

Robust Minutiae Watermarking in Wavelet Domain for Fingerprint Security

Rajlaxmi Chouhan^{*}, Pritee Khanna

Abstract—In this manuscript, a wavelet-based blind watermarking scheme has been proposed as a means to provide security to authenticity of a fingerprint. The information used for identification or verification of a fingerprint mainly lies in its minutiae. By robust watermarking of the minutiae in the fingerprint image itself, the useful information can be extracted accurately even if the fingerprint is severely degraded. The minutiae are converted in a binary watermark and embedding these watermarks in the detail regions increases the robustness of watermarking, at little to no additional impact on image quality. It has been experimentally shown that when the minutiae is embedded into wavelet detail coefficients of a fingerprint image in spread spectrum fashion using a pseudorandom sequence, the robustness is observed to have a proportional response while perceptual invisibility has an inversely proportional response to amplification factor “K”. The DWT-based technique has been found to be very robust against noises, geometrical distortions filtering and JPEG compression attacks and is also found to give remarkably better performance than DCT-based technique in terms of correlation coefficient and number of erroneous minutiae.

Keywords—Fingerprint watermarking, minutiae, discrete wavelet transform, PN sequence

I. INTRODUCTION

FINGERPRINTS are unique biometrics mainly used for the establishment of instant personal identity. However they are susceptible to accidental/intentional attacks. Protection of biometric data is gaining interest and digital watermarking techniques are used to protect the biometric data from either accidental or intentional attacks [1-2]. Among the various biometrics, fingerprints are more famous in the authentication area, as they are unique to each person and are widely used in identification and verification of personal individuality. However, they are susceptible to accidental and intentional attacks, when transmitted over network. Thus, a defensive scheme is needed which will preserve fidelity and prevent modifications [3-5].

This problem can be addressed by embedding an invisible structure into a host signal to mark its ownership [4-5]. These structures are called *digital watermarks* and the associated embedding process *digital watermarking*. Watermarking of fingerprint images can be used to secure central databases from which fingerprint images are transmitted on request to intelligence agencies in order to use them for identification purposes [3]. In such cases, identification or verification process is generally preceded by a minutiae extraction and

matching process. There might be a situation when due to some incidental/intentional tampering, the received fingerprint is degraded beyond the capability of providing recognizable minutiae. To provide a solution to such a situation, the minutiae of a fingerprint may be embedded into the fingerprint so that even in case of fingerprint degradation, the minutiae can be robustly extracted and utilized for identification/verification process. The present manuscript addresses this issue.

The general process of watermarking involves the use of a key which must be used to successfully embed and extract the hidden information. The goal is to embed some information in the image without affecting its visual content. The embedding mechanism entails imposing imperceptible changes to the host signal to generate a watermarked signal containing the watermark information, while the extraction routine attempts to reliably recover the hidden watermark from a possibly tampered watermarked signal. At present, digital watermarking research primarily involves the identification of effective signal processing strategies to discreetly, robustly, and unambiguously hide the watermark information into multimedia signals [6-7]. In practice, it is required that a signal is accurately hidden into image data in such a way that it is very difficult to be perceived after hiding and also difficult to be removed [6-7]. It can be stated that the most important features a watermarking technique to be used for Intellectual Property Rights protection should exhibit are unobtrusiveness and robustness [8]. Ideal characteristics of a digital watermark include perceptual and statistical invisibility, fairly simple extraction and accurate detection, robustness to filtering, additive noise compression or image manipulations, and the ability to determine its true owner [7, 9].

A blind watermarking scheme is one where the cover signal (the original signal) is not needed during the detection process to detect the mark. Solely the key or the seed value, which is typically used to generate some random sequence used during the embedding process, is required. It is the blind watermarking schemes that find applications in biometric data communication where the host image is the main biometric data to be transmitted and the watermark can be a property or intrinsic information of that biometric data or an authentic identification of the biometric data owner itself.

Early work on digital watermarking for still images focused on information hiding in the spatial domain [11]. Recent efforts are mostly based on frequency-domain techniques [12-14]. Discrete Cosine Transform (DCT) based technique proposed by Lin *et al.* [12] addresses the watermark embedded at low frequency by using weighted correction to improve the imperceptibility of the watermark. Given the suitability of Discrete Wavelet Transform to model the Human Visual System behavior and its multiresolution properties [13-15], the

Rajlaxmi Chouhan is a Masters student at the Indian Institute of Information Technology, Design & Manufacturing Jabalpur (India) in Electronics & Communication Engineering discipline (email: rajlaxmi1020203@iiitdmj.ac.in)

Pritee Khanna is an Associate Professor in Computer Science & Engineering discipline at the Indian Institute of Information Technology, Design & Manufacturing Jabalpur (India) (email: pkhanna@iiitdmj.ac.in)

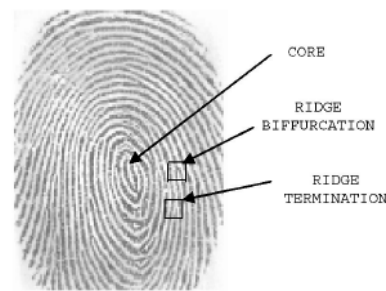
DWT has gained interest among watermarking researchers, and a lot of work has been done in past two decades [16-18]. A wavelet based technique proposed by Abu-Errub *et al.* [16] uses optimization and genetic algorithm for spread spectrum watermarking. Another wavelet based technique [18] using pseudonoise sequence for embedding into detail coefficients.

Embedding a watermark in both low and high frequencies leads to a robust scheme that can resist different kinds of attacks. Embedding in low frequencies increases the robustness with respect to attacks that have low pass characteristics like filtering, lossy compression, and geometric distortions while making the scheme more sensitive to modifications of the image histogram, such as contrast/brightness adjustment, gamma correction, and histogram equalization. Watermarks embedded in middle and high frequencies are typically less robust to low-pass filtering, lossy compression, and small geometric deformations of the image but are highly robust with respect to noise adding, and nonlinear deformations of the gray scale.

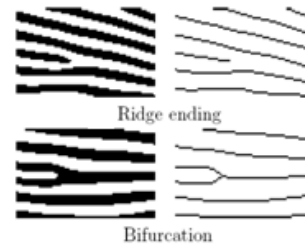
After a comparative study of various watermarking approaches in spatial and frequency domain and keeping the above mentioned points in consideration, a *wavelet-based, blind and robust minutiae watermarking technique for fingerprint protection* has been proposed in this manuscript. Strategic discontinuity information (minutiae) of the fingerprint is extracted and converted into a binary watermark. This watermark is embedded in all the detail coefficients of the DWT transformed coefficients of the cover fingerprint. The objective of this watermarking scheme is to ensure secure transmission of minutiae details even over a noisy communication channel or over one subject to intentional tampering. Our earlier work [18] involved embedding of a binary name label of the owner of the fingerprint. However, since here, the watermark (minutiae) is the intrinsic crucial information of the fingerprint itself, the utility as well as security application is greatly improved. Also, robustness has been improved by using two different pseudorandom sequences for both binary levels of watermark. The key contribution of this work is the application of existing wavelet-based binary watermarking scheme for the purpose of minutiae watermarking. Rigorous pre-processing mechanisms have been investigated to extract accurate minutiae points. These minutiae points have been uniquely used as a binary watermark for embedding. After robust extraction, even in the presence of strong attacks, this watermark is reconverted into minutiae information.

II. FINGERPRINT MINUTIAE

A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. The *minutiae*, which are the local discontinuities in the ridge flow pattern, provide the features that are used for identification (Fig. 1(a)). Details such as the type, orientation, and location of minutiae are taken into account while performing minutiae extraction. Minutiae points are most generally the locations of ending or bifurcation of ridges in a fingerprint (as shown in Fig. 1(b)).



(a) A typical fingerprint image



(b)

Fig. 1 (a) A typical fingerprint showing (b) ridge ending and bifurcation minutiae of a typical fingerprint

The steps of fingerprint minutiae extraction are [19, 20]:

- (a) Fingerprint enhancement
- (b) Feature extraction

A 2-dimensional Gabor filter consists of a sinusoidal plane wave of a particular orientation and frequency, modulated by a Gaussian envelope. Gabor filters are employed because they have frequency-selective and orientation-selective properties. These properties allow the filter to be tuned to give maximal response to ridges at a specific orientation and frequency in the fingerprint image. Therefore, a properly tuned Gabor filter can be used to effectively preserve the ridge structures while reducing noise [21].

Feature (minutiae) extraction includes binarization, thinning followed by morphological operations.

III. PROPOSED WATERMARKING SCHEME

The proposed watermarking scheme has been shown in Fig. 2. The cover image is the fingerprint while the watermark is a binary image equivalent to the minutiae of the cover fingerprint. The scheme has been divided into two sections: *Minutiae Embedding and Minutiae Extraction*. One of the many advantages of the wavelet transform is that it is believed to more accurately model aspects of the Human Visual System (HVS) as compared to the FFT or DCT [14]. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH}. Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

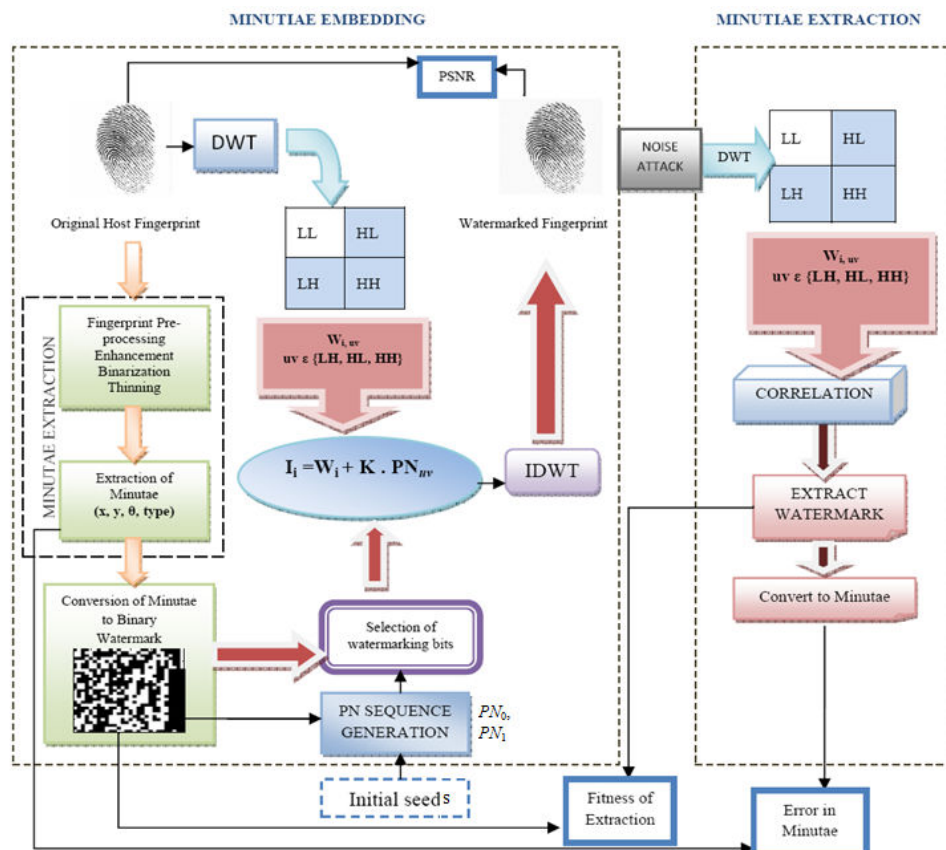


Fig. 2 Proposed Fingerprint minutiae embedding and extraction algorithm

A. Embedding procedure

The steps of minutiae watermark embedding as are follows:

Step 1: The fingerprint image is decomposed into its 1-level two-dimensional DWT coefficients. Out of the four subbands, only the three high resolution detail subbands {LH, HL, HH} are selected.

Step 2: Fingerprint Preprocessing

A real fingerprint might have discontinuities that might lead to erroneous minutiae. Therefore, minutiae extraction is preceded by *fingerprint preprocessing*. This step involves normalization, ridge orientation and frequency estimation. Finally, the ridge orientation and frequency estimation values are used for filtering the fingerprint using Gabor wavelet. Gabor filtering enhances the ridges oriented in the direction of the local orientation, and decreases anything oriented differently. Hence, the filter increases the contrast between the foreground ridges and the background, whilst effectively reducing noise. The filtered output is then binarized and thinned to one-pixel width.

Step 3: Minutiae Extraction

Minutiae points such as end points and bifurcation points are identified by calculating *Crossing number (CN)* [22]. The

Crossing Number method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighbourhood of each ridge pixel using a 3×3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighbourhood.

$$CN = 0.5 \sum_{i=1}^8 |P_i - P_{i+1}|, \quad P_1 = P_9$$

where P_i is the pixel value in the neighborhood of a pixel P . For a pixel P , its eight neighboring pixels are scanned in an anticlockwise direction as follows:

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

After the CN for a ridge pixel has been computed, the pixel can then be classified according to the property of its CN value as shown in Table I.

TABLE I
CROSSING NUMBER (CN) VALUES DENOTING DIFFERENT TYPES OF
FINGERPRINT FEATURE PROPERTIES

CN	Property
0	Isolated point
1	Ridge Ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing points

Out of these, isolated points, and crossing points are unlike to occur in a natural fingerprint. Continuing ridge point cannot be categorized as a strategic location. The only minutiae of interest are ridge endings and bifurcation points (corresponding to $CN=1$ and $CN=3$ respectively). This operation is performed on a specific central region of interest to avoid errors from the boundary of fingerprint images. The minutiae thus extracted have the following information: x and y coordinates, orientation of ridge at that location and the type of minutiae (ending or bifurcation). Type of minutiae can already be set as 0 for ending and 1 for bifurcation, making it a binary format. The remaining three columns of the set of minutiae can be converted into binary form by 8-bit representation and a binary watermark is generated by concatenating the eight individual bit planes. The process of creation of binary watermark from minutiae points is shown in Fig. 3.

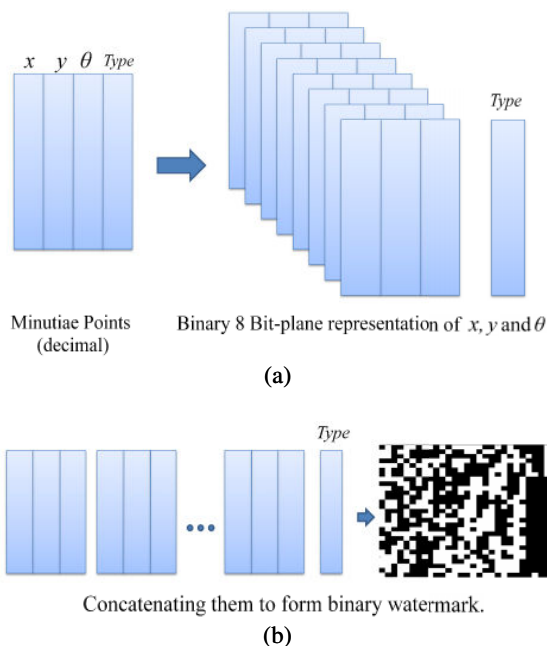


Fig. 3 Creation of binary watermark from (a) Conversion of minutiae points to binary 8-bit representation (b) Concatenation of binary bit planes of x , y , and θ and attaching the binary 'type' in the end

Step 4: Two uniformly distributed, highly uncorrelated, zero-mean, two-dimensional pseudorandom sequences (PN_0 and PN_1) of the size of sub-band matrix is generated for each bit of

the watermark image. The pseudorandom sequence PN_0 is used to embed the '0' watermark bit in the selected sub-band while PN_1 is used to embed the '1' watermark bit.

Step 5: Embed the PN sequences in the selected DWT sub-band using a *watermark amplification factor* K . Number of elements in the selected sub-band and PN sequence must be equal for embedding to take place. If we denote W_i as coefficients matrix of the selected subband, then embedding is done according to the equations as follows:

If the watermark bit is 0

$$I_{i,uv} = W_{i,uv} + K \cdot PN_{uv0} \quad \text{where } uv \in \{LH, HL, HH\} \quad (1)$$

Otherwise,

$$I_{i,uv} = W_{i,uv} + K \cdot PN_{uv1} \quad (2)$$

Step 6: Apply the inverse DWT repeatedly on the transformed image, including the modified sub-band, until the watermarked image is produced.

Peak Signal to Noise Ratio (PSNR) measures the perceptual quality of a watermarked image [23]. This is calculated as a performance metric and determines perceptual transparency of the watermarked image with respect to original host image.

$$PSNR = 10 \log \frac{MN \max_{x,y} P_{x,y}^2}{\sum_{x,y} (P_{x,y} - \bar{P}_{x,y})^2} \quad (3)$$

where

M and N are number of rows and columns respectively in the input image,

$P_{x,y}$ is the original fingerprint, and

$\bar{P}_{x,y}$ is the watermarked fingerprint.

B. Extraction procedure

The steps of minutiae watermark extraction are as follows:

Step 1: Apply 1-level DWT to the watermarked fingerprint. For performance evaluation of the scheme, this step can be preceded by attack on the image. This attack might be noise attack, geometrical distortion, filtering or compression attack.

Step 2: Select the sub-band into which the watermark was embedded.

Step 3: Regenerate the pseudorandom sequence (PN) using the same seed which was used in the watermark embedding procedure described above.

Step 4: Calculate the correlation between the selected watermarked sub-band and the generated pseudorandom sequence.

Step 5: Compare each correlation value with the mean correlation value. If the calculated correlation value is greater than the twice of the mean, then the extracted watermark bit will be taken as a '0', otherwise it is taken as a '1'. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered.

Step 6: Reconstruct the watermark image using the extracted watermark bits, and compute the similarity between the original and extracted watermarks using fitness function. This fitness function is defined as [16]

$$\text{Fitness of recovery } (p) = 100 \times \text{Correlation factor} \quad (4)$$

where correlation factor = cross-correlation coefficient between original watermark and extracted watermark.

Step 7: Minutiae points are then regenerated by stacking bit planes and converting them back to decimal system.

IV. MINUTIAE EMBEDDING/EXTRACTION RESULTS

The extraction has been tested under various noise attacks (salt & pepper, gaussian, speckle), geometrical distortion (scaling), low-pass filtering and JPEG compression attacks. The value of *amplification* or *gain* factor, "K" is changed linearly. For different values of K, the variations in transparency of watermarked fingerprint and robustness to attacks are analysed. The best output for optimum K with perfect recovery has been displayed for the three test watermarks. The main parameters as outputs are *PSNR* of watermarked image and *Fitness of recovery* of extracted watermark (with and without attack). The host image is a 388×374 indexed fingerprint image (Fig. 4(a)). The binary watermark as shown in Fig. 4(b) is formed from the minutiae details of the fingerprint as shown in Table II. Initial seed used a 35×1 vector. This scheme has been tested against a database [24] of eighty fingerprint images. The values have been recorded corresponding to biorthogonal CDF wavelet (9×7 filter) bank as it is found to be most suitable for image watermarking applications.

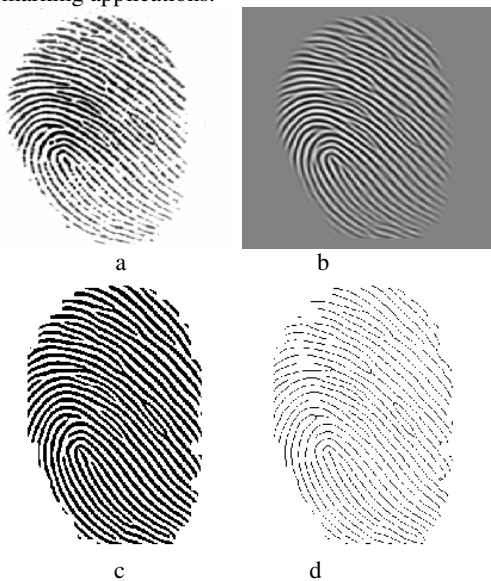


Fig. 4 Input Images (a) Original host fingerprint image (388×374) (b) Gabor filtered output (c) After binarization of Gabor filtered output (d) thinning of binarized output (e) Binary Watermark Label formed from minutiae points of (d)

TABLE II
MINUTIAE EXTRACTED FROM THE HOST FINGERPRINT IMAGE (SHOWN IN FIG. 4(A)) X AND Y ARE COORDINATES OF THE MINUTIAE POINT, ORIENTATION IS IN RADIANES AND TYPE DENOTES WHETHER MINUTIAE IS ENDING POINT (END) OR BIFURCATION (BIF)

X	Y	Orientation	Type
176	127	0.27098	BIF
257	171	0.78768	BIF
154	188	3.0269	BIF
285	215	0.79517	BIF
320	223	0.8684	BIF
320	271	0.86804	BIF
103	97	2.4783	END
102	98	2.42	END
164	135	0.21388	END
116	141	2.6459	END
217	168	0.72237	END
196	181	0.61064	END
170	190	0.27831	END
226	216	0.83156	END
153	218	2.2735	END
105	223	1.7164	END
169	233	1.1235	END
147	243	1.4793	END
186	251	1.0384	END
115	256	1.3264	END

A. Minutiae watermark embedding results

The watermarked images for all values of K (1 to 4) have been displayed in Table III. Table IV shows watermarked fingerprints for four other cover fingerprints from the test database [24].

TABLE III
WATERMARKED IMAGES WITH CORRESPONDING PSNR VALUES FOR
DIFFERENT VALUES OF K















 K=1 PSNR = 35.6 dB	 K=2 PSNR = 28.8 dB	 K=3 PSNR = 21.7 dB
 K=4 PSNR = 20.8 dB	 K=5 PSNR = 19.6 dB	 K=6 PSNR = 14.9 dB

TABLE IV
DIFFERENT WATERMARKED FINGERPRINTS WITH CORRESPONDING PSNR
VALUES FOR K=5

Input Fingerprint	Watermarked Fingerprint	PSNR (dB)
		25.54
		21.35
		22.27
		23.79

B. Minutiae watermark extraction results

Fig. 5 shows watermark extraction in the absence of any noise attack on the watermarked fingerprint. It is apparent that watermark recovery without noise attack is 100%. Number of errors in extracted minutiae points was found to be zero.

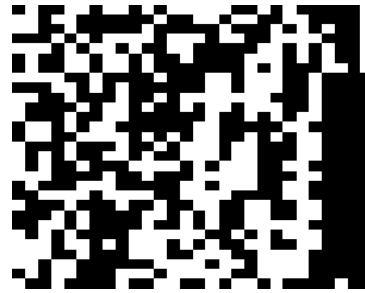


Fig. 5 Recovered Watermark (without attack), Fitness = 100%,
number of erroneous minutiae = 0

Table V shows experimentally calculated fitness values (ρ) of extracted watermark for various values of “K” and noise, scaling, low-pass filtering and JPEG compression attacks. It also shows number of erroneous minutiae points (Err) extracted for different watermarking weights.

TABLE V
FITNESS OF RECOVERY AND NUMBER OF ERRORS IN EXTRACTED WATERMARK
FOR ATTACKED WATERMARKED IMAGES FOR DIFFERENT VALUES OF
AMPLIFICATION FACTOR K

K		Salt & Pepper noise (density =0.04)	Gaussian noise (mean=0 variance =0.04)	Scaling (2:1:2)	Low pass filtering (5 × 5)	JPEG (Q=50)
1	ρ	93.56	89.41	75.45	99.5	95.51
	Err	9	12	21	1	5
2	ρ	95.34	92.35	83.56	99.5	96.35
	Err	5	8	16	1	4
3	ρ	100	94.24	90.35	100	98.23
	Err	0	6	10	0	2
4	ρ	100	97.88	97.62	100	99.5
	Err	0	3	3	0	1
5	ρ	100	98.91	98.42	100	100
	Err	0	2	2	0	0
6	ρ	100	99.76	99.42	100	100
	Err	0	1	1	0	0

C. Discussion

From the values of the fitness, it can be observed that

- K=1 and 2 do not give perfect extraction even for low degrees of noises. Lesser correlation values are obtained on scaling and JPEG compression attacks also.
- K=3 gives fair recovery for attacks other than the scaling attack.
- K=4 gives fair recovery for all the attacks but not perfect.
- K=5 and 6 gives very good fitness of recovered watermark for all kinds of attacks. For noise attacks and low pass filtering, the extraction is 100% or nearly 100%. Good robustness is observed against scaling and JPEG compression attack too. It is apparent that values of K=5 and K=6 are candidates for being the optimum

amplification values, as lower values of K give lesser fitness of correlation.

- Although it might be reckoned that $K=5$ gives PSNR values quite low (19.6 dB), the purpose of its use in fingerprint watermarking does not get defeated because the objective is authenticity check. The verification/identification processes are invariably followed by binarization which can eliminate the effect of watermarking up to $K=5$. $K=6$ is not chosen as the optimum value due to unacceptably low PSNR. This leaves $K=5$ as the optimum value for transparency-robustness trade-off.

V. PERFORMANCE EVALUATION

Fig. 6 shows variation of PSNR for three fingerprints from the database as K is increased.

The following points are apparent from the experimental results:

- All images show perceptibility degradation with increase in K . (Fig. 6).
- Perfect extraction of watermark has been observed for all values of K in the absence of attacks.
- The optimum value of amplification or gain factor, K was found to be 5 for salt and pepper noise density up to 0.04, Gaussian noise of zero mean and variance up to 0.04, scaling, low pass filtering (5×5) and JPEG compression up to quality 50. The scheme can be optimized for robustness-transparency trade-off for $K=5$ as it is found to give good recovery with all attacks.

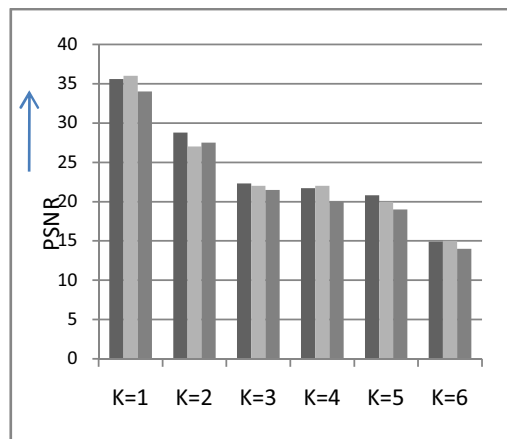


Fig. 6 Relationship between PSNR and K

VI. COMPARATIVE PERFORMANCE

The response of the proposed technique was tested for all the fingerprints of the database [24]. Table VI shows the fitness of recovery values obtained using the proposed

technique in comparison with that obtained using existing DCT-based watermarking technique [11]. It is observed that the performance of the DWT-based technique is better than the plain DCT-based technique in terms of correlation coefficients and erroneous minutiae for all the attacks. This can be explained due to the multiresolution property of DWT. Due to spatio-frequency resolution of DWT, it offers more degrees of freedom as compared with DCT. Furthermore, the computational cost for DWT is lower than that of DCT. The computational cost of DWT is $O(n)$, while that of DCT is $O(n \log(n))$, where n is the order of the transform input vector [17]. Since the computational cost of DWT is lower than that of DCT, the DWT-based fingerprint watermarking technique can be considered suitable to give noteworthy robustness.

TABLE VI
CORRELATION (%) AND NUMBER OF ERRORS IN EXTRACTED WATERMARK FOR ATTACKED WATERMARKED IMAGES USING PROPOSED DWT-BASED, EXISTING DCT-BASED AND SVD-BASED TECHNIQUES FOR $K=5$

Attacks	DWT		DCT [11]	
	ρ	Err	ρ	Err
Salt & pepper noise (density =0.04)	100	0	94.4	6
Gaussian noise (mean=0 variance =0.04)	98.1	2	95.3	5
Scale (2:1:2)	98.42	2	90.9	9
LPF (5×5)	100	0	89.5	12
JPEG (Q = 5)	100	0	99.9	1

VII. CONCLUSIONS

The proposed minutiae-watermarking scheme is found to be an efficient technique using DWT. The embedding/extraction for all images in the database have been achieved successfully and the watermarking scheme is found to give equally good results for all fingerprints in the database. It is experimented successfully for all possible cases – recovery under normal extraction and with noise attacks of varying degrees (gaussian, salt & pepper), geometrical distortion (scaling), low pass filtering and JPEG compression attacks. Since minutiae can be robustly extracted for even severely degraded watermarked fingerprints, this technique can be considered useful for secure transmission of fingerprint details over a channel. The purpose of the proposed watermarking scheme to extract minutiae from even tampered fingerprint is successfully met with good efficiency.

REFERENCES

- [1] S. Jain, "Digital watermarking techniques: A case study in fingerprints & faces" in *Proc. Indian Conference on Computer Vision, Graphics and Image Processing ICVGIP 2000*, pp. 139-144, 2000.

- [2] D. Mathivadhani, C. Meena, "A Comparative Study on Fingerprint Protection Using Watermarking Techniques," *Global Journal of Computer Science and Technology*, vol. 9, no. 5, pp. 98-102, 2010.
- [3] M. Vatsa, R. Singh, A. Noore, M. H. Houck, K. Morris, "Robust biometric image watermarking for fingerprint and face template protection," *IEICE Electronic Express* vol. 3, no. 2, pp. 23-28, 2006.
- [4] K. Zebbiche, F. Khelifi, "Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images," *International Journal of Digital Multimedia Broadcasting* 492942, 2008.
- [5] K. Hui, L. Jing, Z. Xiao-dong, Z. Xiao-xu, "Study on Implementation of a Fingerprint Watermark", in *Proc. International Conference on Computer Science and Software Engineering*, vol. 3, pp. 725-728, 2008.
- [6] V. Potdar, S. Han, E. Chang, "A Survey of Digital Image Watermarking Techniques", in *Proc. IEEE International Conference on Industrial Informatics*, pp. 709-716, 2005.
- [7] H. Fu, "Literature Survey on Digital Image Watermarking", *Lectures notes on EE381K Multidimensional Signal Processing*, 1998.
- [8] C.V. Serdean, M. Tomlinson, J. Wade, A.M. Ambroze, "Protecting Intellectual Rights: Digital Watermarking in the wavelet domain," *IEEE Int. Workshop Trends and Recent Achievements in IT*, pp. 16-18, 2002.
- [9] B. Furht, D. Kirovski, *Encryption and Authentications: Techniques and Applications*, USA: Auerbach, 2006.
- [10] I. J. Cox, J. Kilian, T. Leighton, T.G. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia", in *Proc. ICIP'97, USA*, vol. 6, pp. 1673- 1687, 1997.
- [11] S.D. Lin, Chin-Feng Chen, "A robust DCT-based watermarking for copyright protection", (2000) *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 415 - 421.
- [12] J. Delaigle, C. De Vleeschouwer, B. Macq, "Psychovisual Approach to Digital Picture Watermarking", *Journal of Electronic Imaging*, vol. 7, no. 3, pp. 628-640, 1998.
- [13] A. Grapahs, "An Introduction to Wavelets," *IEEE Computational Science and Engineering*, vol. 2, no. 2, pp. 50-61, 1995.
- [14] R.C. Gonzalez, R.E. Woods, *Digital Image Processing*. New Jersey: Prentice Hall, Upper Saddle River, 2002.
- [15] A. Abu-Erubb, A. Al-Haj, "Optimized DWT Based Image Watermarking," (2008) *Proc. IEEE First International Conference on Applications of Digital Information and Web Technologies*, pp. 1-6.
- [16] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking", (2007) *Journal of Computer Science*, vol. 3, no. 9, pp. 740-746.
- [17] R. Safabakhsh, S. Zaboli, A. Tabibiazar, "Digital Watermarking on Still Images Using Wavelet Transform," in *Proc. International Conference on Information Technology: Coding and Computing ITCC'04*, IEEE, 2004.
- [18] R. Chouhan, A. Mishra, P. Khanna, "Wavelet-based robust digital watermarking scheme for fingerprint authentication", *Proc. International Conference on Intelligent Computational Systems*, pp. 29-33, 2011.
- [19] F. Zhao, X. Tang, "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction," *Pattern Recognition*, vol. 40, pp. 1270 - 1281, 2007.
- [20] M. Kaur, M. Singh, A. Girdhar, P.S. Sandhu, "Fingerprint verification system using Minutiae extraction technique", *World Academy of Science, Engineering and Technology*, vol. 46, pp. 2008.
- [21] S. Bernard, N. Boujema, D. Vitale, C. Bricot, "Fingerprint Segmentation using the Phase of Multiscale Gabor Wavelets", in *Proc. 5th Asian Conference on Computer Vision*, Melbourne, Australia, January 2002.
- [22] S.A. Sudiro, M. Paindavoine, T.M. Kusuma, "Simple Fingerprint Minutiae Extraction Algorithm Using Crossing Number On Valley Structure," in *Proc. IEEE Workshop on Automatic Identification Advanced Technologies '07*, pp. 41 - 44, 2007.
- [23] F.A.P. Petitcolas, "Watermarking Schemes Evaluation", *IEEE Signal Processing Magazine*, vol. 17, pp. 58-64, 2000.
- [24] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*. Second ed., London: Springer, 2009, DB1_B set from FVC2000 and FVC2002 databases.



Rajlaxmi Chouhan received her Bachelor's degree (Hons.) in Electronics & Communication Engineering from Jabalpur Engineering College, Jabalpur, RGPV Bhopal (India) in 2009. She is currently pursuing Master of Technology in the field of image processing from Indian Institute of Information Technology, Design & Manufacturing Jabalpur, India. Her research interests include Image processing, Watermarking and Stochastic resonance-based image processing applications and Biometrics. She has over 8 publications in international conferences and journals and is a graduate student member of the IEEE Signal Processing Society.



Pritee Khanna is an Associate Professor in Computer Science & Engineering discipline, PDPM Indian Institute of Information Technology, Design & Manufacturing (IIITDM) Jabalpur, India. Dr. Khanna was awarded Ph.D. degree from Kurukshetra University, Kurukshetra, India in 2004. She has 20 publications in various journals and conferences. She also authored a book titled "Geometric Modelling of Statically and Dynamically Symmetric Patterns, Theory, Generation and Application". Her research interests include Computer Graphics, Image Processing, and Biometrics.