A Robust Source Coding Watermark Technique Based on Magnitude DFT Decomposition

S. K. Muttoo[1] and **Sushil Kumar**[2]

Submitted in April 2012; Accepted in July 2012

Abstract – ***Image watermarking is considered a powerful tool for Copyright protection, Content authentication, Fingerprinting and for protecting intellectual property. We present in this paper a watermarking algorithm based on block wise changing magnitude of DFT domain. This algorithm can be used as an application for copyright protection. To provide multi-level securities we have first used best self-synchronizing T-codes to encode the watermark. The encoded watermark is then embedded into the cover image using a stego-key. We have analyzed our algorithm against noise such as Salt and Pepper, Gaussian and Speckle.***

Index Terms – Watermark, DFT Composition, Image Processing

1. INTRODUCTION

Watermarking is a branch of information hiding that talks about data embedding in the inconspicuous files or cover objects such as images, video, audio, graphics, texts or packet transmission in a perceptually transparent manner. Digital watermarking is an attempt to solve the growing concerns about proof of ownership, content authentication, copyright violation, tamper proofing, illegal copying and distribution and issues such as fake currency. The basic attributes of watermarking techniques are *Robustness, Security and Undetectability.*

There are three common steps of watermarking techniques viz.,

1. Design of watermark,
2. Watermark embedding and
3. Watermark extraction.

There are various domains of information hiding viz., *spatial domain*, t*ransform domain and spread spectrum domain*. The simplest spatial domain method of watermark embedding is changing the least significant bits (LSB's) of the cover image, but it is not robust to addition of noise or lossy compression. Since the degradation in smoother regions of an image is more noticeable to the human visual system (HVS), it is preferable to hide watermark in noisy regions and edges of images. The transform domain based hiding techniques has not only the potential to achieve higher capacity than the spatial domain based techniques, they are also found to be more robust. Therefore, methods based on transform domain have got more attention than the spatial domain. One can embed watermark by changing the LSB's in the block based transform domain or in the global transform domain. A watermark embedding operation can be carried out in a transform domain, such as *Discrete Fourier Transform* (DFT), *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT), *Singular Value Decomposition* (SVD) *Transform, Karhunen-Loeve Transform (*KLT*)* and *discrete Hadamard Transform* (DHT).

This paper is about information hiding in still images. Most of the research on watermarking is focused on images. Apart from text, images have been used widely as cover objects for the purpose of information hiding as their digital representation provide high degree of redundancy. These techniques are independent of an image formats and hide data in more significant areas of the transformed image. The details of such different watermarking techniques can be found in [3, 4, 12, 15, 17, 19, 20, and 21].

M. Barni et al [7] and R. Dugad [8] have shown DCT or DWT domain semi-blind watermarking schemes to be robust against a number of attacks. However, their method resulting in a weaker detection when a geometric attack (e.g., rotation, translation, and scaling) is tried due to the change in the location of the transform coefficients. Therefore, some researchers [2], [9], [11] have emphasized on DFT-based watermarking because of the properties of the DFT. The DFT of an image is generally complex valued and this leads to a magnitude and phase representation for the image. Most of the information about any typical image is contained in the phase and the DFT magnitude coefficients convey very little information about the image. Thus one would expect that good image compression techniques would give much higher importance to preserving the DFT phase than the DFT magnitude.

Ridzon R and Levicky D [16] have discussed the robust watermarking techniques and proposed one robust digital image watermarking technique based on the discrete Fourier transform and log-polar mapping.

V. Solachidis and I.Pitas [18] have presented an algorithm for rotation and scale invariant water -marking of digital images. An invisiblemark is embedded in magnitude of the DFT domain. The algorithm is shown to be robust to compression, filtering, cropping, translation and rotation.

M. Ramkumar et al [13] have observed that all major compression schemes such as JPEG, SPIHT and MPEG preserve the DFT magnitude coefficients as well as preserve the DFT phase. The other advantage for using the DFT

[1]*Department of Computer Science, University of Delhi, Delhi, India*
[2]*Rajdhani College, University of Delhi, New Delhi, India*
E-mail: [1]*skmuttoo@cs.du.ac.in and* [2]*azadsk2000@yahoo.co.in*

magnitude domain for watermarking is lying in its property of translation- or shift-invariance. A cyclic translation of an image in the spatial domain does not affect the DFT magnitude, and because of that, watermark embedding in the DFT magnitude domain remains translation-invariant.

Farid Ahmad [1] has proposed a dual Fourier-Wavelet domain watermarking technique for authentication and identity verification. He has embedded a robust signature and hidden it in a mid-band wavelet subband using Fourier domain bit-embedding algorithm. His method shows the compression tolerance.

In this paper, we present a watermarking algorithm based on DFT magnitude domain using a self-synchronized variable length codes, viz., T-codes for embedding the watermark. In section 2 we explain the proposed algorithm. The experimental results of the algorithm are present in section 3. In section 4, we conclude and give the suggestion on the future scope of this paper.

2. THE PROPOSED WATERMARKING TECHNIQUE

We propose a watermarking technique of block wise changing magnitude of DFT coefficients. The cover image is divided into 8x8 or 16x16 blocks and one bit of secret message (watermark) is embedded into each randomly selected DFT blocks. The maximum payload (capacity) of watermark is equal to the number of blocks constructed in the cover image. Moreover, the watermark (i.e., the hiding message) is imperceptible. The purpose of using Best T-codes in the embedding process has two-fold advantages. First is that we can have better embedding capacity and second is the inherent self-synchronizing property of T-codes. Ulrich [6] has shown that T-codes show the best synchronization performance amongst the most efficient variable length codes and require anything between 1.5 to 3 characters to attain synchronization following a lock loss. Further, A.C.M. Fong et al [5] have shown that T-codes provide better performance for robustness against most common signal distortions. S.K.Muttoo and Sushil Kumar [10] have shown that T-codes give better results of imperceptibility (in PSNR) when they replace Huffman codes in the steganographic methods (jpeg-jsteg/Outguess). The steps of the embedding method are described in the figure 2.1.

The Embedding algorithm is summarized as follows:

……

0. *Input the Cover image and watermark (i.e., text)*
1. *Divide the cover image into 16x16 (or 8x8) blocks and apply DFT to each block*
2. *Enter watermark (i.e., text or message)*
3. *Obtain the secret message, m, by encrypting the original message using best T-codes*
4. *Let n = size (secret message) and nb= total number of blocks.*
5. *Use PRNG to obtain a permutation of 'nb'- random numbers, say r_i*
6. *While (n <= nb) do*
   For i= 1 to n do
   6.1 Select the random DFT block r_i
   6.2 Embed m_i secret message bit into r_i as follows:
   If m_i = '1'
   Change the block r_i's magnitude by some amount such that
   It should be perceptible
   Else
   'r_i remains unchanged'
7. *Output: Watermarked image.*

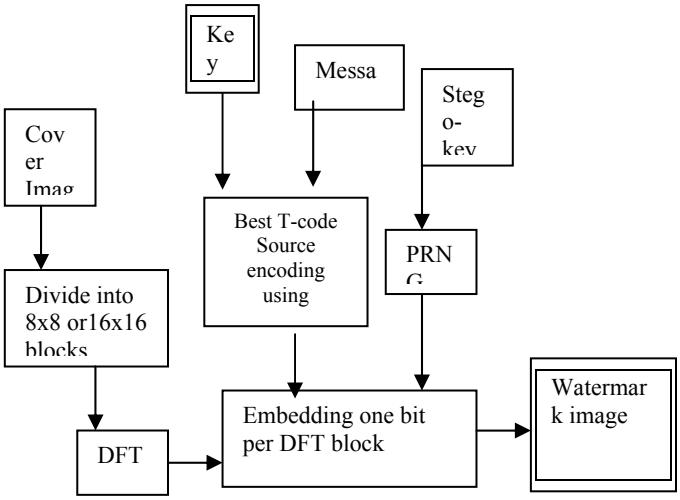

Figure 2.1: "The block diagram for watermark embedding process"

For extracting watermark, we compare each DFT block's magnitude of watermark image with DFT block's magnitude of original image. If they come out to be same, then bit embedded is '0' otherwise it is '1'. The original message is then obtained by decrypting the extracting message using best T-codes. The extraction process is shown in the figure 2.2.

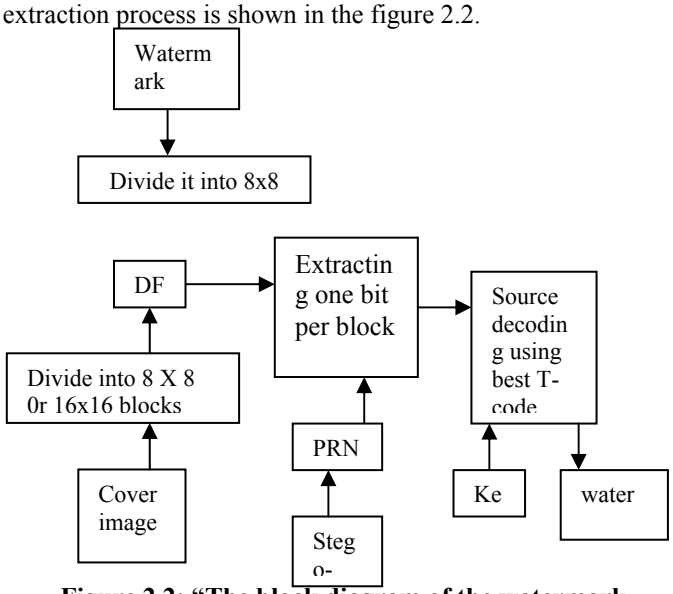

Figure 2.2: "The block diagram of the watermark extraction process"

3. EXPERIMENTAL RESULTS

We have implemented our algorithm on Matlab 7.0 on the 'png' and 'tif' images. The issues of imperceptibly, robustness and security are analyzed.

3.1 Imperceptibility

For imperceptibility, we used the PSNR as a measure of perceptibility. The summary of some of the results obtained are shown in the table 3.1

Length of Secret Message, n	MSE	PSNR Secret message, n
28	0.1657	55.937305
74	0.4971	51.165959
1047	0.8614	48.779914
470	3.1162	43.194567
937	6.1120	40.388943
1023	7.4837	39.389613

[1] $PSNR = 10 \log_{10} (255^2 / MSE)$

$MSE=(1/N)^2 \sum\sum (x_{ij} - x'_{ij})^2$

where x denotes the original pixel value

Table 3.1: "Image: 'lena.png';
Size of image: 512 x 512 x 3"

3.2 Robustness

We have analyzed our technique against Salt & Pepper, Gaussian and Speckle noise. Some of the results are summarized in table 3.2.

Noise	**Noise density/ Variance**	**PSNR**	**imperceptibility**
Salt and Pepper	0.001	33.680459	YES
	0.005	27.354359	Acceptable
	0.01	24.508046	NO
Gussain	0.0001	36.679711	YES
	0.0005	32.201980	YES
	0.01	29.686735	NO
Speckle	0.001	31.795482	YES
	0.01	22.971299	NO

Table 3.2: "Image: 'lena.png' ; n= 1023 ;
PSNR(without noise)=39.423371"

4. CONCLUSION AND FUTURE SCOPE

The algorithm proposed in this paper makes use of DFT magnitude domain for watermark embedding. Watermark can be embedded of capacity equal to the number of blocks created of cover image. Thus, one can have better embedding capacity. From the experimental results as shown above, we observe that the method is robust against adding noise such as Salt and Pepper, Gaussian and Speckle to the extent the image remains imperceptible.

Our extraction algorithms need the original cover image to reveal the hidden text from stego_image, i.e., our scheme is '*cover escrow scheme'*. The other scheme known as '*blind scheme' that* does not require the original cover image to detect the hidden message. It is observed that traditional block transform coding of images may generate artifacts near block boundaries that degrade low bit rate coded images. The Wavelet transforms in the frequency domain techniques have been used because they make the process of imperceptible embedding more effective. Wavelet transform produces much less blocking artifacts than the DCT and they also perform well in image de-noising. Wavelets are found to be well adapted to point singularities but they have a problem with orientation selectivity. They are not efficient in representing the contours not horizontally or vertically. To eliminate the blocking effect new transforms such as *ConTourletstransform* (CTT) and *Lapped transforms* (LOT) have been investigated in the past. These transforms have not yet been explored fully in information hiding. A combination CTT-DWT is suggested to be a good candidate for new compression codec in the literature.

ACKNOWLEDGEMENT

The authors wish to thank Elham Moinaddini and Shweta Chaudhary for their help in the Matlab implementation.

REFERENCES

[1]. Farid Ahmad: A dual Fourier-wavelet domain authentication-identification watermark, Optics Express, Vol. 15, Issue 8, pp. 4804-4813, 2007

[2]. R. Caldelli, M. Barni, F. Bartolini, A. Piva: Geometric-Invariant Robust Watermarking throughConstellation Matching in the Frequency Domain, Proceedings of the 2000 International Conference on Image Processing (ICIP 2000), Vancouver, BC, Canada, Vol. II, Vancouver,Canada, September 10-13, pp. 65-68, September 10-13, 2000.

[3]. Chris Shoemaker: Hidden Bits: A Survey of Techniques for Digital Watermarking,2002

[4]. Edin Muharemagic and Borko Furht: Survey of Watermartking Techniques and Application, In: Borko Furht and Darko Kirovski, Multimedia watermarking Techniques and Application, Auerbach Publicatin, 452, pp. 91-130, 2006

[5]. Fong A.C.M., Higgie G.R., Fong B: Multimedia Application of Self-Synchronizing T-codes, Proc. IEEE Int. Conf. On IT: Coding and Computing, April 2001, pp.519-523.

[6]. Gunther Ulrich: Robust Source Coding with Generalised T-codes, a thesis submitted in the University of Auckland, 1998
[7]. M. Barni, F. Bartolini, V. Cappellini, and A. Piva: DCT-Domain System for Robust ImageWatermarking, Signal Processing, Special Issue on Copyright Protection and Control, 66(3), pp.357-372, 1998.
[8]. R. Dugad, K. Ratakonda, and N. Ahuja: A New Wavelet-Based Scheme for Watermarking Images, Proceedings of 1998 International Conference on Image Processing (ICIP 1998) , Vol. 2, Chicago, IL,October 4-7, pp. 419-423, 1998
[9]. C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, Y. M. Lui: Rotation, Scale, and TranslationResilient Watermarking for Images, IEEE Transactions on Image Processing , 10(5), May 2001.
[10]. Muttoo S.K. and Sushil Kumar: Image steganography using self-synchronizing variable codes, International conference on Quality, Reliability and Infocom technology, ICQRIT-06, Macmillan India ltd., 2007
[11]. S. Pereira and T. Pun: Robust Template Matching for Affine Resistant Image Watermarks,
[12]. IEEE Transactions on Image Processing, 9(6), pp. 1123-1129, June 2000
[13]. Peter Meerwald: Digital Image Watermarking in the Wavelet Trasform Domain,Diploma thesis,University of Salzberg, January 2001.
[14]. Muttoo S.K. and Sushil Kumar, "Data hiding in JPEG images", BVICAM's International Journal of Information Technology, BIJIT, Vol. 1, No. 1, Jan. – July, 2009.
[15]. Muttoo S.K. and Sushil Kumar, "Robust Source coding Steganographic technique using Wavelet Transforms", BVICAM's International Journal of Information Technology, BIJIT, Vol. 1, No. 2, July – December, 2009.
[16]. Ramkumar M., Akansu A.N. and Alatan A.A.: A Robust Data Hiding Scheme for images using DFT, Proceeding of International Conference on Image Processing,1999, vol. 2, 211-215
[17]. Ridzon, R, Levicky,D: Robust digital watermarking in DFT and LPM domain, 50th International Symposium, ELMAR, 2008
[20]. Salomon David: Data Compression, Springer-Verlag, N.Y., second edition, 2000.
[21]. V. Solachidis and I.Pitas: Circularly Symmetric Watermark Embedding in 2-D DFT Domain, Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Vol. 6, Phoenix, AZ, March 15-19, pp. 3469-3472, 1999
[22]. Stefan Katzenbeisser, Fabien A.P. Petitcolas: Information Hiding Techniques for Steganography and Digital Watermarking, Artech House,Inc, 2000
[23]. Ton Kalkar: Basics of Watermarking, Stanford, February 2004.

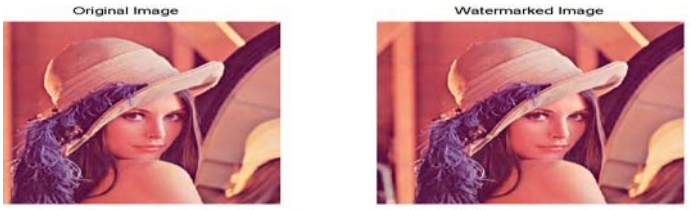

Figure 3.1: "The original and watermarked image of 'lena.png' for n=1023"

The images with the added noise as given in the table are shown in figure 3.2.

spll8.png

8ns5.png

Figure 3.2: "The above images (noise density) are as follows"
Salt and Pepper: spf.png (0.001), spp8.png (0.005), spll.png (0.01);
Gaussian : gf8.png (0.0001), gg8.png (0.0005), gll8.png(0.001)
Speckle : 8su1.png (0.001), 8ns5.png (0.01))

Continued from page no. 479

[7]. Dutta Avijit; An Emerging Perspective of ICT Assisted Knowledge Production, INDIACom – 2008, Page; 127-132.
[8]. Dutta Avijit; Collaborative Knowledge with Cloud Computing, Proceedings of the 4th National Conference, INDIACom – 2010.
[9]. Derek H C et al; The Knowledge Economy, the KAM Methodology and World Bank Operations; The World Bank Washington DC 20433, October 19 2005.
[10]. Economic Intelligence Unit, 2001, 2002, 2003, 2004, 2005,2006,2007,2008 E-Readiness Ranking, White Paper.
[11]. Measuring Knowledge In The World Economies World Bank, Knowledge For Development (K4D) Program.
[12]. Eric Knorr, Galen Gruman; What cloud computing really means; InfoWorld, April 07,2008, http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031.
[13]. Hans-Jorg Happel, Andreas Schmidt, Knowledge Maturing as a process model for describing software.
[14]. Hendriks P (1999) Why share knowledge? The influence of ICT on the motivation for knowledge sharing. Knowledge and Process Management 6(2), 91-100.
[15]. IBM'S Perspective on the state of Information Technology; Autonomic Computing http://www.research.ibm.com/autonomic/overview/.
[16]. ITU, Measuring the Information Society, 2010.
[17]. ITU, Measuring the Information Society, 2011.
[18]. Maria R. Lee, From Web 2.0 to Conversational Knowledge Management: Towards Collaborative Intelligence; Journal of Entrepreneurship Research, June 2007, Vol.2, No.2,P.47-62.
[19]. Peter Gloor, Deloitte Consulting- Collaborative knowledge Networks.
[20]. Prusak L, Where did Knowledge Management Come from? IBM SYSTEMS JOURNAL, VOL 40, NO 4, 2001.
[21]. Rajiv, Manohar Lal "Web 3.0 in Education & Research", BIJIT Issue 6: (July-December, 2011 Vol.3 No.2)
[22]. http://en.wikipedia.org/wiki/History_of_the_Internet.
[23]. http://en.wikipedia.org/wiki/Donald_Davies.
[24]. http://www.webopedia.com/DidYouKnow/Hardware_Software/2002/FiveGenerations.asp.
[25]. http://en.wikipedia.org/wiki/Enterprise_2.0.
[26]. http://learnsumthingnew.weebly.com/assessment-2.html
[27]. http://www.crisscrossed.net/2007/06/10/what-isenterprise20-five-pillars-for-efficient-knowledge-sharing/.
[28]. http://www.cc.gatech.edu/current/doctoral/phdcs-qualifier/hci/ubicomp.
[29]. http://sandbox.xerox.com/want/papers/ubi-sciam-sep 91 .pdf.