

Fig.ure 2c. Source image ‘Lenna’

Figure 2d. Source image ‘Fruits’

Figure 2e. Authenticating image ‘Earth’

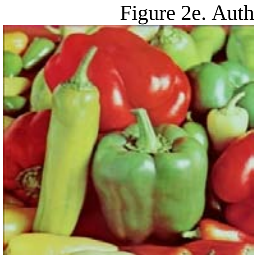

Figure 2f. Embedded image using STZ-DIA

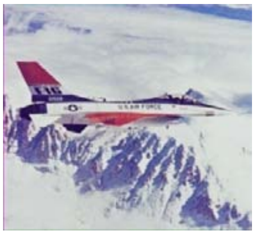

Figure 2g. Embedded image using STZ-DIA

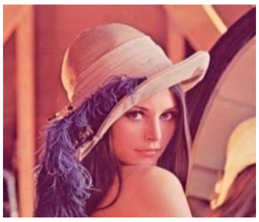

Figure 2h. Embedded image using STZ-DIA

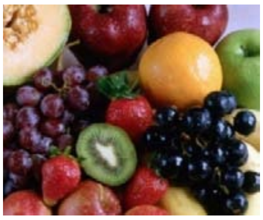

Figure 2i. Embedded image using STZ-DIA

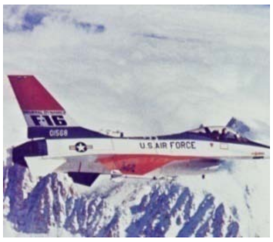

Figure 2j Magnified Embedded image

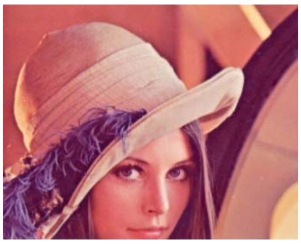

Figure 2k. Magnified Embedded image

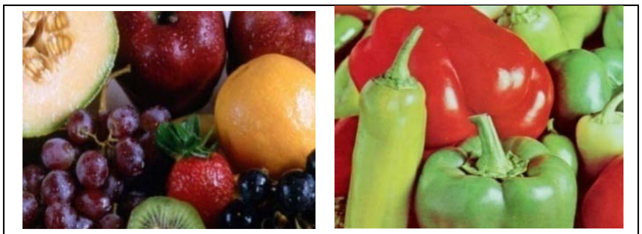

Figure 2l Magnified Embedded image

Figure 2m. Magnified Embedded image

Figure 2. Comparison of fidelity in embedded 'Peppers', 'Airplane', 'Lenna' and 'Fruits' images using STZ-DIA

Table 1: Capacities and PSNR, IF, and MSE in STZ-DIA on two bits Embedding

Carrier images	Capacity (byte)	MSE	PSNR in dB	IF
Airplane	71708	4.297176	46.893208	0.999920
Baboon	71708	3.652638	48.759319	0.999948
Lenna	71708	4.117269	47.296757	0.999992
Oakland	71708	3.679952	48.272072	0.999949
Peppers	71708	4.075100	47.311897	0.999974
Sailboat	71708	4.295314	48.004406	0.999982
San Diego	71708	3.768353	48.701622	0.999984
Splash	71708	4.123469	46.334290	0.999925
Tiffany	71708	3.718095	46.452286	0.999955
Woodlad	71708	3.956707	48.609322	0.999926
Average	71708	3.968407	47.66358	0.99995

Table 2: Capacities and PSNR for Lenna image in the existing technique [22]

Technique	Capacity(bytes)	PSNR in dB
SCDFT	3840	30.1024
QFT	3840	30.9283
DCT	3840	30.4046
STZ-DIA	**71708**	**47.66358**

V. CONCLUSIONS

STZ-DIA technique is an image authentication process in frequency domain to enhance the security compared to the existing algorithms. In compare to SCDFT, DCT and QFT based watermarking technique STZ-DIA algorithm is applicable for any type of color images authentication and strength is high. First frequency component in each mask is used for re-adjusting to overcome the negativity and fractional value. The control technique is applied to optimized the noise addition as a result PSNR is increased with low MSE and IF is nearer to 1. In the proposed STZ-DIA authentication is done in frequency domain without changing visual property of the authenticated image. In STZ-DIA distortion of image and change of fidelity (like sharpness, brightness etc) is negligible.

VI. ACKNOWLEDGEMENTS

The author expresses the deep sense of gratitude to the Dept. of Engineering and Technological studies, University of Kalyani, West Bengal, India, where the work has been carried out.

VII. REFERENCES

[1] Ghoshal N., Mandal, J. K. "A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT)", Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, pp. 24-32, 2008.

[2] Ghoshal N., Mandal, J. K. "A Bit Level Image Authentication / Secrete Message Transmission Technique (BLIA/SMTT)", Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition, Vol. 51, No. 4, pp. 1-13, France, 2008.

[3] Ghoshal N., Mandal, J. K. et al., "*Masking based Data Hiding and Image Authentication Technique (MDHIAT)*", Proceedings of 16th International Conference of IEEE on Advanced Computing and Communications ADCOM-2008, ISBN: 978-1-4244-2962-2, December 14-17th, Anna University, Chennai, India, pp. 119-122, 2008.

[4] R. Radhakrishnan, M. Kharrazi, N. Menon, "*Data Masking: A new approach for steganography*", Journal of VLSI Signal Processing, Springer, Vol. 41, pp. 293-303, 2005.

[5] Nameer N. EL-Emam, "Hiding a large Amount of data with High Security Using Steganography Algorithm," Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.

[6] P. Amin, N. Lue and K. Subbalakshmi, "Statistically secure digital image data hiding," IEEE Multimedia Signal Processing MMSP05, pp. 1-4, Shanghai, China, Oct. 2005.

[7] B. Chen and G. W. Wornnel, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," IEEE Trans. On Info. Theory, vol. 47, no. 4, pp. 1423-1443, May 2001.

[8] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proc. of ICIP, Thissaloniki, pp. 1019-1022, Greece, 2001.

[9] S. Dumitrescu, W. Xiaolin and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Trans. on Signal processing, Vol. 51, no. 7, pp. 1995-2007, 2003.

[10] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information Hiding," IEEE Trans. On Info. Theory, vol. 49, no. 3, pp. 563-593, March 2003.

[11] S. Pavan, S. Gangadharpalli and V. Sridhar, "Multivariate entropy detector based hybrid image registration algorithm," IEEE Int. Conf. on Acoustics, Speech and Signal Processing, Philadelphia, Pennsylvania, USA, pp. 18-23, March 2005.

[12] P. Moulin and M. K. Mihcak, "A framework for evaluating the data-hiding capacity of image sources," IEEE Transactions on Image Processing, vol. 11, pp. 1029-1042, Urbana, Illinois, Sept. 2002.

[13] A. H. Al-Hamami and S. A. Al-Ani "A New Approach for Authentication Technique", Journal of computer Science, ISSN 1549-3636, Vol. 1, No. 1, pp. 103-106, 2005.

[14] A. Ker, "Steganalysis of Embedding in Two Least-Significant Bits", IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 2, No. 1, pp. 46-54, 2008

[15] C. Yang, F. Liu, X. Luo and B. Liu, "Steganalysis Frameworks of Embedding in Multiple Least Significant Bits", IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 3, No. 4, pp. 662-672, 2008.

[16] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, Image steganographic scheme based on pisel-value differencing and LSB replacement methods, Proc. Inst. Elect. Eng., Vis. Images Signal Processing, Vol. 152, No. 5, pp. 611-615,2005

[17] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, Adaptive Data Hiding in edge areas of Images With Spatial LSB Domain Systems, IEEE Transaction on Information Forensics and Security, ISSN 1556-6013, Vol. 3, No. 3, pp 488-497, 2008

[18] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[19] N. Ahmidi, R. Safabkhsh, A novel DCT-based approach for secure color image watermarking, in Proc. Int. Conf. Information technology: Coding and Computing, vol. 2, pp. 709-713, Apr. 2004.

[20] C. H. Chou, Y. C. Li, A perceptually tuned subband image coder based on the measure of just-noticeable distortion profile, IEEE Trans. Circuits Syst. Video Technology vol. 5, no. 6, pp. 467-476, Dec. 1995.

[21] P. Bas, N. L. Biham, and J. Chassery, Color watermarking using quaternion Fourier transformation, in Proc. ICASSP, Hong Kong, China, pp. 521-524, Jun. 2003.

[22] T. T. Tsui, X. –P. Zhang, and D. Androutsos, Color Image Watermarking Usimg Multidimensional Fourier Transfomation, IEEE Trans. on Info. Forensics and Security, vol. 3, no. 1, pp. 16-28, 2008.

[23] M. Kutter and F. A. P. Petitcolas, “A fair benchmark for image watermarking systems”, Electronic Imaging ’99, Security and Watermarking for Multimedia Content, San Josh CA, USA 25-27, Vol. 3657, January 1999, pp. 226-239.