World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:10, 2007

An Improved Method to Watermark Images Sensitive to Blocking Artifacts

Afzel Noore

***Abstract*—**A new digital watermarking technique for images that are sensitive to blocking artifacts is presented. Experimental results show that the proposed MDCT based approach produces highly imperceptible watermarked images and is robust to attacks such as compression, noise, filtering and geometric transformations. The proposed MDCT watermarking technique is applied to fingerprints for ensuring security. The face image and demographic text data of an individual are used as multiple watermarks. An AFIS system was used to quantitatively evaluate the matching performance of the MDCT-based watermarked fingerprint. The high fingerprint matching scores show that the MDCT approach is resilient to blocking artifacts. The quality of the extracted face and extracted text images was computed using two human visual system metrics and the results show that the image quality was high.

***Keywords*—**Digital watermarking, data hiding, modified discrete cosine transformation (MDCT).

I. Introduction

A number of digital watermarking embedding methods exist [1]-[4]. The watermark must not degrade the perceived quality of the host image and must be robust from external attacks and tampering. Chen and Wornell proposed a class of information embedding system called Quantization Index Modulation [5]. This is effective compared to the previously proposed methods such as spread spectrum and low bit modulation techniques [6]-[8]. Information embedding systems use block-transformation techniques for coding images [9], [10]. The block transformation based watermarking of images using DCT is simple, effective, and widely used. The image is typically divided into 8 x 8 blocks. DCT is applied to these blocks and the transform coefficients are individually quantized. The watermark is embedded into the host image in the transformation domain and the inverse transformation is performed to generate the watermarked image. The block transform watermarking process introduces a number of undesirable artifacts into the images; two kinds of reconstruction artifacts are typical in transform coefficients, mainly at low bit rates. The blocking artifacts arise because the concatenation of the reconstructed blocks generates signal discontinuities across block boundaries. The ringing artifacts arise because the quantization errors on the transform coefficients generate signal reconstruction errors that last for the entire block duration. These artifacts constitute a serious bottleneck for many important visual applications. In this paper we focus on the structural integrity of a watermarked image besides the visual quality. This is especially important in watermarking fingerprint images for security. A watermarking scheme that introduces artifacts and discontinuities among the pixels of the adjacent blocks may keep the fingerprint secure but can seriously affect the fingerprint matching ability. We propose using the Modified Discrete Cosine Transform (MDCT), for watermarking because the transformation coefficients correspond to non-independent overlapping signal blocks. We compare our results with the performance of other existing methods using standard images. Our proposed approach is extended to watermarking fingerprint images with two contextual watermarks, face and demographic text data, that are typically collected by law enforcement personnel while registering the fingerprint of an individual. The ridge patterns of the fingerprint are sensitive to artifacts that cause structural discontinuities and affect the matching performance. The effectiveness of the proposed MDCT watermarking approach is quantitatively assessed by an Automatic Fingerprint Identification System (AFIS) to verify the integrity of the original fingerprint and the watermarked fingerprint. The original face and text images are quantitatively compared with the extracted images from the watermarked fingerprint by using pixel based metrics and human visual system based quality metrics.

Manuscript received November 16, 2004. This work was supported in part by the U.S. Department of Justice under Grant 2003-RC-CX-K001.

A. Noore is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506-6109 (phone: 304-293-0405; fax: 304-293-8602; e-mail: noore@ csee.wvu.edu).

II. Proposed MDCT based watermarking

In this section, the properties of MDCT which are helpful in eliminating the blocking artifacts are highlighted. Let ‘a’ be a one dimensional discrete time signal of length N that is segmented into n blocks denoted as a(n). Each block is assumed to consist of two parts, right half and left half, denoted by $a'(n) = [a_l'(n)\ a_r'(n)]$. After the application of the MDCT transform, each signal block is left with l coefficients, where l = 2n. The adjacent blocks after transformation overlap by l-n coefficients, which is equal to a 50% overlap. There are n basis functions of length 2n. The resulting transform matrix consists of coefficients that are given by $c(n) = BT[a_r'(n-1)\ a_l'(n)\ a_r'(n)\ a_l'(n+1)]$, where B is a 2n x n matrix with basis functions as columns. Here the resulting coefficient blocks

contain information not only about a(n) but also about $a_r(n-1)$ and $a_l(n+1)$, the corresponding adjacent signal blocks. The implementation of MDCT on a sequence of data results in equal number of samples before and after the transformation. After performing the inverse MDCT, the transformed data does not resemble the original data. When these blocks of data are concatenated, the errors introduced by the transform cancel out due to the time domain aliasing. The MDCT for a two dimensional array is defined as,

$$X(k,l)=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}s(i,j)\cos\left[\frac{\pi}{N}(2k+1)(i+n)\right]\cos\left[\frac{\pi}{N}(2l+1)(j+1)\right] \quad (1)$$

where, $n=\frac{1}{2}\left(\frac{N}{2}+1\right)$

When it is implemented effectively with FFT algorithm and the coefficients are symmetrical,

$$\begin{aligned} x(k,l) &= x(N-k-1,\,N-l-1) \\ &= -x(k,\,N-l-1) \\ &= -x(N-k-1,\,l) \end{aligned} \quad (2)$$

This reduces the spectrum size from N^2 to $(n/2)^2$. The nverse MDCT is defined as,

$$Y(k,l)=\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\frac{4}{N}s(i,j)\cos\left[\frac{\pi}{N}(2k+1)(i+n)\right]\cos\left[\frac{\pi}{N}(2l+1)(j+n)\right] \quad (3)$$

In our proposed approach, the image features such as lines ınd edges are extracted using phase congruency since it is ndependent of the image intensity and contrast. The extracted ine and edge features of the host image are transformed to ıMDCT domain. A binary image watermark is embedded into he MDCT coefficients of the host image features. The block liagram of the proposed MDCT watermarking method is hown in Fig. 1.

Let 'O' be the original image and 'W' be the watermark mage.

$$O=\sum_{i=1}^{n}\sum_{j=1}^{m}\{O_{i,j}\} \quad (4)$$

where m and n are the length and width of the image coefficient matrix. The image features from phase congruency are extracted and decomposed using MDCT. The size of the watermark image is adjusted to the size of the image feature matrix M, which is to be watermarked. The coefficients of the transformed matrix are watermarked as shown in (5). A secret key is used for selecting the coefficients of the host image randomly.

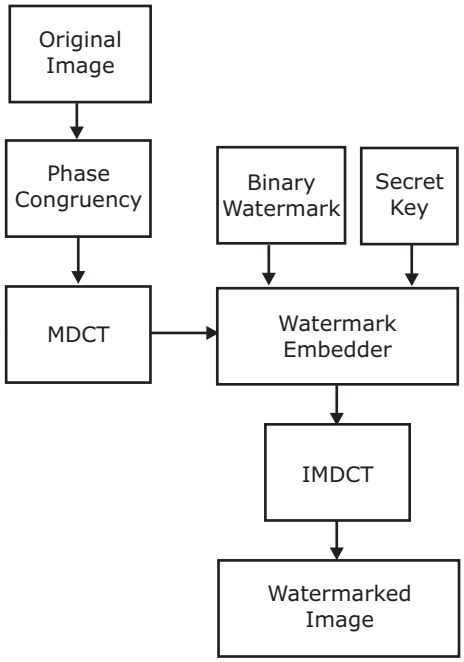

Fig. 1 Proposed MDCT Watermarking Embedding Process

$$S(r,s)=\sum_{i=1}^{r}\sum_{j=1}^{s}M(i,j)+\alpha*\sum_{i=1}^{r}\sum_{j=1}^{s}W(i,j) \quad (5)$$

α is the coefficient of watermarking strength. Coefficients i and j are randomly selected using a secret key. The watermarked coefficients (S) will replace the corresponding coefficients in the original image. The inverse transform (IMDCT) is performed to obtain the watermarked image, W, in spatial domain. This completes the embedding process. For extraction of the watermark, the reverse procedure of (5) is used. The secret key, α value, and the original image are needed for decoding the watermark.

III. Validation of the MDCT Based Watermarking

To determine the effectiveness of the proposed MDCT based digital watermarking technique we compare the performance with existing work using known JPEG test images. The similarity of the original image and the watermarked image are quantitatively determined using several metrics. Table 1 compares the peak signal to noise ratio (PSNR) of the proposed MDCT approach with existing methods. The watermark embedded by the proposed method is highly imperceptible compared to other known traditional watermarking techniques [11]-[14].

TABLE I
Performance Comparison of PSNR with Existing Approaches

	Cox Method-1	Cox Method-2	Xia Method	Jong Method	Proposed MDCT
PSNR	51.36	42.43	50.12	52.46	56.01

The performance when a watermarked image is subjected to frequency and spatial attacks is also studied. The similarity between the original watermark and the extracted watermark is calculated using,

$$Sim(X, X') = \frac{X \cdot X'}{\sqrt{X' \cdot X'}} / \frac{X \cdot X}{\sqrt{X \cdot X}} \times 100 \quad (6)$$

where X is original watermark and X' is the extracted watermark after the watermarked image has undergone different transformations. The values obtained from the similarity equation are compared with existing techniques. Fig. 2 shows that the proposed MDCT approach is robust and has a high correlation between the original watermark and the extracted watermark after the watermarked image has undergone different attacks such as like JPEG compression at 70%, Gaussian noise, wavelet compression, cropping, and salt and pepper noise.

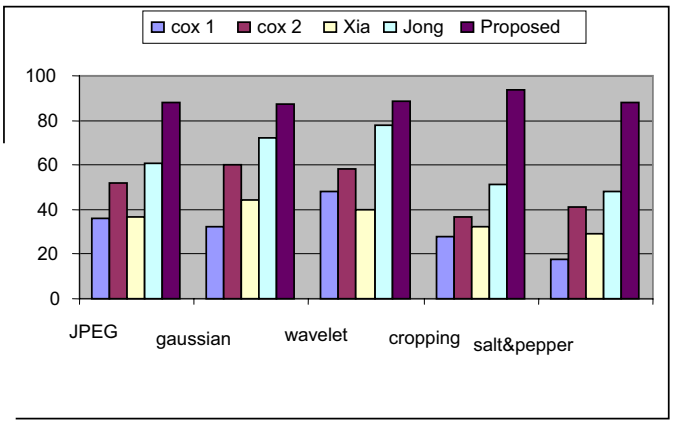

Fig. 2 Performance comparison with different attacks

We also use two recent human visual system based (HVS) mage quality metrics, the Structural Similarity Metric (SSIM) 15] and the Universal Image Quality Index (UIQI) [16], to neasure the similarity between original image and the roposed MDCT based watermarked images.

TABLE 2
IUMAN VISUAL SYSTEM METRICS OF ORIGINAL AND WATERMARKED IMAGES

Image	Structural Similarity Metric	Universal Image Quality Index
Lena	0.8760	0.9245
Baboon	0.8259	0.8411
Peppers	0.9031	0.9662

Table 2 shows that there is negligible perceptible difference between the original images and the watermarked images. Next, the effectiveness of the MDCT based watermarked approach is assessed by subjecting the watermarked image to various attacks and calculating the human visual system based (HVS) image quality metrics.

TABLE 3
HUMAN VISUAL SYSTEM METRICS OF ORIGINAL AND EXTRACTED WATERMARK UNDER ATTACKS

Attack	Structural Similarity Metric	Universal Image Quality Index
JPEG Compression	0.7432	0.7852
Wavelet Compression	0.8823	0.9144
Gaussian Noise	0.8594	0.9363
Salt & Pepper Noise	0.7920	0.8247
Cropping	0.5091	0.4680

Table 3 shows that the extracted watermark from the attacked watermarked image closely resembles the original watermark image. The watermark embedded in the original host image using the proposed MDCT approach is imperceptible and robust. The 50% overlap in the block size of the MDCT approach has eliminated the blocking artifacts and the quality of the watermarked image is greatly improved.

IV. MULTIPLE WATERMARKING OF A FINGERPRINT IMAGE USING MDCT

In this section we apply the proposed MDCT based approach to watermark fingerprint images. A fingerprint is composed of composite structures with light and dark regions called ridges and valleys. The most important discriminating features of a fingerprint used in matching process are the minutiae, which represent the local discontinuities in the ridge flow pattern. The automated fingerprint matching systems use two types of minutiae features, the ridge ending and ridge bifurcation. The minutiae location and angle of orientation are attributes used for representing the fingerprint and for matching. These attributes of the minutia points are invariant to light and dark regions of the ridge structures, which ensures their consistent extraction even when the image is degraded due to noise or contrast variance. When watermarking fingerprints to improve security, the structural integrity of the ridge patterns should be preserved. Any discontinuity in the ridges caused by blocking artifacts introduces spurious minutiae and can affect the ability to match a fingerprint correctly.

A. Watermark Embedding

Fingerprint images collected by law enforcement agencies are stored in a database along with the demographic text data of the individual and a face image. A contextual watermarking scheme shown in Fig. 3 embeds the face image and demographic text image of an individual as watermarks in the fingerprint image using the MDCT watermarking approach. The integrity of the watermarked fingerprint images is secured. In addition, the face and the text images are used for identification purposes. Hence the extracted watermarks

should be of high quality.

The application of MDCT results in smooth edge decomposition and the watermarked fingerprint ridge structures do not degrade. The fingerprint image is decomposed into transform domain using MDCT. The ridge structure locations are identified by converting the grayscale fingerprint image to binary using a global threshold and locating the dark regions.

$$R(i,j) = \sum_{i=1}^{M}\sum_{j=1}^{N} F(i,j) \rceil G_T$$

$$R_T = MDCT(R) \tag{7}$$

where F is the grayscale fingerprint image of size M x N and G_T is the global threshold for binarization. The size of the ridge structure matrix is assumed to be greater than the combined image sizes of the watermarks. The MDCT coefficients corresponding to ridges are represented as R_T.

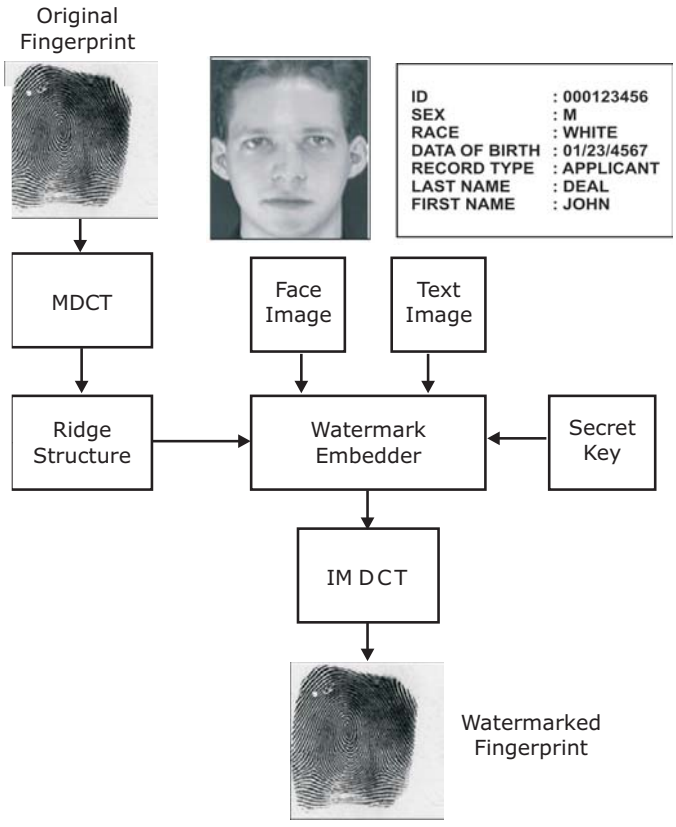

Fig. 3 MDCT based fingerprint watermarking using multiple watermarks

The two watermarks are embedded at two different locations without overlap. The embedding process follows (8) for the facial image W_f, which is of the size P x Q.

$$\dot{R}_T(i,j) = \sum_{i=1}^{P}\sum_{j=1}^{Q} R_T(i,j) + \alpha 1 * W_f(i,j) \tag{8}$$

where $\dot{R}_T$ is the ridge coefficient matrix embedded with the face watermark. The embedding process for the text image W_t of size S x T is given in (9).

$$\ddot{R}_T(i,j) = \sum_{i=P}^{S}\sum_{j=Q}^{T} R_T(i,j) + \alpha 2 * W_t(i,j) \tag{9}$$

where $\ddot{R}_T$ is the ridge coefficient matrix embedded with both face and text watermarks. The watermarked fingerprint, W, is obtained by reconstructing the embedded ridge coefficients with Inverse Modified Discrete Cosine Transform (IMDCT). A secret key is used to select the embedding locations randomly to secure the original fingerprint and the embedded face and text watermarks from tampering. The amplifying factors, α1 and α2, are computed from the perceptual model [17] that varies the watermarks such that maximum amount of information can be hidden in the host fingerprint image depending on luminance and contrast properties of the embedding region.

B. Verifying the integrity of watermarked fingerprint

The proposed embedding algorithms are implemented using a 512 x 512 fingerprint image as the host image. The original face image of size 102 x 102 and the original text image of size 220 x 220 are used as contextual watermarks. The proposed MDCT watermarking algorithm is used to embed the face and the text images in the fingerprint. The resulting watermarked fingerprint image is securely protected and can be used to verify the chain of custody or if the fingerprint has been tampered. Any degradation in visual image quality between the original fingerprint image and the watermarked fingerprint image is very small and is hardly discernable.

To verify the effect of watermarking on fingerprint images, an AFIS system is used. A set of fingerprint images is watermarked using the proposed algorithm and are matched with other fingerprints stored in the database of the AFIS system. The results of the matching scores are shown in Fig. 4.

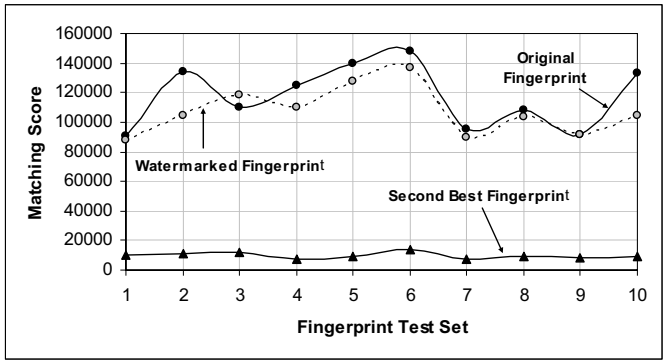

Fig. 4 AFIS matching scores of the watermarked fingerprint images

The high matching scores of the original fingerprint image and the watermarked fingerprint image validate that the fingerprint features such as ridge bifurcations and ridge endings that are used for matching purposes have not been altered. This is possible when artifacts in the form of discontinuities are not introduced. The 50% overlap in block size eliminates any break in image structures. In the case of fingerprints, the breaks can increase the number of minutiae

points and affect the fingerprint integrity and matching score. Fig. 4 also shows that the matching score of the next closest fingerprint or the second best fingerprint from the database is so low that it would not be classified as a possible match in the AFIS system.

C. Extraction of Face and Text Images

The process to extract the text and face image from the watermarked fingerprint is shown in Fig. 5. The extraction process is the reverse of the embedding process. The same secret key used during embedding is now used to determine the order of extracting the bits. The extraction process of the watermark images in the MDCT based technique includes the selection of ridge MDCT coefficients using the same global threshold for binarization and subtracting the magnitude of these coefficients from the corresponding original fingerprint image coefficients. This is then scaled with the amplification factors as given in (10) and (11).

$$E_f(i,j) = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q} R(i,j) - \ddot{R}(i,j)}{\alpha 1} \quad (10)$$

$$E_t(i,j) = \frac{\sum_{i=P}^{S}\sum_{j=Q}^{T} R(i,j) - \ddot{R}(i,j)}{\alpha 2} \quad (11)$$

E_f is the extracted facial image and E_t is the extracted text mage. Fig. 5 shows the extracted face and the extracted text mages from the MDCT based watermarked fingerprint image. The original fingerprint image is required for the extraction of vatermarks.

D. Determining the Quality of Extracted Images

We next quantitatively determine the degree of similarity between the original watermark images and the extracted vatermark images using two different types of metrics. The eak signal to noise ratio (PSNR), mean square error (MSE), nd correlation between the original and modified images give he pixel-based similarity between the images. The structural imilarity measure (SSIM) and universal image quality index UIQI) compare the images based on human visual system HVS).

Table 4 shows the degree of similarity between the original text and the face images, and the extracted images.

TABLE 4
IMAGE QUALITY METRICS

Image	Pixel-based Metrics			HVS-based Metrics	
	PNSR	MSE	Correlation	SSIM	UIQI
Face	52.50	76	0.9230	0.8219	0.9341
Text	64.72	52	0.8439	0.9576	0.7780

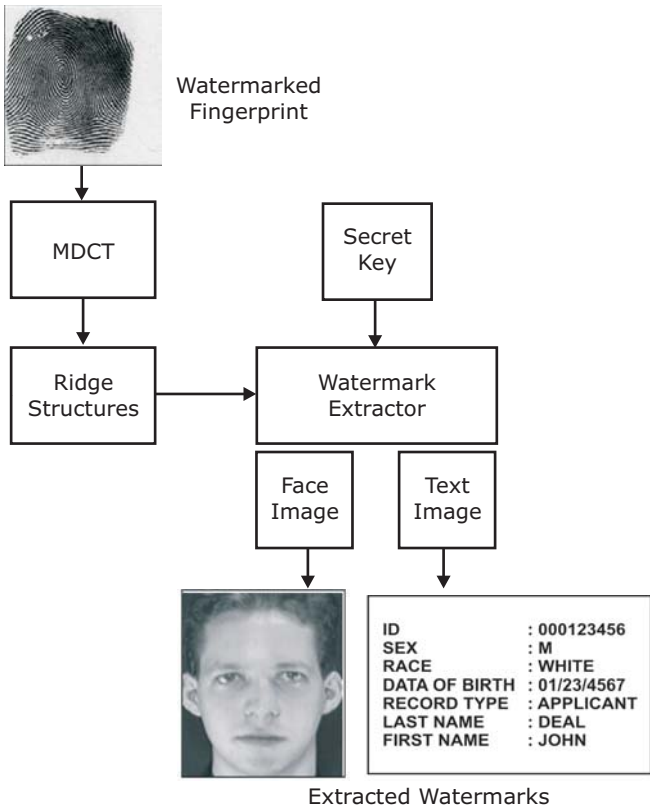

Fig. 5 MDCT based multiple watermark extraction showing extracted face and extracted text

The similarity values obtained by using both the pixel based metrics and the human visual system image quality metrics show a high level of correlation between the original images used as watermarks and the extracted watermark images.

The electronic transmission of watermarked fingerprints introduces degradations in the image data due to compression, noise and filtering. The effects of these on the watermarked fingerprint are studied. The results of the tests show that the watermarked fingerprint is resilient to various distortions that commonly occur during the image transmission process. A high similarity value is obtained between the original and extracted watermarks for up to 70% of JPEG compression level, median filter window size of 5 and Gaussian noise variance of 0.05.

Next, the quality of the extracted face and text from the watermarked fingerprint image are computed. Since the visual quality of the text and the face images are commonly used for personal identification, it is appropriate to use the human visual metrics for comparison purposes. The two HVS based metrics, SSIM and UIQI, are used. The proposed watermarking technique is also robust to spatial domain attacks such as cropping and rotation. The 512 x 512 watermarked fingerprint image is cropped to 450 x 450 at the center and the angle of rotation is 10 degrees. The moderately high correlation between the original and extracted watermarks shows that the proposed techniques are robust to cropping and rotation.

TABLE 5
RESILIENCE OF MDCT BASED METHOD TO SPATIAL ATTACKS

Spatial Attacks	Face Image		Text Image	
	SSIM	UIQI	SSIM	UIQI
Cropping	0.7302	0.6649	0.6851	0.6937
Rotation	0.7108	0.6285	0.6350	0.6748

V. CONCLUSION

An improved digital watermarking algorithm using MDCT is presented. The binary watermark is embedded into selected image features of the host image. Using JPEG test images the experimental results show that the proposed technique using MDCT eliminates blocking artifacts and introduces a more natural degradation of the image at low bit rates and has better anti-aliasing properties. At higher bit rates the smoothing effect produces very high quality images. The proposed method is robust to various spatial and frequency domain attacks. The MDCT approach is applied to fingerprints using two contextual watermarks. A face image and the corresponding demographic text data of an individual are embedded into selected regions of fingerprint image. The watermarked fingerprint provides added protection from tampering and the fingerprint matching ability is not affected even when subjected to common attacks. Quantitative results show that the extracted face and text images are of high quality suitable for identification purposes. Using the proposed approach, the absence of watermarks or visual distortions in the extracted watermarks would reveal if the integrity of the fingerprint image has been compromised.

ACKNOWLEDGMENT

The author thanks Sagem Morpo for the AFIS system and the database of over two million fingerprints that was used during this research.

REFERENCES

[1] T. Liu, Z.-D. Qiu, "The survey of digital watermarking-based image authentication techniques," in *Proc. 6th Intl. Conf. on Signal Processing*, vol.2, pp. 1556-1559, 2002.

[2] Y. Wang, J.F. Doherty, R.E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. Image Processing*, vol. 11, no. 2, pp. 77-88, 2002.

[3] D.P. Mukherjee, S. Maitra, S.T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication," *IEEE Trans.on Multimedia*, vol. 6, no. 1, pp. 1-15, 2004.

[4] W. N. Cheung, "Digital image watermarking in spatial and transform domains," in *Proc. TENCON 2000*, vol. 3, pp. 374 – 378, September 2000.

[5] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Information Theory*, vol. 47, no. 4, pp. 1423-1443, May 2001.

[6] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermarking recovering without restoring to the uncorrupted original image," in *Proc. IEEE Intl. Conference on Image Processing*, vol. 1, pp. 520-523, 1997.

[7] A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in *Proc. IEEE Intl. Conference on Image Processing*, vol. 3, pp. 231-234, 1996.

[8] C. T. Hsu and J. L. Wu, "DCT-based watermarking for video," *IEEE Trans. Consumer Electronics*, vol. 44, no. 1, pp. 206-216, Feb 1998.

[9] I. J. Cox, J. Killian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," NEC Research Institute, Technical Report 95 - 10, 1995.

[10] O.-H Kwon, Y.-S Kim, R.-H Park, "Watermarking for still images using the human visual system in the DCT domain," in *Proc. 1999 IEEE Intl. Symp. on Circuits and Systems*, vol. 4, pp. 76 – 79, June 1999.

[11] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec.1997.

[12] Hsu, C. T., and Wu, J. L. "Hidden Digital Watermarks in Images," *IEEE Trans. Image Processing*, vol. 8, pp. 58-68, 1999.

[13] X. Xia, C. Boncelet, and G. Arce, "Multiresolution Watermark for Digital Images," in *Proc. IEEE Int. Conf. on Image Processing*, vol. 1, pp. 548-551, Oct. 1997.

[14] J. R. Kim and Y. S. Moon, "A Robust Wavelet-Based Digital Watermark Using Level-Adaptive Thresholding," in *Proc. 6th IEEE Intl. Conf. on Image Processing*, pp. 202, Kobe, Japan, Oct. 1999.

[15] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," *IEEE Trans. Image Processing*, vol. 13, no. 1, 2004.

[16] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "A Universal Image Quality Index," *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81-84, 2002.

[17] C. I. Podilchuk, W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525-539, 1998.

Afzel Noore received his Ph.D. in Electrical Engineering from West Virginia University in 1987. From 1980 to 1983, he worked as a digital design engineer at Philips India where he developed microprocessor based scientific instruments in collaboration with Philips Eindhoven Holland. He is an Associate Professor in the Lane Department of Computer Science and Electrical Engineering. He served as the Associate Dean for Academic Affairs and Special Assistant to the Dean in the College of Engineering and Mineral Resources at West Virginia University from 1996 to 2003. His research interests include digital watermarking, fuzzy and neural systems, fault-tolerant computing, software reliability, biometrics, and consumer electronics. His research has been funded by Westinghouse, GE, NSF, Electric Power Research Institute, Department of Energy, NASA and the US Department of Justice.