Volume 2, No. 1, Jan-Feb 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

DFT based Hiding Technique for Colour Image Authentication (DFTHTCIA)

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

J. K. Mandal
Department of Computer Science and Engineering
University of Kalyani
Kalyani, Nadia, Pin. 741235, West Bengal, India
jkm.cse@gmail.com

Abstract: In this paper a novel data hiding technique in frequency domain has been proposed using Discrete Fourier Transform (DFT) for colour image authentication and secret message transmission. Image authentication is done by embedding message/image in frequency domain by choosing image blocks of size 2 × 2, called mask, from the source image in row major order and transform it into the frequency domain using DFT. Here three algorithms are developed for embedding secret data into the source image. In the 1st algorithm two bits of authenticating message/image/message-digest are fabricated within the real parts of each source image byte except first frequency component of each mask and in 2nd and 3rd algorithm three and four bits of authenticating or secrete data are embedded respectively. In all the proposed techniques the dimension of authenticating image followed by message digest (MD) and the content of authenticating message/image are embedded. Inverse DFT (IDFT) is performed on embedded data to transform embedded frequency component to spatial component. In order to keep the quantum value positive and non negative in spatial domain a strong and robust technique is incorporated mainly on the first frequency component and sometimes on other component depends upon situations. The decoding is done by applying the reverse algorithm. Experimental results conform that the proposed algorithm performs better than DCT, QFT and SCDFT schemes.

Keywords: QFT, DFT, IDFT, DCT, MD and SCDFT

I. INTRODAUCTION

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 [1, 2, 3] 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.

The proposed DFTHTCIA emphasizes on information and image protection against unauthorized access in frequency domain to achieve a better tradeoff between robustness and perceptibility. This paper aims to exploit embedding process invariant of positive or negative frequency component. This paper used the Discrete Fourier Transform to get frequency component for each pixel value. The Discrete Fourier Transform (DFT) of spatial value f(x , y) for the image of size M x N is defined in equation (1) for frequency domain transformation.

$$F(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\, e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \quad (1)$$

where u = 0 to M – 1 and v = 0 to N-1.

Similarly inverse discrete Fourier transform (IDFT) is used to convert frequency component to the spatial-domain value, and is defined in equation (2) for transformation from frequency to spatial-domain.

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v)\, e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \quad (2)$$

where u = 0 to M – 1 and v = 0 to N-1.

This paper presents a technique for image protection by inserting two, three and four bits of message/image along with message digest MD into the source image for image identification and also for secure message transmission. In DFTHTCIA using 24 bits color image, multiple bits of secrete data are inserted in each of the red, green and blue components from LSB. DFTHTCIA embeds large amount of authenticating message/image with a bare minimum change of visual pattern with better security against statistical attacks.

Problem motivation and formulation is given in section II. 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.

II. MOTIVATIO AND FORMULATION OF DFTHTCIA TECHNIQUE

The main motivation of the authentication problem is to achieve a better tradeoff between robustness and perceptibility. Robustness can be achieved by increasing the strength of the embedded authenticating message/image without visible distortion. Many human visual system based watermarking have been invented. Small portion of them are designed for colour images. These are not so robust for embedding large amount of information without image quality distortion. This paper aims to exploit proper quantum value handling in frequency domain and embeds large amount of information. In this technique each time we have taken an image block of size 2 x 2 and applying DFT. Considering a mask of size 2 x 2 and the values are {a, b, c, d} from the source image. The formulation of a mask in DFT is as follows:- After DFT the frequency components for four image bytes are F(a) = ½ (a + b + c + d) = W (say), F(b) = ½ (a – b + c – d) = X (say), F(c) = ½ (a + b – c – d) = Y (say), and F(d) = ½ (a – b – c + d) = Z (say) for four a, b, c, and d spatial domain image bytes. Here W, X, Y, and Z are all frequency components for a, b, c, and d spatial values respectively and all imaginary components are zeros because the imaginary component is the multiple of Π (pi). Embedding is done on X, Y, Z but not on W because W is used as re-adjust phase to balance the quantum values between original and embedded data. The corresponding IDFT values are $F^{-1}(W)$ = ½ (W + X + Y + Z), $F^{-1}(X)$ = ½ (W – X + Y –Z), $F^{-1}(Y)$ = ½ (W + X –Y –Z), and $F^{-1}(Z)$ = ½ (W – X – Y + Z). After re-adjusting phase all IDFT values are non negative and without fractional values. In this phase to remove the fractional value numeric 1 is to be added with the first component of each mask. In another treatment is applied to remove the negativity of the IDFT value by incrementing the positive quantum value 1 at a time and then apply IDFT and need to do repetition to complete the entire process.

III. THE TECHNIQUE

DFTHTCIA 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 DFTHTCIA embeds authenticating message/image $AI_{p,q}$ of size 2*(m x n), 3*(m x n) and 4*(m x n) bits respectively for different 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 (1). Depending on colour composition of source images two, three and four bits of authenticating message/image are 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 IDFT 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. 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.

In the frequency-domain all spatial-domain values are in form a + i*b, i.e. the complex frequency component. In DFTHTCIA we cleverly chose the image block of size 2 x 2 from the source image to avoid the non-zero imaginary frequency component in the transformed value. The DFT for the 2 x 2 mask is F(u, v) = ½∑∑f(x, y)[cos2Π(ux/2 + vy/2) – i sin2Π(ux/2 + vy/2)] =∑∑f(x , y)[cosΠ(ux + vy) – i sinΠ(ux + vy)] where value of spatial variables x, y are 0, 1 and the value of frequency variables u, v are 0,1. For any values of x, y, u, and v the value of the imaginary components are zero and values of real components are either +1 or -1. So for transformation of all elements of 2 x 2 matrix will be in the form of a + i*0 i.e. either +a or -a. The proposed DFTHTCIA technique embeds authenticating data into the 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 discrete Fourier transform (IDFT) to get the embedded image in spatial domain. Applying IDFT on identical mask with embedded data the quantum values may changes it can generate the following situation:

[a] The converted value may by negative (-ve).
[b] The converted value in spatial domain may be a number with non zero fractional value i.e. pure non integer number.
[c] 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 IDFT. 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 IDFT. This process is continuing until any value of the mask is greater than 255. The entire process of the DFTHTCIA technique is given in Fig. 1.

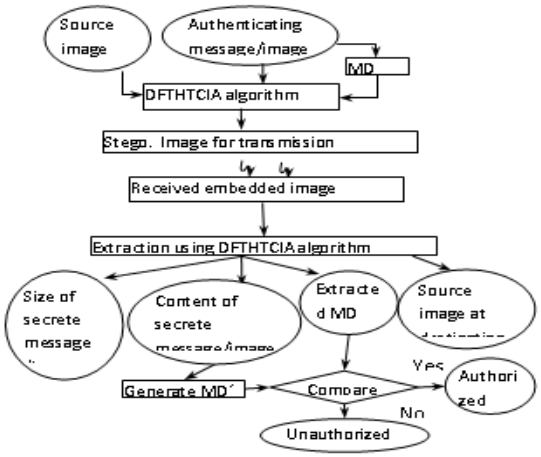

Figure 1. Schematic diagram of IATFDDFT technique

A. *Algorithm for Insertion*

In this algorithm all insertion is made in frequency domain i.e. each byte of source image in each mask of size 2 x 2 is transformed to frequency domain using DFT using (1). The DFTHTCIA scheme uses colour image as the input to be authenticated by text message/image. The authenticating message/image bits size is 2*(m x n) – (MD+L), 3*(m x n) – (MD+L) and 4*(m x n) – (MD+L) respectively in 1st, 2nd and 3rd algorithm where MD and L are the message digest and dimension of the authenticating image respectively for the source image size m x n bytes.

Steps:

[a] Obtain 128 bits message digest MD from the authenticating message/image.
[b] Obtain the size of the authenticating message/image (32 bits, 16 bits for width and 16 bits for height)
[c] Read authenticating message/image data do
[i] Read source image matrix of size 2 × 2 mask from image matrix in row major order and apply DFT.
[ii] Extract authenticating message/image bit one by one.
[iii] Embed the secrete 2/3/4 bits in each source image byte (excluding 1st component of the mask).
[d] Apply inverse DFT using identical mask.
[e] Apply re-adjust phase if needed.
[f] Apply control phase.
[g] Repeat step 3 to step 6 for the whole authenticating message/image size, content and for message digest MD.
[h] Stop.

B. *Algorithm for Extraction*

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.

Steps:

[a] Read embedded source image matrix of size 2 × 2 mask from image matrix in row major order and apply DFT.
[b] For each mask do
[i] Extract the message/image 2/3/4 bits from the LSB of real frequency part (excluding 1st frequency component of each mask) for each embedded image quantum value where authenticating message/ image bits are available.
[ii] For each 8 (eight) bits extraction construct one alphabet/one primary (R/G/B) colour image.
[c] Repeat step 1 and step 2 to complete decoding as per size of the authenticating message/image.
[d] Obtain 128 bits message digest MD′ from the extracted authenticating message/image. Compare MD′ with extracted MD. If both are same the image is authorized else unauthorized.
[e] Apply inverse DFT using identical mask.
[f] Stop.

C. *Example*

In this section the process of proposed DFTHTCIA technique is figuratively presented sequentially. Consider the message string ‘SACHIN’ (Fig. 2a) to be embedded into the source image matrix as given in Fig. 2b. Fig. 2c shows the scheme for transformation of one 2 × 2 submatrix from spatial domain to frequency domain using DFT using (1). Here carrier image bits are replaced by message bits at 2

Positions of real part (transformed value) of source transformed value from LSB. Figure 2d shows the control and re-adjusting phase. Inverse transformation IDFT of the embedded image is shown in Fig. 2e for transformation from frequency domain to spatial domain. Before IDFT the control technique is applied to optimize the noise integration. After IDFT in each mask to remove the negativity and fractional value of each quantum values the re-adjust phase is applied.

Character	ASCII Code
S	01010011
A	01000001
C	01000011
H	01001000
I	01001000
N	01001110

Figure 2a. Secrete Data

15	36	19	45
17	20	55	78
11	10	16	80
4	6	18	91
0	34	15	54
30	15	12	70

Figure 2b. Source Image

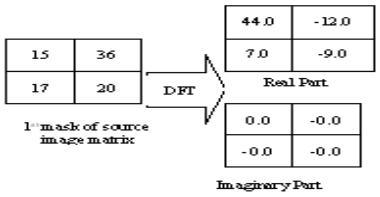

Figure 2c. Conversion of image matrix into frequency domain using DFT

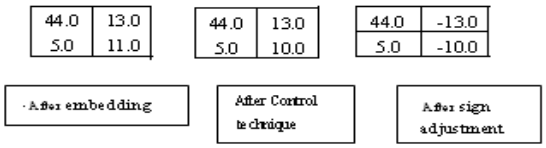

Figure.2d. Re-adjust phase in intermediate stage of DFTHTCIA

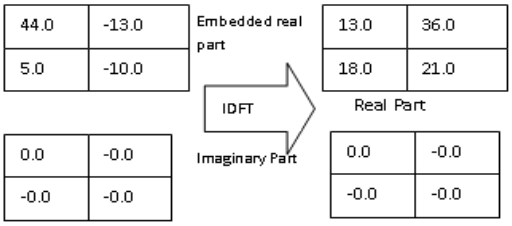

Figure 2e. Conversion from frequency domain to spatial domain

IV. RESULT. COMPARISON AND ANALYSIS

This section represents the results, discussion and a comparative study of the proposed technique DFTHTCIA 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 DFTHTCIA, the technique is

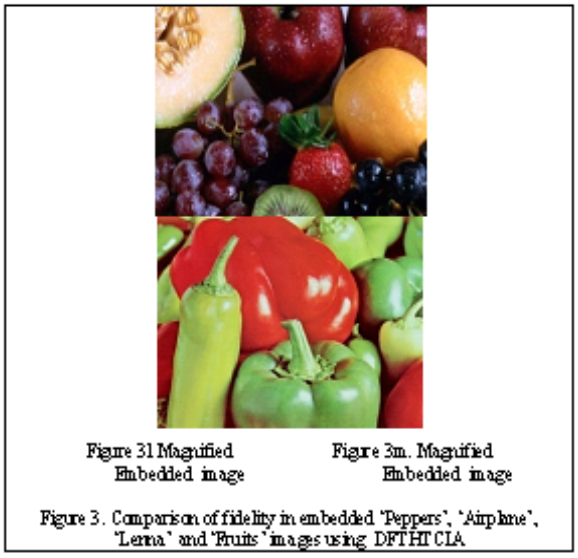

Figure 31 Magnified Embedded image

Figure 3m. Magnified Embedded image

Figure 3. Comparison of fidelity in embedded 'Peppers', 'Airplane', 'Lenna' and 'Fruits' images using DFTHTCIA

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

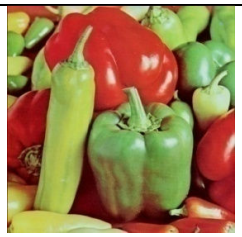

Fig.ure 3a. Source image 'Peppers'

Figure 3b. Source image 'Airplane'

Fig.ure 3c. Source image 'Lenna'

Figure 3d. Source image 'Fruits'

Figure 3e. Authenticating image 'Earth'

Figure 3f. 2 bits Embedded image using DFTHTCIA

Figure 3g. 3 bits Embedded image using DFTHTCIA

Figure 3h. 4 bits Embedded image using DFTHTCIA

Figure 3i. 4 bits Embedded image using DFTHTCIA

Figure 3j Magnified Embedded image

Figure 3k. Magnified Embedded image

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. 3a, 3b, 3c and 3d and 147456 bytes of information are embedded into 3a, 221184 bytes of secrete information are embedded in 3b and 294912 bytes secrete information are embedded in 3c and 3d. The dimension of each source colour images is 512 x 512 and the dimension of authenticating colour image is 220 x 220 for 2 bits embedding in each source image byte, 270 x 270 for 3 bits embedding in each source image byte and 310 x 310 for 4 bits embedding in each source image byte shown in Fig. 3e. Fig. 3f, 3g and Fig. 3h, 3i are 2, 3 and 4 bits embedded images using DFTHTCIA. 2/3/4 bits of authenticating information are embedded from LSB of real part of the frequency component excluding first component in each mask.

We use the peak-to-signal noise ratio (PSNR) to evaluate qualities of the stegoimages. Table I shows the 147456 bytes of secrete data embedding is done with higher PSNR values for different source images. Here 2 bits of secrete data are embedded in each carrier image byte. Table II shows the 221184 bytes of secrete data embedding is done with little bit less PSNR values than previous method for different source images. Here 3 bits of secrete data are embedded in each carrier image byte. Table III shows the 294912 bytes of secrete data embedding is done with some less PSNR values for different source images. Here 4 bits of secrete data are embedded in each carrier image byte. Table IV 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 DFTHTCIA the average embedding capacity is 147456, 221184 and 294912 bytes on 2 bits, 3 bits and 4 bits embedding with higher average PSNR values 46.81, 40.86 and 34.63 respectively and completely recoverable the authenticating message/image. The proposed algorithm is capable to embed huge amount of data without visual distortion. Using DFTHTCIA technique the average PSNR enhancements are 16.17, 15.89 and 16.41 dB than SCDFT, QFT and DCT respectively with 143616 bytes of more embedding capacity.

Table I : Capacities and PSNR, IF, and MSE in DFTHTCIA on two bits Embedding

Source images	Capacity (bytes)	PSNR in dB	IF	MSE
Sandiego	147456	46.96	.999934	1.308355
Sailboat	147456	46.96	.999934	1.308355
Woodlad	147456	47.03	.999946	1.289431
Baboon	147456	47.08	.999933	1.273585
Airplane	147456	46.60	.999959	1.432666
Peppers	147456	46.67	.999916	1.398483
Fruits	147456	46.50	.999879	1.456752
Splash	147456	46.46	.999915	1.470612
Oakland	147456	46.96	.999939	1.308215
Lenna	147456	46.87	.999933	1.335721
Average	147456	46.81	0.999929	1.358218

Table II: Capacities and PSNR, IF, and MSE in DFTHTCIA on three bits Embedding

Source images	Capacity (byte)	PSNR In dB	IF	MSE
Sandiego	221184	41.32	.999827	4.796300
Sailboat	221184	41.13	.999747	5.015907
Woodlad	221184	41.26	.999797	4.859393
Baboon	221184	41.42	.999755	4.683716
Airplane	221184	40.24	.999824	6.156797
Peppers	221184	40.75	.999671	5.471458
Fruits	221184	40.14	.999476	6.300003
Splash	221184	40.23	.999642	6.186651
Oakland	221184	41.25	.999773	4.874138
Lenna	221184	40.89	.999734	5.299942
Average	221184	40.86	0.999725	5.364431

Table III : Capacities and PSNR, IF, and MSE in DFTHTCIA on four bits Embedding

Source images	Capacity (byte)	PSNR In dB	IF	MSE
Sandiego	294912	35.23	.999297	19.520439
Sailboat	294912	34.96	.998956	20.733816
Woodlad	294912	35.12	.999164	19.983373
Baboon	294912	35.35	.999008	18.990873
Airplane	294912	33.92	.999246	26.391301
Peppers	294912	34.58	.998636	22.664080
Fruits	294912	33.54	.997604	28.801844
Splash	294912	33.87	.998455	26.688204
Oakland	294912	35.14	.999072	19.889028
Lenna	294912	34.57	.998860	22.701757
Average	294912	34.63	0.99883	22.636472

Table IV.: 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
DFTHTCIA (2 bits in each bytes)	147456	46.81
DFTHTCIA (3bits in each bytes)	221184	40.86
DFTHTCIA (4 bits in each bytes)	221184	34.63

V. CONCLUSIONS

DFTHTCIA technique is an image authentication process in frequency domain to enhance the security compared to the existing algorithms. Using this technique 2/3/4 bits of secrete data embedding in each carrier image byte is possible depending on the colour quantum value. In compare to DCT and QFT based watermarking technique DFTHTCIA 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 DFTHTCIA authentication is done in frequency domain without changing visual property of the authenticated image. In DFTHTCIA 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 Computer Sc. and Engg. & Department 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.