



Twin Image Authentication by Distributed Data Hiding (TIADDH)

Anirban Goswami*

Dept. of Information Technology, Techno India,
EM 4/1 Salt Lake, Sec-V
Kolkata-700091, India
an_gos@yahoo.com

Dipankar Pal

Dept. of Computer Science and Engineering, Techno India
EM 4/1 Salt Lake, Sec-V
Kolkata-700091, India
mail2dpal@yahoo.com

Nabin Ghoshal

Dept. of Engineering and Technological Studies, University of Kalyani,
Kalyani, Nadia-741235 West Bengal, India
nabin_ghoshal@yahoo.co.in

Abstract: In frequency domain steganography, use of gray scale images for secret data hiding has already been proved authentic. But to enhance the level of authenticity and secrecy of steganography and also to increase the volume of data to be hidden, pairs of gray scale carrier images are used in the proposed work. Each image is considered as a collection of contiguous blocks. The spatial values in each block of size 2×2 are first converted to frequency components by applying Discrete Cosine Transform (DCT). Then a message digest is generated for the payload/secret data. Both the payload data and the generated message digest are fabricated within the carrier frequency components. The first frequency component of each block is not used for embedding but is used for re-adjustments to maintain the quantum values positive and non-fractional in spatial domain and also to reduce the integrated noise due to embedding of payload. Further, to enhance the strength of secrecy of the embedded message a method has been devised which deduces pseudo-random positions for embedding and subsequent extraction of secret data bits. Finally, each block of frequency components is reverted back into spatial domain by applying Inverse Discrete Cosine Transform (IDCT). The results, after experimenting with the proposed technique, establish its superiority over other similar techniques in terms of capacity and imperceptibility.

Keywords: Image Authentication, Digital Watermarking, Steganography, DCT, IDCT, MSE, PSNR, IF, SSIM

I. INTRODUCTION

The demand of privacy acts as a key factor in increasing the importance of communication security. Had information been transmitted over an insecure channel, there is a risk that the information may be stolen by illegal third party. There are two methods to protect the confidentiality of information. One solution utilizes encryption [20], but its drawback is that encrypted messages can inspire any unauthorized individual to block and even attempt to decrypt the encrypted content. The second solution is steganography [2, 3], which aims to embed any secret information such as text, audio, image, video, database, etc. into a non-sensitive cover object (audio/video/image), without arousing any human suspicion.

The technique of steganography emphasizes on message embedding without introducing detectable alteration on statistics of the cover media. For an image steganography system two important factors are capacity [5] and imperceptibility [4]. The term capacity means the quantity of bits that can be embedded into a cover image and imperceptibility means that embedding should not introduce perceptual distortion which may arouse human suspicion.

Here, in this context, we discuss some of the notable research works in the field of image steganography implemented using Discrete Cosine Transform (DCT):

a. Combination of LSB and DCT based steganography. Dr. Ekta Walia et al. [13] implements DCT based

Steganography by embedding the text message in least significant bits (LSB) of the Discrete Cosine (DC) coefficients of a digital picture.

- b. Statistical distributions of DCT coefficients. Rufen Chu et al. [14] takes advantage of the similarities of DCT coefficients between the adjacent image blocks and makes the embedding distortion spread to the adjacent image blocks.
- c. Huffman coding incorporated with block DCT. A Nag et al. [15] implemented Huffman encoding on the secret messages/images before embedding and each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks.
- d. Implementation of four layer security in frequency domain (DCT). Thekra Abbas et al. [16] figured out that the data in the cover image are modified without deteriorating the integrity of the cover image and the message is embedded mimicking the characteristics of the cover bits.
- e. DCT and Average Covariance based steganography. N Satisha et al. [17] considered 0.15 as the threshold value of Average Covariance and the Most Significant Bits (MSBs) of payload are embedded into the cover image based on ACCI and DCT coefficients.
- f. Use of magnitude modulation technique in DCT based steganography. Saad M. A. AL-MOMEN et al [18] devised an algorithm which embeds data in the middle and high frequency region of the DCT domain. The embedding

module hides the bits sequence in a chosen area in the frequency domain, after applying a magnitude modulation method on the chosen transformed coefficients to imply uniform quantization.

Study of the existing algorithms reveal that digital data can be effectively hidden in an image with imperceptible degradation to the host image but less protection against various attacks. Moreover the data is hidden in a single image which may result in increase of vulnerability in detection of the secret data. Hence, the combination of capacity and security is the core issue in designing our proposed steganography algorithm.

TIADDH proposes a technique that facilitates secret document authentication by embedding the data adaptively in two overlapping gray images in dynamically generated positions. The algorithm has been designed considering the various aspects of human visual system (HVS) along with key features like high capacity [19] and low distortion.

Figure 1 pictorially demonstrates the insertion and extraction processes of our algorithm. The methods of two dimensional Discrete Cosine Transform (DCT) and Inverse Discrete Cosine Transform (IDCT), used in our algorithm, are explained in sub section A. Sec. II explains the insertion and extraction algorithms of TIADDH. The experimental results based on SSIM, MSE, PSNR in dB and IF are depicted in sec. III followed by conclusion in sec. IV.

A. Two Dimensional Discrete Cosine and Inverse Discrete Cosine Transform:

The general equation of two-dimensional DCT implemented on M x N matrix is defined below:

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

$$0 \leq q \leq N-1$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{2}/M, & 1 \leq p \leq M-1 \end{cases} \quad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{2}/N, & 1 \leq q \leq N-1 \end{cases}$$

B_{pq} is the DC coefficient of spatial value A_{mn} . After applying DCT on four spatial values {a, b, c, d} considering a block (size 2x2) from the source image, the resultant frequency components are: $W = DCT(a) = 1/2 (a + b + c + d)$, $X = DCT(b) = 1/2 (a - b + c - d)$, $Y = DCT(c) = 1/2 (a + b - c - d)$ and $Z = DCT(d) = 1/2 (a - b - c + d)$.

The general equation of IDCT is expressed as,

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

$$0 \leq n \leq N-1$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{2}/M, & 1 \leq p \leq M-1 \end{cases} \quad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{2}/N, & 1 \leq q \leq N-1 \end{cases}$$

The corresponding IDCT values are $DCT^{-1}(W) = 1/2 (W + X + Y + Z)$, $DCT^{-1}(X) = 1/2 (W - X + Y - Z)$, $DCT^{-1}(Y) = 1/2 (W + X - Y - Z)$, $DCT^{-1}(Z) = 1/2 (W - X - Y + Z)$.

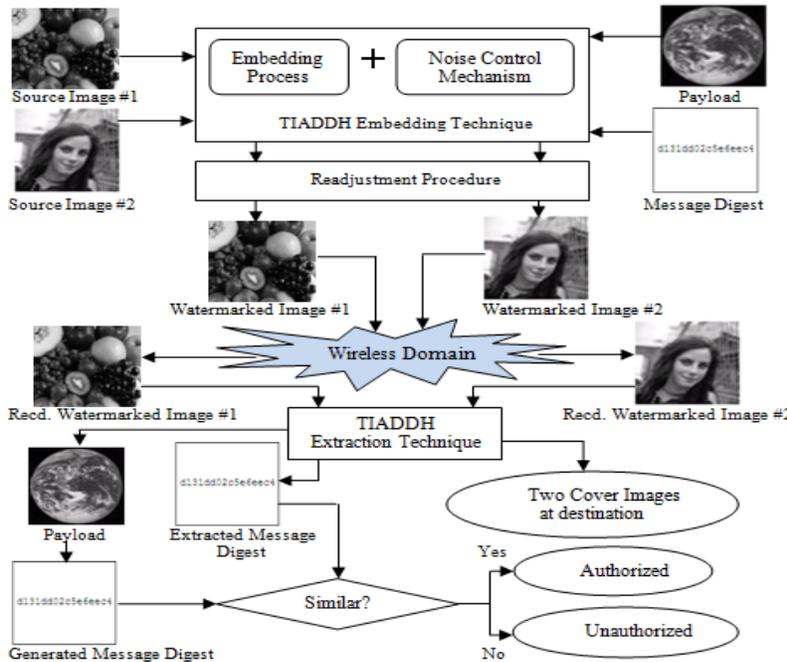


Figure 1. Illustration of Embedding and Extraction techniques using TIADDH

II. THE TECHNIQUE

We take 2x2 sized blocks, consisting of spatial values, alternatively from the two cover images. The spatial values are first converted to corresponding frequency values on application of DCT. Payload data bits are then fabricated in

the 2nd, 3rd and 4th frequency coefficients of each block at a pseudorandom bit position, ranging between 0 (LSB) and 3. The position is produced by a self devised method and is stored in a variable, ipos. Without altering the value of the fractional part, only the integer part of each frequency component is considered for embedding payload data and the generated message digest. On account of embedding, the noise

generated is reduced by making a minor re-adjustment on the modified frequency components.

In the process of extraction, selection of blocks and other related applications are implemented in the same method as mentioned above. Bits are retrieved from the 2nd, 3rd and 4th pixel of each sub image block and the location of extraction is decided by the same method as used earlier.

The sub-sections below, describe all the steps in detail.

A. Embedding Algorithm

Input: Two gray cover images and an authenticating gray message/image.

Output: Two gray images with the embedded authenticating data.

Steps:

1. Generate a message digest from the authenticating image.
2. Copy the header information of the cover images into the output images.
3. Access blocks of pixels (size 2 x 2) sequentially from the cover image (corresponding to two images alternatively) in row major order.
4. Repeat steps 4.1 to 4.7 until the header information, the message digest and all the pixels of authenticating message/image are embedded,
 - 4.1 Discrete Cosine Transform is applied on the current block of a source image.
 - 4.2 Generate a pseudorandom number (0 - 3) and store in ipos.
 - 4.3 Only the integer part of each frequency component is accessed to embed the authenticating message/image bits at the position earmarked by ipos.
 - 4.4 A readjustment procedure is applied to eliminate negative, fractional and greater than 255 spatial values (explained below).
 - 4.5 The noise evoked due to embedding is reduced by adjusting some of the modified frequency components.
 - 4.6 To revert the frequency values back into spatial domain, apply IDCT on the present block.
 - 4.7 The spatial block is written back into the output image in the same sequence as picked-up in step 3.
5. Stop.

Necessary Readjustments after embedding: The above embedding process may arouse erroneous results in some cases like:

1. Negative pixel values, which may get eliminated by subsequent increment of the DC coefficient of the current block.
2. Fractional spatial values sprout due to existence of 1/2 in the mathematical expression of DCT. The problem dies down after changing the value of the sum obtained at post-DCT operation to an even number.
3. The output pixel value may become greater than the maximum gray intensity (i.e. 255) which is

eliminated by adjusting the affected frequency components.

B. Extraction Algorithm

Input: Two gray watermarked images.

Output: An authenticating gray message/image.

Steps:

1. Access blocks of pixels (size 2 x 2) sequentially from the watermarked image (corresponding to two images alternatively) in row major order.
2. The header information, the embedded message digest and all the pixels of the output image are extracted from the input images by repeating steps 2.1 to 2.5,
 - 2.1 Discrete Cosine Transform is applied on the current block.
 - 2.2 Generate a pseudorandom number (0 - 3) and store in ipos.
 - 2.3 Consider the integer part of the frequency values to extract the embedded bit from the position specified by ipos.
 - 2.4 First, the header information and the embedded message digest are formed by combining the extracted bits. Later on bytes representing pixel intensity values of the authenticating image are formed sequentially.
3. A message digest is calculated on the extracted authenticating data.
4. Compare the extracted message digest with the calculated message digest to check the authenticity of the output image.
5. Stop.

C. Generation of ipos and Noise Control

To generate the pseudorandom value for ipos we implement the following steps.

Input: x and y (two dynamic variables having 8 bit integer values)

Output: A two bit integer value (0-3) in the variable ipos.

Step 1: $p = (x \text{ XOR } 03H) \text{ AND } y$

Step 2: $q = p \text{ AND } 03H$

Step 3: $r = p \text{ SHR } 6$

Step 4: $\text{ipos} = q \text{ XOR } r$.

Considering M as the mean value of the current block, the value of ipos is further modified as: if $(M > T)$ then $\text{ipos} = [0..3]$, else $\text{ipos} = [0..2]$, where T could be any value between 64 and 192.

The accrued noise in the embedding operation is minimized by modifying the unaffected bits of the stego image byte only if the original image byte and the resulting stego image byte differ. This is implemented by altering the bits on the right (i.e. towards LSB) and/or left (i.e. towards MSB) of the cover frequency component with respect to the value of ipos.

III. RESULT, COMPARISON AND ANALYSIS

The quality of each steganographic image received after implementing the proposed algorithm is scrutinized by various objective metrics namely, Mean Square Error (MSE) [8], Peak

Signal to Noise Ratio (PSNR) [8], Image Fidelity (IF) and Structural Similarity Index Metric (SSIM) [8].

Further the proposed technique is compared with other existing watermarking methods such as DCT-based [1, 12], QFT-based [6] and SCDFT-based [7, 9] on the basis of Peak Signal-to-Noise Ratio (PSNR).

A. Objective Image Comparison Metrics

- a. Mean Square Error (MSE): Computes an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal.
- b. Peak Signal To Noise Ratio (PSNR): The ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation.
- c. Image Fidelity (IF): A characteristic of an image that measures the perceived image degradation (typically, compared to an ideal or perfect image).
- d. Structural Similarity Index Metric (SSIM): This procedure is sensitive to distortions that disintegrate the natural spatial correlation of an image. It is expressed as a product of $l(f, g)$, $c(f, g)$ and $s(f, g)$, where $l(f, g)$ is luminance comparison function, $c(f, g)$ is contrast comparison function and $s(f, g)$ is structural comparison function. It is the best method to evaluate image quality till date.

The proposed algorithm has been tested on a substantial number of paired PGM images and it seems that the algorithm can survive almost all visual or statistical attacks. Figure 2 shows the visual interpretation of different images on execution of the proposed algorithm. Sample paired images like ‘Grapes & Kaya’, ‘Fruits & Sailboat’, ‘Splash & Tiffany’ and ‘Baboon & Airplane’ are shown in fig ia, iia, iiiia, iva, va, via, viia and viiia respectively. In our test the payload/authenticating image used is ‘Earth’ and is shown in fig. 2a. The stego images are shown in fig ib, iib, iiib, ivb, vb, vib, viib, and viiib respectively. Fig. ic, iic, iiic, ivc, vc, vic, viic and viiic shows magnified source images and fig. id, iid, iiid, ivd, vd, vid, viid and viiid shows magnified stego images respectively. The source and stego images exhibit no visual difference as scrutinized under Human Visual System (HVS).

Application of TIADDH on different pairs of gray images is shown in Table I in terms of data hiding capacity and the results of image quality metrics. Figure 3 and 4 pictorially shows the analysis of PSNR and SSIM values, resulted from the experimentation of the proposed algorithm on different pairs of images. Table II depicts scaling in terms of hiding capacity of secret data and PSNR in dB in the proposed scheme.

TIADDH is also compared with some existing techniques like Reversible Data Hiding Based on Block Median Preservation (RDHBBMP) [10] and A Steganographic Scheme for Color Image Authentication using Z-Transform (SSCIAZ) [11]. As compared with RDHBBMP (117314 bits) and with SSCIAZ (50208 bits) more data can be embedded with a hike of 1.45 dB and 1.31 dB in PSNR value signifying low rate of bit-error in our proposed scheme.

The comparative analysis in Table III shows better PSNR values with much more capacity of embedding than the existing techniques like DCT-based, QFT-based, SCDFT-based and CSSDCT watermarking schemes. Capacities in SCDFT, QFT, and DCT is 3840 bytes each, in CSSDCT it is 123301 bytes and PSNR values are 30.10 dB, 30.93 dB, 30.40 dB and 39.04 dB respectively but the capacity of TIADDH is 148518 bytes, which is fully recoverable and PSNR value is 50.37 dB.

Figure 2. Visual Interpretation of Source, Stego. & Payload Images using TIADDH

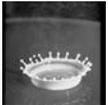
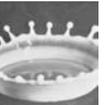
Source Images	Stego. Images using TIADDH	Magnified Source Images	Magnified Stego Images
 Fig.ia. Grapes	 Fig. ib .	 Fig. ic.	 Fig. id.
 Fig. iia. Kaya	 Fig iib.	 Fig. iic.	 Fig.iid.
 Fig.iiiia. Fruits	 Fig. iiib.	 Fig. iiic.	 Fig.iiid.
 Fig. iva. Sailboat	 Fig. ivb.	 Fig. ivc.	 Fig.ivd.
 Fig. va. Splash	 Fig. vb.	 Fig. vc	 Fig. vd
 Fig. via. Tiffany	 Fig. vib	 Fig. vic	 Fig. vid
 Fig. viia. Baboon	 Fig. viib	 Fig. viic	 Fig. viid
 Fig. viiia. Airplane	 Fig. viiib	 Fig. viiic	 Fig. viiid
 Fig. 2a. Earth (Payload)			

Table 1. Capacities and Metric values of images in TIADDH

Source Images	Embedded (bytes)	MSE	PSNR	IF	SSIM
Grapes Kaya	44100	1.468094	46.463264	0.999501	0.999729
		1.289150	47.027767	0.999288	0.999873
Fruits Sailboat	44100	0.955944	48.326477	0.999804	0.999762
		0.929020	48.450504	0.999169	0.999903
Splash Tiffany	44100	1.312355	46.950291	0.999722	0.999775
		1.314350	46.943691	0.999652	0.999002
Baboon Airplanr	44100	0.872101	48.725136	0.999616	0.999771
		1.487206	46.407093	0.998999	0.999683
Average	44100	1.203527	47.411777	0.999469	0.999687

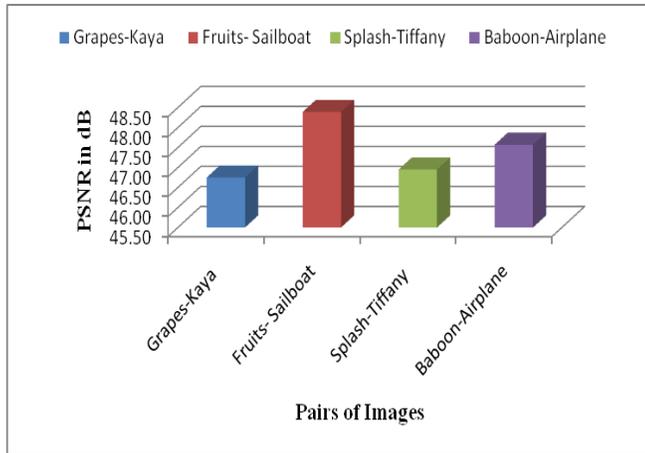


Figure 3. Analysis of PSNR values

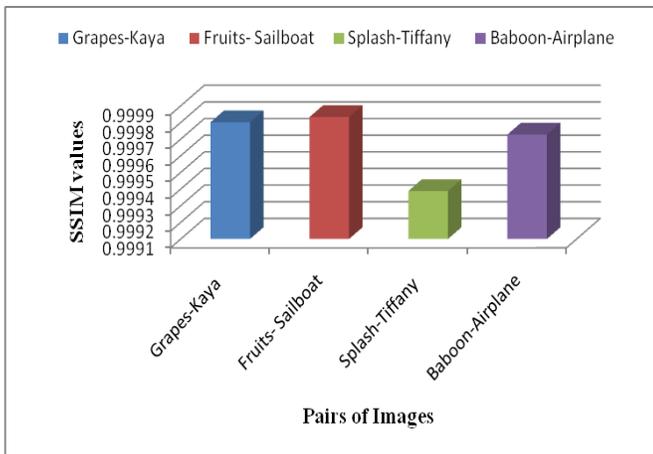


Figure 4. Analysis of SSIM values

Table 2. Comparison of PSNR in RDHBBMP, SSCIAZ & TIADDH

Test images	Indicator	EL=0	EL=0	EL=0
		RDHBBMP	SSCIAZ	TIADDH
Lenna	Embedded(bits)	26,465	64,896	90,000
	PSNR	49.68	49.89	50.42
Baboon	Embedded(bits)	36,221	64,896	90,000
	PSNR	49.80	49.87	51.97
Average	Embedded(bits)	31,343	64,896	90,000
	PSNR	49.74	49.88	51.19

Table 3. Comparison between TIADDH and DCT, QFT, SCDFT & CSSDCT

Technique	Capacity (bytes)	PSNR (dB)
SCDFT	3840	30.10
QFT	3840	30.93
DCT	3840	30.40
CSSDCT	123301	39.04
TIADDH	148518	50.37

The existing algorithms namely ATILD [22], IATDCT [23], ZIG-ZAG PVD [24] produces the value of MSE as 20.496414, 2.179449 and 1.8017 respectively whereas in TIADDH it is 1.203528. The computed value of Image Fidelity in algorithms namely S-Tools [25], ATILD, IATDCT and TIADDH are 0.990808, 0.999085, 0.999658 and 0.999469 respectively. The study of PSNR value in different algorithms shows that in ASIWT [21], EIDCT, CSSDCT, RDHBBMP, SSCIAZ, and TIADDH it is 31.35, 38.66, 39.04, 49.74, 49.88 and 51.19 respectively. Hence the comparative analysis of different several existing algorithms with the proposed algorithm in terms of MSE, IF and PSNR shows considerable improvement in results for TAIDDH, as represented pictorially in Figure 5, 6 and 7 respectively.

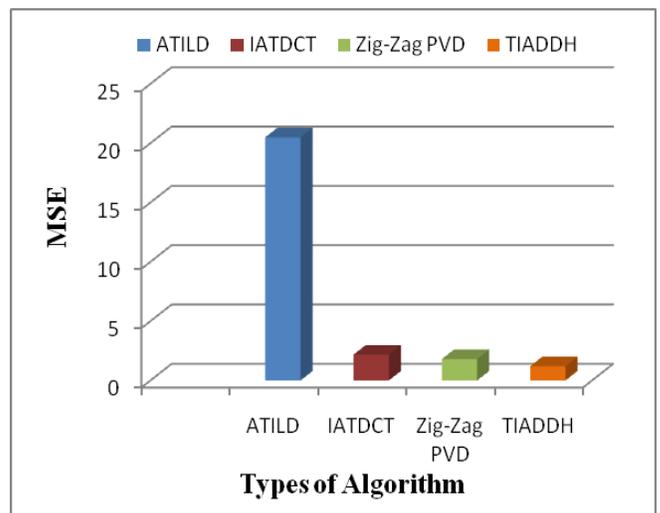


Figure 5. Comparative Study of Mean Square Error (MSE)

VI. REFERENCES

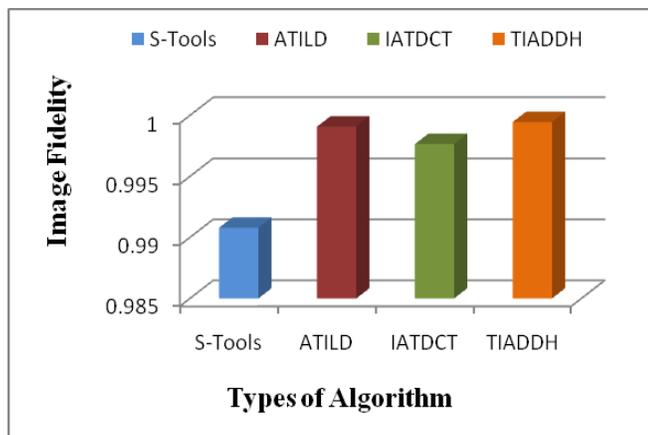


Figure 6. Comparative Study of Image Fidelity (IF)

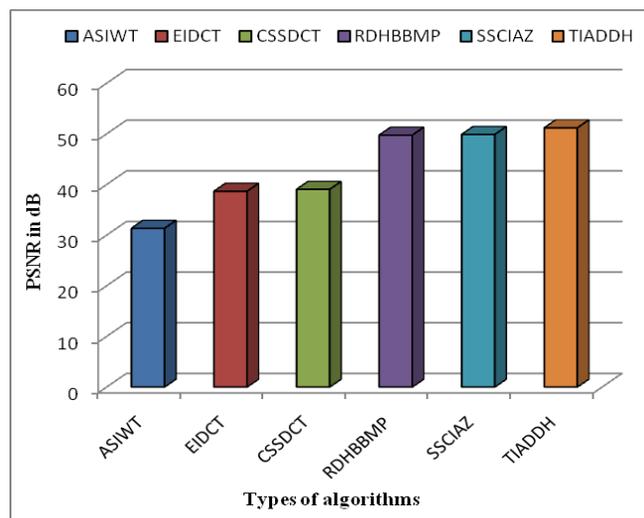


Figure 7. Comparative Study of PSNR values

IV. CONCLUSION

The technique of using two gray images for image steganography (TIADDH) has been proposed with the view of increasing the hiding capacity of secret data in addition to enhanced imperceptibility. Secrecy of authentic data is maintained meticulously by fabricating authenticating message/image bits at dynamically generated positions in the carrier image bytes. Extensive care has also been taken to eliminate visual suspicion which may arise due to noise accretion in the embedding phase. So, by analyzing the experimental results, it may be concluded that the proposed technique can shield the hidden data from potential hackers, more effectively.

V. ACKNOWLEDGMENT

The authors express their deep sense of gratitude to the faculty members of the Dept. of Engineering and Technological Studies, University of Kalyani, West Bengal, India, where the work has been carried out. The work has been financially supported by DST, PURSE.

- [1] N. Ahmadi, R. Safabakhsh, "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.
- [2] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", Proc. Inst. Elect. Eng., Vis. Images Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005.
- [3] 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.
- [4] 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.
- [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. Bas, N. L. Biham, and J. Chassery, "Color watermarking using Quaternion Fourier transformation", in Proc. ICASSP, Hong Kong, China, pp. 521-524, Jun. 2003.
- [7] T. T. Tsui, X. -P. Zhang, and D. Androutsos, "Color Image Watermarking Using Multidimensional Fourier Transformation", IEEE Trans. on Info. Forensics and Security, vol. 3, no. 1, pp. 16-28, 2008.
- [8] C.Sasi Varnan, A.Jagan, Jaspreet Kaur, Divya Jyoti, Dr.D.S.Rao, "Image Quality Assessment Techniques on Spatial Domain", International Journal of Computer Science and Technology, IJCST Vol. 2, Issue 3, September 2011, ISSN : 2229-4333(Print), ISSN : 0976-8491(Online).
- [9] Ghoshal, N. and Mandal J. K., "Discrete Fourier Transform based Multimedia Colour Image Authentication for Wireless Communication (DFTMCIAWC)", 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Wireless Vitae 2011, ISBN: 978-1-4577-0787-2/11, Chennai, India, 2011.
- [10] 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.308-3.
- [11] Nabin Ghoshal, Soumit Chowdhury, J. K Mandal, "A Steganographic Scheme for Color Image Authentication using Z-Transform (SSCIAZ)", Advances in Intelligent & Soft Computing, vis INDIA-2012, pp 209-216, 2012, 10.1007/978-3-642-27443-5_24, ISBN 978-3-642-27442-8 ISSN:1867-5662, 2012.
- [12] K.B.Shiva Kumar, K.B.Raja, R.K.Chhotaray, Sabyasachi Pattnaik, "Coherent Steganography using Segmentation and DCT", IEEE International Conference on Computational Intelligence and Computing Research (ICIC), 2010, E-ISBN: 978-1-4244-5967-4, Print ISBN: 978-1-4244-5965-0, Coimbatore.

- [13] Dr. Ekta Walia a, Payal Jainb, Navdeep, “ An Analysis of LSB & DCT based Steganography”, P a g e | 4 Vol. 10 Issue 1 (Ver 1.0), April 2010 Global Journal of Computer Science and Technology,GJCST Computing Classification F.2.1 & G.2.m).
- [14] Rufeng Chu, Xinggang You, Xiangwei Kong, Xiaohui Ba , “A DCT-based Image Steganographic Method Resisting Statistical Attacks”, 0-7803-8484-9/04/\$20.00 ©2004 IEEE , V - 953 , ICASSP2004).
- [15] A Nag, S Biswas, D Sarkar, P P Sarkar ,”A novel technique for image steganography based on block DCT and Huffman Coding”, Journal of Computer Science and Information Technology (2010) ,Volume: 2, Issue: 3, Pages:10 ,DOI: 10.5121/ijcsit.2010.2308).
- [16] Thekra Abbas, Zou Beiji, Maan Younus Abdullah “Information Security Technique in Frequency Domain” , ,International Journal of Digital Content Technology and its Applications(JDCTA)Volume5,Number12,December2011,,doi:10.4156/jdcta.vol5.issue12.35).
- [17] N Sathisha, K Suresh Babu, K B Rsja, Venugopal K R, L M Patnaik,“Embedding Information in DCT Coefficients based on Aerge Covariance”, International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. 4 April 2011).
- [18] Saad M. A. AL-MOMEN, Loay E. GEORGE, ”Image Hiding Using Magnitude Modulation on the DCT Coefficients”, Journal of Applied Computer Science & Mathematics, no. 8 (4) /2010, Suceav).
- [19] Ghoshal N., Mandal, J. K. “A Novel Technique for Authentication of Image/Hiding Large Volume of Data (AI/HLVD)”, Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), International journal of Signal Processing and Pattern Recognition, ISSN 1240-4543, Vol. 53, No. 2, pp. 1-13, France, 2009.
- [20] C. Rechberger, V. Rijman and N. Sklavos, “The NIST cryptographic Workshop on Hash Functions”, IEEE Security & Privacy, vol. 4, Austria, Jan-Feb 2006, pp. 54-56.
- [21] R. O. El Safy, H. H. Zayed and A. El Dessouki, “An Adaptive Steganographic Technique Based on Integer Wavelet Transform,” IEEE Proceedings on International Conference on Networks and Media, pp. 111 – 117, March 2009.
- [22] Nabin Ghoshal, J. K. Mandal and A. Khamrui. “A Novel Authentication Technique for Image/Legal Document (ATILD)”, International Journal of Signal Processing Systems, ISSN (Print) 1939-8018, ISSN (Online) 1939-8115, J Sign Process Syst (2012) pp. 67:187–199 DOI 10.1007/s11265-010-0557-7 Springer Verlag.
- [23] Nabin Ghoshal, Anirban Goswami, Jyotsna Kumar Mondal and Dipankar Pal, “Image Authentication Technique Based on DCT (IATDCT)”, in Proc. Advances in Intelligent and Soft Computing, 2012, Volume 167/2012, pp. 863-871, DOI:10.1007/978-3-642-30111-7_83.
- [24] M.Padmaa, Dr.Y.Venkataramani, “ZIG-ZAG PVD – A Nontraditional Approach”, International Journal of Computer Applications (0975 – 8887), Volume 5– No.7, August 2010.
- [25] S-Tools:<http://digitalforensics.Champlain.Edu/download/stools4.zip>