VOL. 12, NO. 11, JUNE 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A CRT BASED ROBUST IMAGE WATERMARKING USING DISCRETE TCHEBICHEF TRANSFORM

J. L. Divya Shivani and Ranjan K. Senapati
Department of Electronics and Communication, K. L. University, A. P., India
E-Mail: shivanidivya18@gmail.com

ABSTRACT

This paper presents a Chinese Remainder Theorem (CRT) based digital watermarking technique in Discrete T-Chebyshef Transform (DTT) domain which is robust to several common attacks. The proposed technique is compared with the recently proposed CRT based Discrete Cosine Transform (DCT) domain technique. Extensive simulation experiments show the better robustness to the common image manipulations such as brightening, sharpening, cropping, noise and compression. At the same time, the proposed technique successfully makes the watermark perceptually invisible. Better Tamper Assessment Function (TAF) value of 30-40% is achieved in comparison to 30-40% in DCT and 10-40% on Singular Value Decomposition (SVD) techniques. Similar to DCT domain watermarking, it is possible to maintain the imperceptibility and low TAF for various values by doubling the capacity of the watermark.

Keywords: Chinese remainder theorem, discrete cosine transform, discrete tchebichef transform, imperceptibility, tamper assessment factor.

1. INTRODUCTION

With the rapid growth i**n** technology and internet applications it made easy access for every user to download multimedia data like images, videos etc. through the internet, whereas this data can easily be tampered or manipulated, for which data integrity must be ensured. Digital watermarking is used to verify integrity. There are many techniques in watermarking owing to the characteristics, imperceptibility, inseparability from the cover content and its inherent ability to undergo the same transformations as experienced by the cover content. Among the techniques, this is efficient only if the watermark is imperceptible, secure and robust.

Digital watermarking techniques are performed in the spatial domain [1] [2] and in transform domain [1] [3]. Transformed domain is more robust and provides more imperceptibility than spatial domain [5]. In transform domain DCT make use of energy distribution properties and human visual system scheme for embedding watermark. Blind watermarking scheme [5] [6] with interesting results have been proposed. Some of the other transformed-domain watermarking schemes have been proposed in SVD is also used in watermarking (where the properties of U coefficients [10] [12] modification cause less degradation of image quality. Some of the watermarking techniques using Ridgelet transform also proposed.

CRT based scheme which provides robustness against some common image processing manipulations are proposed. Digital watermarking is also performed using segmentation of DCT blocks. Each DC coefficients is extracted and stored in a matrix before processing making it expensive in terms of memory requirement, techniques were developed to use middle DCT coefficient for embedding watermark. The algorithm is not much robust against JPEG compression.

Watermarking schemes can be implemented in VLSI chips. Hardware implementation in consumer electronic devices such as digital camera, PDAs, and mobile devices requires low power, high reliability, real-time performance and easy integration. For example, viability of integration of watermarking chips in any digital camera/JPEG codec. Several issues related to hardware implementation of several watermarking algorithms for images and videos [8] [9].

DCT domain watermarking is popular for hardware implementation because there are a number of fast algorithms [5] [6]. 8x8 DCT is mostly used for hardware implementation. 4x4 DCT provides less computation at a cost of less energy compaction.

Discrete Tchebichef Transform (DTT) is a new transform and has relatively similar properties with DCT. The properties include (i) Energy compaction, (ii) Seperability and Symmetry, and (iii) Orthogonal. There are many works related to compression. DTT can be used in applications such as feature extraction, pattern recognition, blind integrity verification, and artifact measurement. However, to the best of our knowledge no such work in Security applications have been reported in the literature. This paper presents a novel robust image watermarking scheme in DTT domain. The scheme uses CRT for its robustness. As the polynomials of DTT matches closely with HVS, the scheme provides higher perceptual quality than DCT based watermarking scheme. The proposed methodexhibit superiority in terms of SSIM and TAF over most of the schemes. Good TAF values are also obtained in case of most of the common attacks such as cropping, tampering, noise addition, brightening, sharpening and compression. Attacks such as scaling, rotation, filtering and geometric transformation are not considered in this paper.

The rest of the paper is as follows: Section 2 discusses the implementation of embedding and extraction aspect of the proposed scheme. Comparison results are presented in Section 3. Finally, in Section 4 conclusion and future research direction have been made.

2. PROPOSED SCHEME

The block diagram of the proposed scheme is shown in Figure-1. The uniqueness of the scheme is that the 'key' is generated randomly during embedding process instead of using a known key for embedding compared to other methods. Along with watermarked image, the key will be send to the receiver.

The embedding and extraction technique of the proposed method is based on the combining CRT technique in the DTT domain. This method produces the better security, the better robustness and also needs the simple operation during extraction phase.

2.1 Embedding procedure

The following steps describe the watermark embedding procedure on the host image.

Step-1. Partition of blocks

The host image is taken as a gray scale image and watermark is a binary image. Initially, the host image is divided into blocks of 8 ×8pixels. The single watermark bit is then embedded in a single block selected. Then the blocks are chosen as random.

Step-2. Selection of DTT coefficients

In order to improve robustness, the preferred choice is to embed the watermark into the most significant coefficients. However, it will degrade the quality of the watermark. If insignificant coefficients are used for embedding, the watermark may have lost during lossy compression [8] [9]. Since proposed scheme use block size 8×8 pixels, resulting DTT block is also of same size. This gives a total of 64 DTT coefficients.

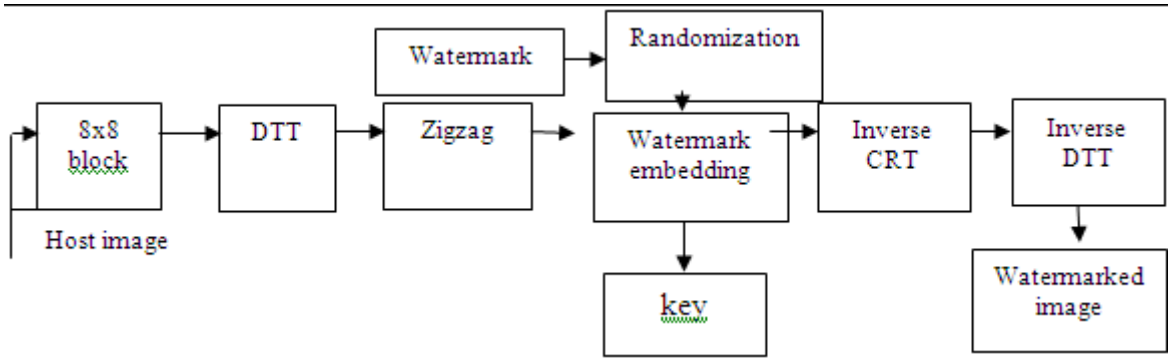

Figure-1. Block diagram of watermark embedding process.

We have included both DC and low frequency AC coefficients for embeddingin order to achieve trade-off between quality and robustness. The DC component and the first 60 low frequency AC components are selected as the possible locations for embedding the watermark bits in the DTT domain.

Step-3. Randomization

After zig-zagging the DTT coefficients, one value must be selected. During that selection randomizing the coefficients is done using Arnold Transform instead of using the regular selection procedure. Using randomization technique, security and authentication are more as the value is changing for every execution. During randomization, one of the selected coefficients is chosen and it is stored as a secret key whenever we execute the code. This feature adds more security to the data while embedding and extraction procedure.

Step-4. Embedding the watermark bits

After dividing 8×8 blocks, one watermark bit gets embedded in each of the block. Considering one block at a time, the procedure for embedding the watermark bits is listed as follows:

a) Randomly selectan 8×8 block from host image and apply DTT to the block.

b) Randomly select a watermark bit from the watermark image in order to embed into the block.

c) Randomly select a DTT coefficient (DC or one of the AC components) to embed the watermark bit. Let its value be denoted as *X*.

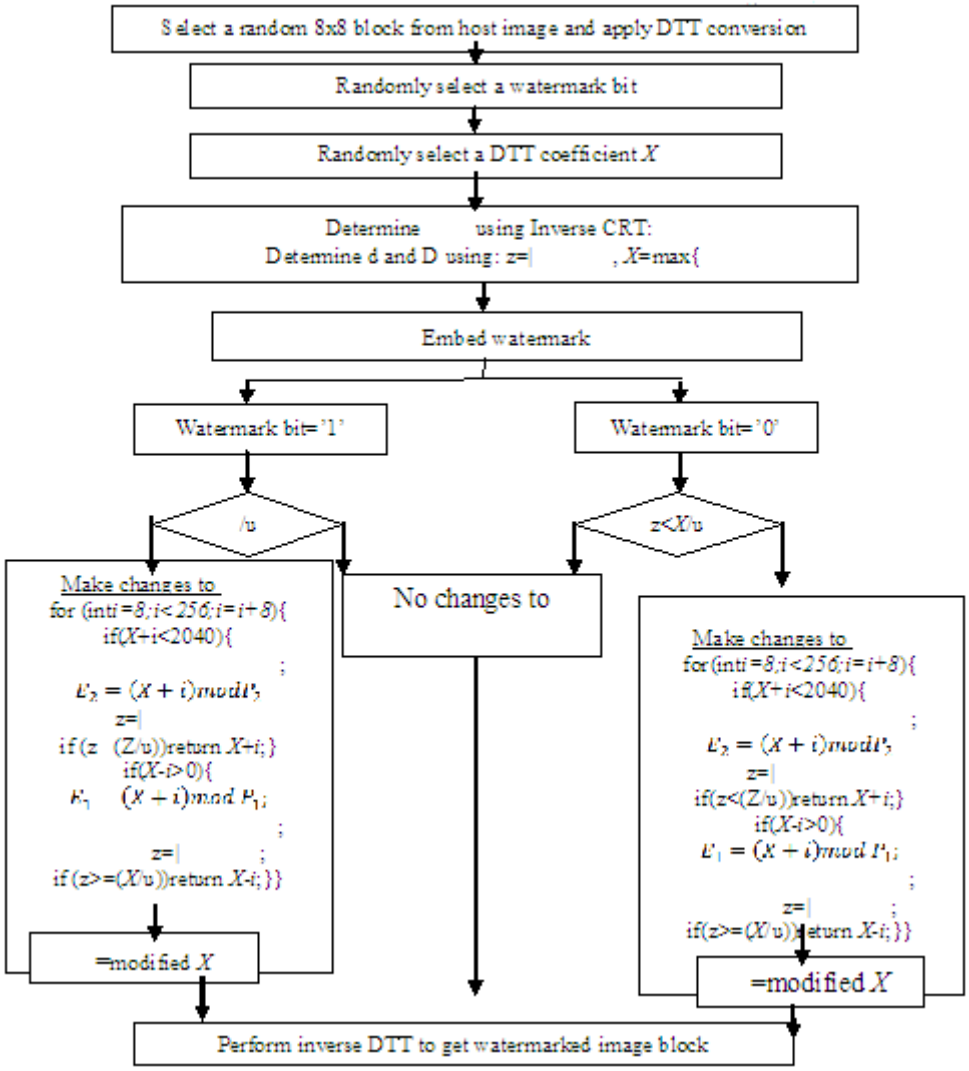

Figure-2. Flow chat for embedding watermark bit.

d) Let *P*1 and *P*2 be the pair-wise co-prime numbers used in CRT (say, P1=38 and P2=107) for the DC coefficient. For an AC coefficient, let the values of *P*1=38 and *P*2=55.

e) Find *E*1 and *E*2 by applying the inverse CRT to *X*.

f) Determinethe values of 'z' and '*X*'.

g) The required condition for embedding watermark bit '1', isz ≥ *X*/u (1) where u= 2 if *X* is DC coefficient, otherwise, u= 4. If condition is not satisfied, then *X* is modified to $\hat{X}$until the required condition in (1) is satisfied.

h) The required condition for embedding watermark bit '0' is z <*X*/u (2) If the condition in (2) is not satisfied, then *X* is modified to $\hat{X}$until the required condition is satisfied. The process of the embedding bit '0' and the bit'1' is illustrated in the Flow Chart Figure-3.

i). Reconstruct DTT block with the modified DTT coefficient, $\hat{X}$ and apply inverse DTT to the block to construct the watermarked image block.

j). Repeat the steps 1-9 for all the remaining blocks until all the watermark bits got embedded.

Note that the range of possible values for DC and the AC coefficients are not the same. The range of the DC coefficient is from values 0 to 2040 and for AC coefficients; it will be from the -1020 to +1020 in monochrome images. According to CRT, the product of the pair-wise co-prime numbers (also called the dynamic range) must be greater than the largest possible number (Patra *et al.*, 2010).

The flow chart for embedding procedure is shown in Figure-2.

2.2 Extraction procedure

The procedure of extraction is that reverse of embedding procedure. Figure-3 shows the extraction process. For this, following information must be known to get watermark extracted from watermarked image: (i) Image which is watermarked, (ii) Size of watermark. (iii)Watermark Key, and (iv) A pair-wise numbers of co-prime P1 and P2.

With knowledge of the watermark key, the DTT coefficient that is embedded with watermark information *X* is extracted. Thus, with values of P1, P2 and *X*, the E1,

E2 are determined. Next, comparison is made between the z and *X*. If z = *X*/u, the bit '1' would be get extracted, otherwise the bit '0' would be get extracted. The scale factor, u is then set to 2 for the coefficient of DC otherwise it is get set to 4. Thus the above steps were then repeated until every block consecutively to get all watermark bits extracted.

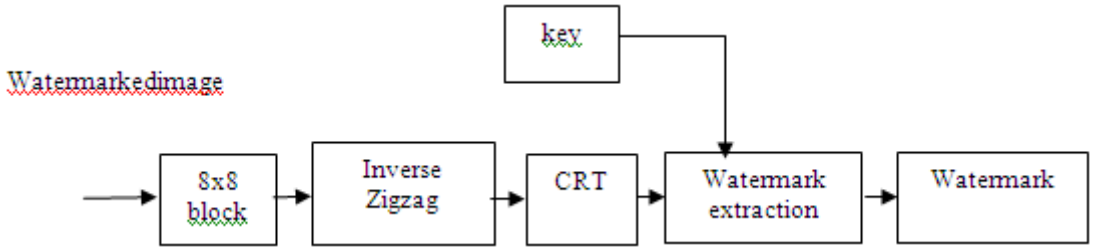

Figure-3. Extraction of watermark.

3. EXPERIMENTAL RESULTS

The performance of the proposed method with other schemes is evaluated using (i) Peak signal-to-noise ratio (PSNR), (ii) Tamper Assessment Function (TAF) and (iii) Structural similarity (SSIM)

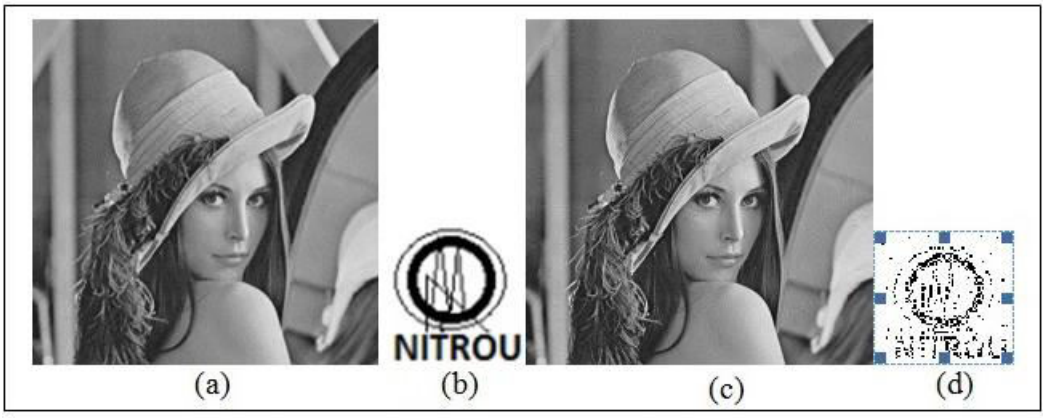

Figure-4. Original(a) Lenna, (b) Watermark (c) Watermarked image (35.6 dB), (d) Reconstructed watermark (TAF-32%)

Table-1. Time complexity (in sec) comparison.

Images	Patra *et al*	Proposed
Lenna	8.544	12.02
Mandrill	8.504	12.07
Barbara	8.469	11.96

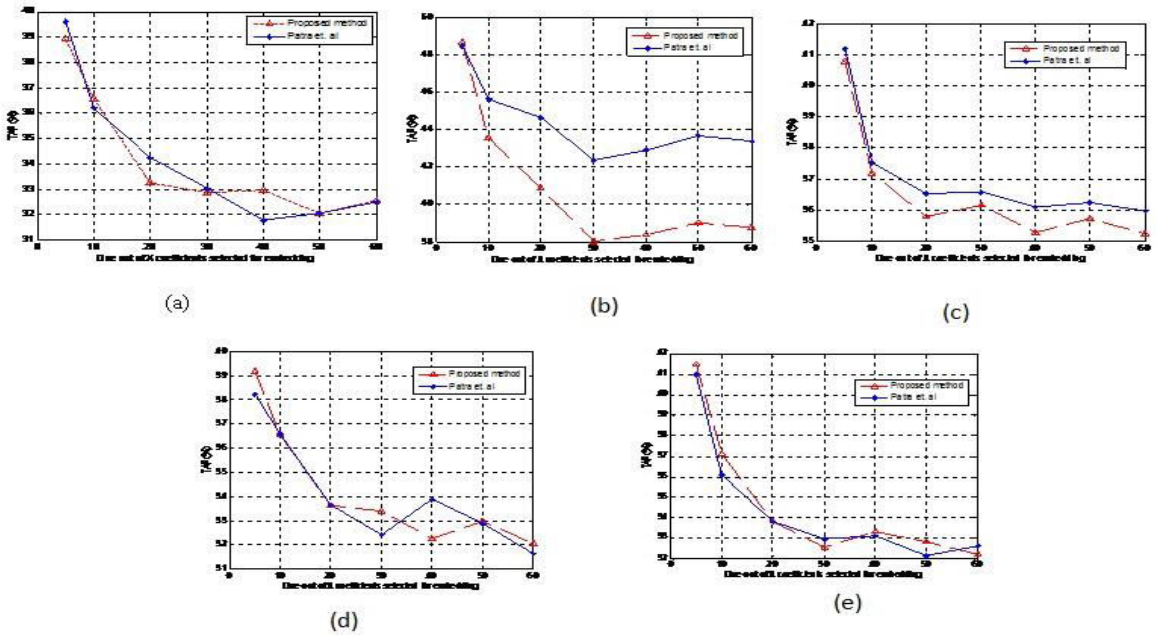

Figure-5. (a)-(b) show the test image (Lenna) and watermark image. Figure-4 (c) and (d) show the watermarked image and extracted watermark, respectively. We have tested the watermarked image with various common attacks like, cropping, Noise addition, Brightening, Sharpening, Compression. The TAF comparison plots are presented in Figure-5 (a)-(e). It is observed that using the proposed technique the watermark image can be restored. From Figure-5, the proposed technique exhibit better watermark image in (b) cropping, (c) noise (d) sharpening, (e) brightening and compression operation than (Patra *et al*., 2010). However, the quality of the watermark is 30-40% in both schemes. As the proposed algorithm uses CRT for embedding the watermark in the host image, additional robustness is achieved at the cost of TAF value.

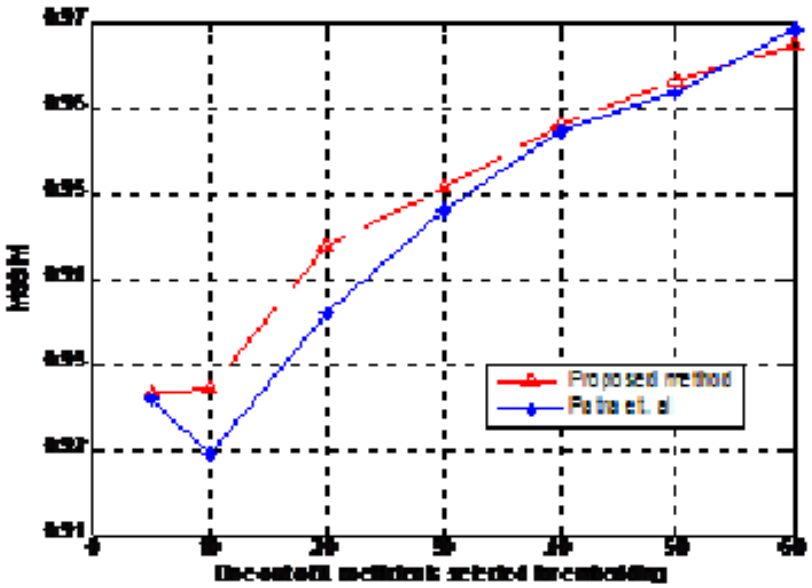

Figure-6. MSSIM performance of Watermarked image under without attack.

Table-2. PSNR and SSIM comparison table for Lenna image.

One out of X Coeff used	Scheme	Without attack PSNR	SSIM	Cropping attack PSNR	SSIM	Salt and pepper Noise PSNR	SSIM	Sharpening PSNR	SSIM	Brightening PSNR	SSIM
X=5	Patra *et al*	36.9835	0.9261	36.973	0.9258	36.9000	0.9253	36.9931	0.9267	36.8015	0.9254
	Proposed	36.7904	0.9267	36.754	0.9259	36.7186	0.9273	36.7186	0.9273	36.7885	0.9270
X=10	Patra *et al*	36.2618	0.9195	36.3484	0.9200	36.2451	0.9193	36.2729	0.9185	36.3400	0.9199
	Proposed	36.1026	0.9272	36.1526	0.9284	36.2644	0.9300	36.1883	0.9292	36.1736	0.9289
X=20	Patra *et al*	35.6821	0.9361	35.7596	0.9362	35.6833	0.9364	35.8105	0.9368	35.7496	0.9369
	Proposed	35.7132	0.9440	35.7069	0.9433	35.6997	0.9431	35.6357	0.9426	35.7387	0.9438
X=30	Patra *et a*l	35.4068	0.9481	35.4095	0.9497	35.4479	0.9484	35.4469	0.9479	35.4132	0.9789
	Proposed	35.4119	0.9508	35.4102	0.9512	35.4643	0.9513	35.4558	0.9512	35.4102	0.9512
X=40	Patra *et al*	35.2375	0.9574	35.252	0.9565	35.3071	0.9582	35.2031	0.9571	35.2212	0.9578
	Proposed	35.2076	0.9582	35.2569	0.9573	35.2613	0.9576	35.2068	0.9580	35.2466	0.9568
X=50	Patra *et al*	35.1516	0.9620	35.1801	0.9644	35.1109	0.9643	35.1126	0.9636	35.1986	0.9647
	Proposed	35.1125	0.9634	35.1282	0.9636	35.1322	0.9641	35.1474	0.9648	35.1417	0.9630
X=60	Patra *et al*	35.0935	0.9694	35.0212	0.9691	35.0620	0.9710	35.062	0.9710	35.0799	0.9699
	Proposed	35.0185	0.9674	35.0384	0.9673	35.0090	0.9676	35.0257	0.9682	35.0418	0.9682

Table-3. TAF quality comparison between DCT and DTT based schemes.

Scheme	Sharpen (50%)	Noise (Salt and Pepper)	Brighten (110%)	Without attack	crop	Compression (50%)
Patra *et al*						
Proposed						

It was demonstrated that the SVD [10] [12] and CRT based spatial domain technique do not work for cropping, brighten, sharpen and compression operations. The proposed technique is better than SVD [10] [12] and CRT based, because it can withstand all aforementioned operations. Considering the case about the reconstructed watermarked image quality, our technique exhibit better visual quality than the other existing schemes [7] [21]. The improvement in SSIM value from Table-2 is a clear evidence of the reconstructed watermarked image quality. Table-4 shows the reconstructed watermark quality comparison under different attacks. It has been seen that the reconstructed image quality is robust to almost all attack.

Table-1 shows the time complexity of the watermark embedding and extracting process. It shows that the proposed technique has more time complexity (about 4 sec) than DCT based technique. This is because; DTT execution time is more than DCT. The higher order polynomials of DTT, depend on recursive relationship with lower order polynomials, it is not the case for DCT. Therefore, the iterative nature of DTT consumes slightly more time than DCT. However, this is trivial in hardware implementation as the Hardware uses DTT kernel coefficients like DCT. Therefore, the proposed method will exhibit similar time complexity as with DCT in a hardware platform. PSNR and SSIM comparison [13] [17] is between DCT and DTT watermarking scheme is shown in Table-2. Table-3 shows the TAF quality comparison between DCT and DTT schemes. It is evident that DTT based scheme outperform in most of the cases compared to DCT scheme.

4. CONCLUSION AND FUTURE SCOPE

A new approach of watermarking scheme using CRT on DTT domain for authentication and copyright protection is proposed. Incorporation of CRT gives advantages in terms of improved security and low computational complexity. In addition to the above, further security feature due to random selection of watermarking blocks and location of watermarked bits is incorporated. The performance of the proposed scheme is compared against CRT based DCT scheme for common attacks. It is shown that it performs well for some major attacks such as brightening, sharpening, cropping and compression. As the computation of CRT is modular, the time required for embedding and extraction depends on the type of transform. The proposed scheme is slightly

complex (in time) than DCT scheme. However, it is trivial for hardware implementation as the DTT kernel coefficients can be implemented directly in hardware, like DCT kernel coefficients. As the correlation between the proposed scheme and CRT based DCT are similar in approach, we expect that by doubling the watermarking scheme, the imperceptibility and robustness against various attacks can be maintained. The proposed scheme can also be applied to text, audio and video.

REFERENCES

[1] Ahmed A.M. and Day D.D. 2004. Applications of the naturalness preserving transform to image watermarking and data hiding, Digital Signal Process. 14: 531-549.

[2] Barni M., Bartolini F., Cappellini V., Piva A. 1997. A DCT-domain system for robust image watermarking, Signal Process. 66: 357-372.

[3] Cox I.J., Kilian J., Leighton F.T., Shamoon T. 1997. Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6(12): 1673-1687.

[4] Chen T.H. and Tsai D.S. 2006. Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol, Pattern Recogn. 39(8): 1530-1541.

[5] Chung K.L., Yang W.N., Huang Y.H., Wu S.T., Hsu Y.C. 2007. On SVD-based watermarking algorithm, Appl. Math. Comput. 188(1): 54-57.

[6] Chan Y. -H. and Siu W.-C. 1992. On the realization of discrete cosine transform using distributed arithmetic. IEEE Trans, Circuits Syst. I: Fundam. Theory Appl. 39(9): 705-711.

[7] Chang C.-C., Tsai P., Lin C.-C. 2005. SVD-based digital image watermarking scheme. Pattern Recogn. Lett. 26: 1577-1586.

[8] Deng C., Gao X., Li X., Tao D. 2009. A local Tchebichef moments-based robust image watermarking. Signal Process. 89: 1531-1539.

[9] Hsu C.T. and Wu J.L. 1999. Hidden digital watermarks in images. IEEE Trans. Image Process. 8(1): 58-68.

[10] Huang H., Coatrieux G., Shu H., Luo L., Roux C. 2012. Blind integrity verification of medical images. IEEE Trans. on information technology in Biomedicine. 16(6): 1122-1126.

[11] Ishwar S., Meher P.K., Swamy M.N.S. 2008. Discrete Tchebichef transform-A fast 4 × 4 algorithm and its application in image/video compression. IEEE Int. Symp. Circuits and Systems (ISCAS), Seattle, USA. pp. 260-263.

[12] Kalantari N.K., Ahadi S.M., Vafadust M. 2010. A robust image watermarking in the Ridgelet domain using universally optimum decoder. IEEE Transactions on Circuits and Systems for Video Technology. 20: 396-406.

[13] Kougianos E., Mohanty S.P., Mahapatra R.N. 2009. Hardware assisted watermarking for multimedia. Comp. Electrical Eng. 35: 339-358.

[14] Karthanasis H.C. 1995. A low ROM distributed arithmetic implementation of the forward/inverse DCT/DST using rotations. IEEE Trans. Consumer Electron. 41(2): 263-272.

[15] Lu Z.M., Zheng H.Y., Huang J. 2007. A digital watermarking scheme based on DCT and SVD. In: Proceedings of 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp. 241-244.

[16] Liu K.-C. 2010. Wavelet-based watermarking for color images through visual masking. AEU Int. J. Electronics Commun. 64(2): 112-124.

[17] Liu R. and Tan T. 2002. An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans. Multimedia. 4(1): 121-128.

[18] Lin C.Y. and Chang S.F. 2001. A robust image authentication method distinguishing JPEG compression from malicious manipulation. IEEE Trans. Circuits Systems Video Technol. 11(2): 153-168.

[19] Lee S., Jang D., Yoo C.D. 2005. An SVD-based watermarking method for image content authentication with improved security. In: Proc. IEEE Int. Conf. On Acoustics, Speech, and Signal Process. 2: 525-528.

[20] Li L., Zhu H., Yang G., Qian J. 2014. Reference less measure of blocking artifacts by Tchebichef kernel analysis. IEEE signal proc. Letts. 21(1): 122-125.

[21] Senapati R.K., Pati U.C., Mahapatra K.K. 2011. A fast zigzag pruned 4 × 4 DTT algorithm for image compression, WSEAS Trans. Signal Process. 7(1): 34-43.