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

Transform Domain based Steganographic Technique for Image Authentication (TDSTIA)

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

Abstract: The paper proposed a novel steganographic technique based on Discrete Cosine Transform (DCT) for multimedia copyright protection in frequency domain. The transformation is implemented on sub-image block called mask of size 2 x 2 of spatial components in row major order for the entire image. After transformation the host image gets converted into sub band images. For embedding we choose middle frequency ranges. Single bit of authenticating secret message/image is fabricated in the real part of middle frequency component of each sub-image block. A minor re-adjustment is incorporated in the first component of each mask after embedding to keep the pixel values positive and non fractional in spatial domain. This approach improves the performance of the Steganographic technique compared to earlier techniques. Robustness is achieved through embedding secrete bits in variable positions of the carrier image byte determined by pseudo random value and subsequent masking. Experimental results depict enhanced performance of the proposed watermarking technique in terms of PSNR, IF, and MSE.

Keywords: QFT, DFT, DCT, MD and TDSTIA

I. INTRODAUCTION

Copyright protection, ownership verification, of digital images created new challenge due to the proliferation of frequent growth in digital technique and usage of internet. Steganography is an art to secrete writing within the object, where the hidden message will not be apparent to an observer. It is the technique of hiding information into digital images or other media in such a way that no one apart from the sender and intended recipient even realizes that there is hidden information. Secrete data transmission via the internet has some problem such as information security, copyright protection, originality and ownership 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 [1, 2, 3] overcome the problem by hiding the secrete information within 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.

Over the last few years many works have 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).

Various works has also 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.

Proposed TDSTIA emphasizes on secrete information transmission through image against unauthorized access in frequency domain to achieve a better tradeoff between robustness and perceptibility. Secrete message transmission is done by embedding the secrete data into the carrier colour image without changing visible property. This paper aims to exploit embedding process invariant of positive or negative frequency component. The proposed watermarking scheme for colour image authentication by hiding secretes data using some pseudo random mathematical calculation. The result of the proposed technique TDSTIA compared with the existing Reversible data hiding based on block median preservation (RDHBBMP [24]), DCT, QFT, SCDFT based watermarking method in terms of visual interpretation, MSE, PSNR in dB and IF. Fig. 1 and Fig. 2 shows the insertion and extraction process of TDSTIA.

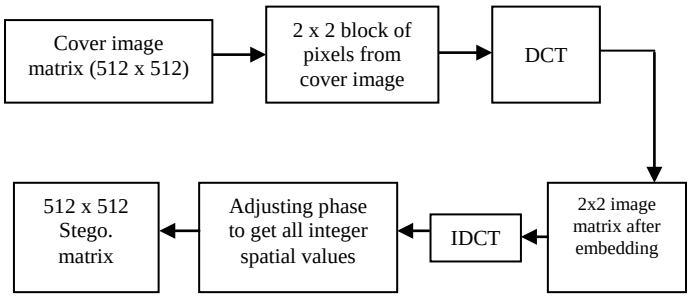

Figure 1. The process to embed the Secrete data into the source image

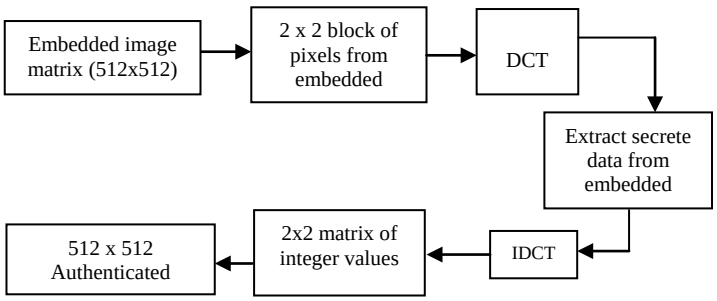

Figure 2. The process to extract the Secrete data from the stego. Image.

The proposed technique used two dimensional Discrete Cosine Transform and two dimensional Inverse Discrete Cosine Transform. The DCT represents an image as a sum of co sinusoids of varying magnitudes and frequencies. The property of DCT for a typical image is that significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. The two-dimensional DCT of an M x N matrix is defined as follows:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad (1)$$

The IDCT is an invertible DCT transform, and is given by

$$A_{mn} = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad (2)$$

The IDCT equation can be interpreted as any M x N matrix say A can be written as a sum of M x N functions of the form:

$$\alpha_p \alpha_q \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

These functions are called the basis functions of the DCT. The DCT coefficients Bpq, can then be regarded as the heights applied to each basis function.

This paper presents a technique for image protection by inserting one bit of secrete message/image into the medium frequency component along with message digest MD into the source image for secure message transmission and also for image identification. In TDSTIA using 24 bits color image, 1 (one) bit of secrete data are inserted in medium frequency component with a bare minimum change of visual pattern with better security against statistical and visual attacks.

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

II. THE TECHNIQUE

TDSTIA 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 TDSTIA embeds authenticating message/image $AI_{p,q}$ of size .75*(m x n) bits 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 DCT (1). Single bit of authenticating message/image are inserted from LSB in 2nd and 3rd real part of each frequency component of source image block. 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. After embedding the authenticating data in frequency domain then the IDCT is applied using (2) 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. The reverse operation is performed at the receiving end to extract bits of authenticating message/image and message digest MD for authentication at destination.

In the proposed algorithm after embedding we have used inverse Discrete Cosine Transform (IDCT) to get the embedded image in spatial domain. Applying IDCT on identical mask with embedded data the quantum values may changes it can generate the following situation:

i) f′(x, y) is not purely integer.
ii) f(x, y) + f′(x, y) < 0.
iii) f(x, y) + f′(x, y) > 255.

For the above problems the embedded image can not be realized in spatial domain. To resolve the above problems some deliberate action or re-adjust are to be needed. The concept of re-adjust phase is to handle the above three serious problems by using the unchanged portion of each frequency component of each mask. To overcome the problem (i) i.e. for non integer IDCT just complementing the LSB bit of 1st frequency component if needed. For

fractional value after stripping the LSB of the first frequency component the summation value of DCT component becomes even. In this phase if the converted value is -ve i.e. for problem (ii) the operation $\delta(u, v) + \varepsilon$ is applied where $\delta(u, v)$ and ε are change of variation in IDFT after embedding and 2^n respectively. This repeating process continues until all are not will be non negative. For case (iii) if the number is greater than the maximum value then perform $\delta(u, v) - \varepsilon$ where terms of expression indicates same meaning and then apply IDCT. This process is continuing until any value of the mask is greater than 255. The entire process of the TDSTIA technique is given in Fig. 3.

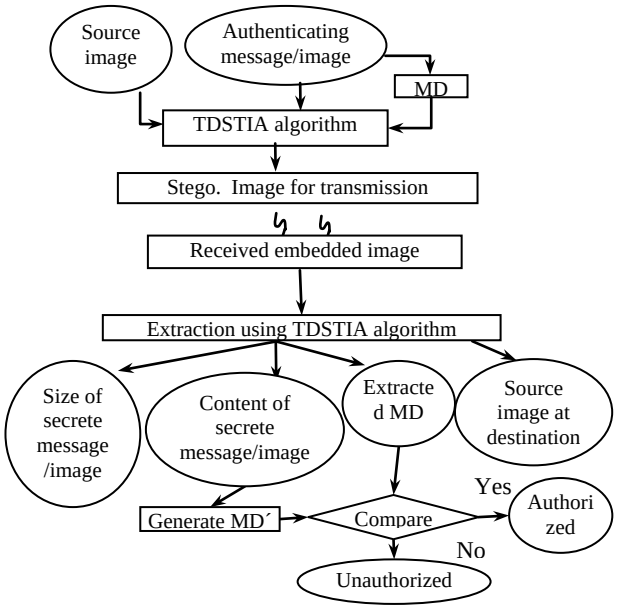

Figure 3. Schematic diagram of TDSTIA technique

A. Algorithm for Insertion:

The Insertion of the secrete data is performed into the frequency values. The frequency values obtained after performing the Discrete Cosine Transform on 2 x 2 sub-image matrix of the original image matrix one by one. Hence, in order to perform the insertion operation of the authenticating image into converted original image byte, bits from authenticating image are embedded in single bit position under each byte of the source image. Point of insertion of a bit is obtained dynamically by executing the pseudo random function and subsequent masking. Secrete bits are fabricated into the 2^{nd} and 3^{rd} image byte of each pixel. The TDSTIA scheme uses colour image as the input to be authenticated by text message/image. The authenticating message/image bits size is $.75*(m \times n) - (MD + L)$ where MD and L are the message digest and dimension of the authenticating image respectively for the source image size m x n bytes. The insertion and extraction algorithm are as follows:

Input: A source image and authenticating message/image.

Output: An authenticated image.

Method: Embedding is been performed only in the integer part of frequency value, whereas the fractional part remains intact. The fractional part has been re-added after embedding the secrete bits in the integer part of the pixels values of the source image. The algorithm is as follows:

a. Obtain the Dimension of the secrete image and MD from secrete image.
b. Read the source image type, dimensions and maximum intensity from source image and write in the output image.
c. Repeat the following steps until all pixels have been read from the source image file,
   i. Take 2 x 2 blocks of pixels from the source image matrix in row major order and perform DCT on the current block of pixels.
   ii. Compute a pseudo random number ip (between 0 - 5) using pseudo random function and subsequent mask [4] where the watermark bits will be embedded.
   iii. Read the authenticating image i.e. secret data.
   iv. Embed the watermark bits in the source image byte where the position of embedding is defined by the variable ip.
   v. Compute the Inverse DCT of the 2 x 2 block of pixels.
   vi. If any pixel is found to be of negative value, then the value at 1st position in the mask is incremented by 1, the value of sum is subsequently incremented by 1.
   vii. Repeat steps 3.5 to 3.6 until the negative value is eliminated.
   viii. Repeat the steps from 3.1 to 3.7 until all the pixels of watermark image have been embedded.
d. Stop

B. Algorithm for Extraction:

The extraction of the authenticating message/image is performed on the frequency component of stego. image bytes. The frequency values are obtained after performing the DCT operation on the embedded image. A mask based detection scheme has been proposed to retrieve the embedded watermark from a colour carrier image. In case of retrieval of the authenticating message/image, we will have only one extracted bit from 2^{nd} and 3^{rd} pixel of each mask of the stego. image. Point of extraction of a bit is obtained by executing the pseudo random function and subsequent mask.

The authenticated image is received in spatial domain. During decoding the embedded image has been taken as the input and the authenticating message/image size, image content and message digest MD are extracted data from it. All extraction is done in frequency domain from frequency component.

Input: Authenticated image.

Output: The original image, authenticating message/image.

Method: Extraction has been performed on the integer values only while the floating point part has been made intact and has been added after extracting the security bits from the integer part of the pixels values of the source image. The algorithm is as follows:

a. Read from the stego. image the image type and maximum intensity and write in the output image.
b. Repeat the following steps until all pixels have been read from the source image,
   i. Take 2 x 2 blocks of pixels from the embedded image matrix and perform DCT on the current block.

ii. Compute a pseudo random number *ip* (between 0 - 5) using random function and subsequent mask [4] from where the embedded bit will be extracted.
iii. Calculate the embedded bit from the steganographic image from the position specified by the number generated in step 2.2.
iv. Combine and convert each 8 bits of 0's and 1's into a decimal value and write the value in the output image.
v. Repeat the steps from 2.1 to 2.4 until all pixels have been transformed and embedded bits have been extracted.

c. Stop.

III. RESULT. COMPARISON AND ANALYSIS

This section represents the results, discussion and a comparative study of the proposed technique TDSTIA 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 TDSTIA, the technique is applied on more than 50 PPM colour images from which it may be reveille that the algorithm may overcome any type of attack like visual attack and statistical attack. Experimental set up for preparing result is any type of PC with 2.00 GHz or above processor speed, 1 GB or higher primary memory and Unix/Linux OS with Gimp (GNU Image Manipulation Program) application. 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. 4a, 4b, 4c and 4d and 48387 bytes of secrete information are embedded. The dimension of each source colour images is 512 x 512 and the dimension of authenticating colour image is 127 x 127 shown in Fig. 4e. For single bit embedding in 2nd and 3rd source image byte shown in Fig. 4f, Fig. 4g, Fig. 4h and Fig. 4i using TDSTIA. Fig. 4j, Fig. 4k, Fig. 4l, and Fig. 4m are showing the magnified version of different embedded images. From the magnified version of different images it is very difficult to identify the presence of secrete data in the carrier images.

Peak signal-to-noise ratio (PSNR) is used to evaluate qualities of the stego-images. Table I and II shows single level of authenticating data byte embedding which is defined by EL=0 based on PSNR values. Table II shows the PSNR values for comparative studies of TDSTIA and Reversible data hiding based on block median preservation (RDHBBMP) and also the enhancement in terms of hiding capacity of secrete data and PSNR in dB. The average enhancement of secrete data embedding is 20550 bits in TDSTIA than the existing technique RDHBBMP and also 2.64 dB of PSNR in EL=0. 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 squire bit-error rate is low. The average improvement is shown in Table II. Table 3 shows the better PSNR values than other exiting techniques like DCT-based [19] watermarking, QFT-based [20] watermarking, and SCDFT-based [22] watermarking in frequency domain. Capacities of existing techniques are 3840 bytes and the PSNR values are 30.1024 dB, 30.9283 dB, and 30.4046 dB in SCDFT, QFT, and DCT respectively. Whereas the capacity of TDSTIT is 48387 bytes and PSNR is 46.8100 dB and which is fully recoverable. 44547 bytes more secrete data embedding is possible in TDSTIA technique than existing techniques with average 15.88 dB more PSNR values. Table IV shows the 48387 bytes of secrete data embedding is done with higher PSNR values for different source images.


Fig.ure 4a. Source image 'Peppers'


Figure 4b. Source image 'Airplane'


Fig.ure 4c. Source image 'Lenna'


Figure 4d. Source image 'Fruits'


Figure 4e. Authenticating image 'Earth'

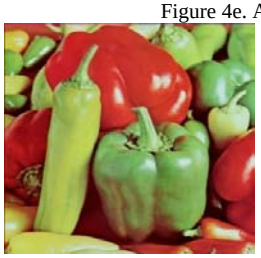
Figure 4f. Embedded image using TDSTIA


Figure 4g. Embedded image using TDSTIA


Figure 4h. Embedded image using TDSTIA


Figure 4i. Embedded image using TDSTIA

Figure 4j Magnified Embedded image


Figure 4k. Magnified Embedded image

Figure 4l Magnified Embedded image

Figure 4m. Magnified Embedded image

Figure 4. Comparison of fidelity in embedded 'Peppers', 'Airplane', 'Lenna' and 'Fruits' images using TDSTIA

Table 1: Capacities and PSNR values of TDSTIA

Test images	Indicator	EL=0
Lenna	C(bits)	139031
	PSNR	48.92
Fruits	C(bits)	139031
	PSNR	49.33
Peppers	C(bits)	139031
	PSNR	48.97
Average Image	C(bits)	139031
	PSNR	47.41

Table 2: Results and comparison in capacities and PSNR of TDSTIA and RDHBBMP

Test images	Indicator	EL=0	
		RDHBBMP	IATDCT
Baboon	C(bits)	36,465	58,890
	PSNR	49.68	52.86
Airplane	C(bits)	46,221	64,896
	PSNR	49.80	51.91
Average Image	Δ Ca	20550	
	Δ PSNRa	2.64	

Table 3: 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
TDSTIA	**48387**	**46.8100**

Table 4: Capacities and PSNR, IF, and MSE in TDSTIA after Embedding

Source images	Capacity (bytes)	PSNR in dB	IF	MSE
Lenna	48387	46.96	.999934	1.308355
Peppers	48387	46.96	.999934	1.308355
Woodlad	48387	47.03	.999946	1.289431
Splash	48387	47.08	.999933	1.273585
Airplane	48387	46.60	.999959	1.432666
Sailboat	48387	46.67	.999916	1.398483
Fruits	48387	46.50	.999879	1.456752
Baboon	48387	46.46	.999915	1.470612
Oakland	48387	46.96	.999939	1.308215
Sandiego	48387	46.87	.999933	1.335721
Average	48387	46.81	0.999929	1.358218

IV. CONCLUSIONS

TDSTIA is a DCT based secrete data transmission process through colour image in frequency domain to enhance the security compared to the existing algorithms. Secrete data transmission is done by embedding secrete data in a carrier image. It is also applicable to authenticate the image and to authenticate the legal document. IATDCT is for increasing the security of data hiding as compared with the existing algorithms. Authenticity is incorporated by embedding secret data in each mask of carrier image byte in randomly generated position. As compared with Reversible data hiding based on block median preservation, proposed IATDCT algorithm is applicable for any types of colour image under the source image of security and authenticity. First bit of (LSB) first frequency component in each mask is used for re-adjusting to overcome the fractional value in IDCT. Before readjusting the control technique is applied to optimize the noise addition as a result PSNR is increased with low MSE and IF is nearer to 1. In this technique just after the maximum embedding positions are consider here and adjust them in such a manner that the changes remain optimal before and after embedding. In the proposed TDSTIA authentication is done in frequency domain without changing visual property of the authenticated image. In TDSTIA distortion of image and change of fidelity (like sharpness, brightness etc) is negligible. The watermarked image in this algorithm is very difficult to detect due to unknown insertion position of the authenticating image bits in the carrier image. Hence, the proposed technique IATDCT is quite secured from almost any possible attacks.

V. ACKNOWLEDGEMENTS

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

VI. 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.

[24] H. Luo, F-X. Yu, H. Chen, Z-L Huang, H. Li, P-H. Wang, Reversible data hiding based on block median preservation, Information sciences, Vol 181, pp.308-328,2011

