ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Steganographic Technique for High Volume Secrete Data Transmission through Colour Image (STHVSDTCI)

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

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

Abstract: This paper presents a novel steganographic technique which demonstrates the secrete data transmission technique through colour image in frequency domain based on the Discrete Fourier Transformation (DFT) which pertain to colour image authentication. Secrete transmission is done by hiding secrete message/secrete image into the transformed frequency component of source image. The DFT is applied on sub-image block called mask of size 2 x 2 in row major order. Three secrete message/image bits are fabricated within the transformed real frequency component of each source image byte except the LSB of first frequency component of each mask. After embedding, a delicate re-adjust phase is incorporated in all the frequency component of each mask, to keep the quantum value positive and non fractional in spatial domain. Robustness is achieved by hiding an authenticating or secretes message/image in the frequency component with both positive and negatives quantum values and invisibility is satisfied in spatial domain using delicate re-adjust phase. Inverse DFT (IDFT) is performed as final steps after embedding to transform embedded image in frequency domain to spatial domain. Experimental results conformed that the proposed algorithm performs better than discrete cosine transformation (DCT), Quaternion Fourier Transformation (QFT) based scheme and Spatio Chromatic DFT (SCDFT).

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

I. INTRODAUCTION

Steganography or secrete writing is a process applied to hide a message within an object, where the hidden message will not be apparent to an observer. It 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. 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.

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).

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 STHVSDTCI 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. 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 three bits of secrete message/image along with message digest MD into the source image for secure message transmission and also for image identification. In STHVSDTCI using 24 bits color image, 3 (three) bits of secrete data are inserted in each of the red, green and blue components from LSB. STHVSDTCI embeds 9 bits of authenticating message/image in each source image pixel 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, acknowledge is drawn in section VI and references are given in section VII.

II. Motivatio And Formulation of STHVSDTCI 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 i.e. sin signal is the multiple of Π (pi). Embedding is done on W, X, Y, and Z. Re-adjust phase is used on all quantum values 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, all quantum values are less than equal to 255 and without fractional values.

III. The Technique

STHVSDTCI 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 STHVSDTCI embeds authenticating message/image $AI_{p,q}$ of size 1.03*(m x n) bytes 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). Three bits of authenticating message/image are inserted from LSB in 2nd, 3rd, and 4th real part of each frequency component of source image block but in the first frequency component two bits of secrete data are embedded after LSB. 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. LSB of first component is used to overcome fractional problem in the embedded data. 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. 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. The DFT for the M x N matrix is: $F(u,v)=1/\sqrt{MN}\sum\sum f(x,y)$ $[\cos 2\Pi(ux/M+vy/N)-i\sin 2\Pi(ux/M+ vy/N)]$ where $0\le u, x\le M-1$ and $0\le v, y\le N-1$,after embedding in the n bits form LSB the frequencu component will be say $F'(u,v) =1/\sqrt{MN}\sum\sum[f(x, y)+f'(x,y)][\cos 2\Pi(ux/M +vy/N)-i\sin 2\Pi(ux/M+vy/N)]$ where f′(x,y) is the change of quantum value in spatial domain for the respective change of quantum value in frequency domain. Here embedding is done only in the absolute integer value in the real part. In STHVSDTCI 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: $F(u,v)=\frac{1}{2}\sum\sum f(x, y)[\cos 2\Pi(ux/2+vy/2) - i \sin 2\Pi(ux/2 + vy/2)] = \sum\sum f(x , y)[\cos\Pi(ux + vy) - i \sin\Pi(ux + vy)]$ where value of spatial variables x, y are 0, 1 and the value of frequency variables u, v are 0, 1. So, the imaginary value of F(u,v) i.e. $I_m(F(u,v)) = 0$ because $\sin(n*\Pi) = 0$. 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 STHVSDTCI 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.

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:

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. Now IDFT of the embedded DFT for 2 x 2 mask is: $f(x, y) + f'(x, y) = 1/2 \sum\sum F'(u, v) [\cos 2\Pi(ux / 2 + vy / 2) - i\sin 2\Pi(ux / 2 + vy / 2)]$ and $f(x, y) = 1/2 \sum\sum F(u, v) [\cos 2\Pi(ux / 2 + vy / 2) - i\sin 2\Pi(ux / 2 + vy / 2)]$ so, it is obvious $f'(x, y) = 1/2 \sum\sum [F(u, v) - F'(u, v)] [\cos 2\Pi(ux / 2 + vy / 2) - i\sin 2\Pi(ux / 2 + vy / 2)] = 1/2 \sum\sum \delta(u, v) [\cos 2\Pi(ux / 2 + vy / 2) - i\sin 2\Pi(ux / 2 + vy / 2)]$ where $\delta(u, v) = F(u, v) - F'(u, v)$. To overcome the problem (i) i.e. for non integer IDFT just changing (complement) of LSB bit of 1st frequency component is needed. For fractional value after stripping the LSB of the first frequency component the summation value after DFT 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 IDFT. This process is continuing until any value of the mask is greater than 255. The entire process of the STHVSDTCI technique is given in Fig. 1.

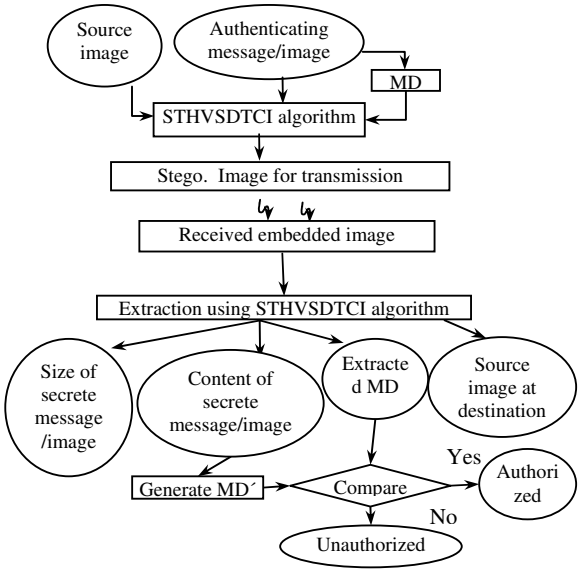

Figure 1. Schematic diagram of STHVSDTCI technique

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 STHVSDTCI scheme uses colour image as the input to be authenticated by text message/image. The authenticating message/image bits size is $1.03*(m \times n) - (MD + L)$ where MD and L are the message digest and dimension of the authenticating image respectively for the source image size m x n bytes.

Steps:

1. Obtain 128 bits message digest MD from the authenticating message/image.
2. Obtain the size of the authenticating message/image (32 bits, 16 bits for width and 16 bits for height)
3. Read authenticating message/image data do
   - Read source image matrix of size 2×2 mask from image matrix in row major order and apply DFT.
   - Extract authenticating message/image bit one by one.
   - Embed the 2 bits secrete data in the 1st except LSB and 3 bits in 2nd, 3rd, and 4th frequency component respectively form LSB in each mask.
4. Apply inverse DFT using identical mask.
5. Apply control phase.
6. Apply re-adjust phase if needed.
7. Repeat step 3 to step 6 for the whole authenticating message/image size, content and for message digest MD.
8. 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:

1. Read embedded source image matrix of size 2×2 mask from image matrix in row major order and apply DFT.
2. For each mask do
   - Extract the message/image 2 bits form 1st except LSB and 3 bits from 2nd, 3rd, 4th frequency components from LSB of real frequency part for each embedded image quantum value where authenticating message/image bits are available.
   - For each 8 (eight) bits extraction construct one alphabet/one primary (R/G/B) colour image.
3. Repeat step 1 and step 2 to complete decoding as per size of the authenticating message/image.
4. 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.
5. Apply inverse DFT using identical mask.
6. Stop.

C. *Example*

In this section the process of proposed STHVSDTCI 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 excluding LSB in 1st and 3 positions in 2nd, 3rd, 4th of real part (transformed value) of source transformed value from LSB. Figure 2d shows the control and re-adjusting phase.

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

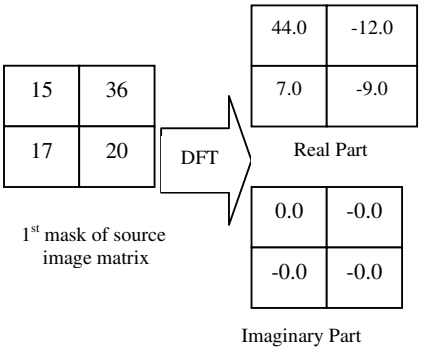

Figure 2c. Conversion of image matrix into frequency domain using DFT

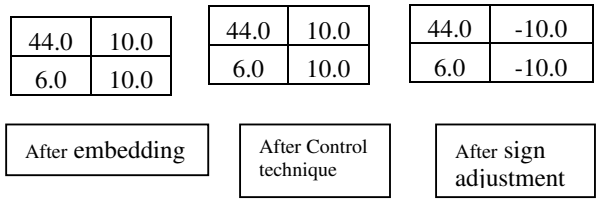

Figure.2d. Re-adjust phase in intermediate stage of STHVSDTCI

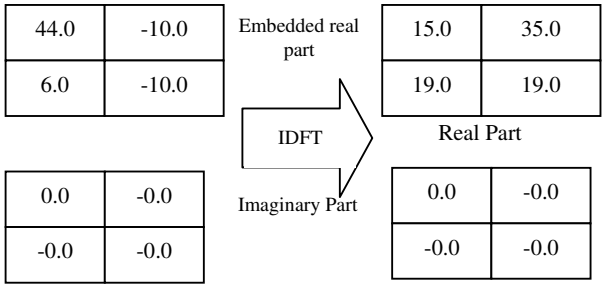

Figure 2e. Conversion from frequency domain to spatial domain

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.

IV. Result, Comparison And Analysis

This section represents the results, discussion and a comparative study of the proposed technique STHVSDTCI 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 STHVSDTCI, 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. 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. 3a, 3b, 3c and 3d and 270336 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 300 x 300 shown in Fig. 3e. For 3 bits embedding in each source image byte shown in Fig. 3f, Fig. 3g, Fig. 3h and Fig. 3i using STHVSDTCI. 2 bits secrete data are embedded in the 1st except LSB and 3 bits of authenticating information are embedded into 2nd, 3rd, 4th frequency component from LSB of real part of the frequency component. Fig. 3j, Fig. 3k, Fig. 3l, and Fig. 3m 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.

We use the peak-to-signal noise ratio (PSNR) to evaluate qualities of the stegoimages. Table I shows that 270336 bytes of secrete data embedding is done with higher PSNR values for different source images. 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 STHVSDTCI the average embedding capacity is 270336 on 3 bits embedding with higher average PSNR values 39.77 and completely recoverable the authenticating message/image. The proposed algorithm is capable to embed huge amount of data without visual distortion as a result huge amount of secrete data transmission is possible though a carrier image. Using STHVSDTCI technique the average PSNR enhancements are 9.67, 8.84 and 9.37 dB than SCDFT, QFT and DCT respectively with 266496

bytes of more embedding capacity. Though the technique STHVSDTCI is capable to embed more bytes of secrete data, due to the application of control technique noise integration is minimizes and image fidelity increases. The average MSE and IF are 6.893558 and .999645 respectively. For higher IF proposed algorithm is able to resist the visual attack.

Figure 3a. Source image 'Peppers'

Figure 3b. Source image 'Airplane'

Figure 3c. Source image 'Lenna'

Figure 3d. Source image 'Fruits'

Figure 3e. Authenticating image 'Earth'

Figure 3f. Embedded image using STHVSDTCI

Figure 3g. Embedded image using STHVSDTCI

Figure 3h. Embedded image using STHVSDTCI

Figure 3i. Embedded image using STHVSDTCI

Figure 3j Magnified Embedded image

Figure 3k. Magnified Embedded image

Figure 3l Magnified Embedded image

Figure 3m. Magnified Embedded image

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

Table I
Capacities and PSNR, IF, and MSE in STHVSDTCI on three bits Embedding

Source images	Capacity (byte)	PSNR In dB	IF	MSE
Sandiego	270336	40.26	.999780	6.121496
Sailboat	270336	40.06	.999677	6.410909
Woodlad	270336	40.18	.999739	6.233676
Baboon	270336	40.35	.999686	6.005305
Airplane	270336	39.35	.999784	7.560054
Peppers	270336	39.42	.999553	7.427592
Fruits	270336	39.07	.999330	8.060610
Splash	270336	39.10	.999537	8.001447
Oakland	270336	40.05	.999700	6.433606
Lenna	270336	39.88	.999665	6.680883
Average	270336	39.77	0.999645	6.893558

Table II.
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
STHVSDTCI	**270336**	**39.7700**

V. CONCLUSIONS

STHVSDTCI technique is a 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. Using this technique 3 bits of secrete data embedding in each carrier image byte is possible. In compare to DCT and QFT based watermarking technique STHVSDTCI algorithm is applicable for any type of color images authentication and strength is high. First bit of (LSB) first frequency component in each mask is used for re-adjusting to overcome the fractional value in IDFT. 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 STHVSDTCI authentication is done in frequency domain without changing visual property of the authenticated image. In STHVSDTCI 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.

