International Journal of Electrical and Computer Engineering (IJECE)
Vol.2, No.4, August 2012, pp. 523~528
ISSN: 2088-8708

Fingerprint Authentication by Wavelet-based Digital Watermarking

Rajlaxmi Chouhan*, Agya Mishra, Pritee Khanna*****
* Indian Institute of Technology Kharagpur (India)
** Jabalpur Engineering College, Jabalpur (India)
*** Indian Institute of Information Technology, Design & Manufacturing Jabalpur (India)

Article Info

Article history:
Received May 30, 2012
Revised Jul 10, 2012
Accepted Jul 16, 2012

Keyword:
Blind watermarking
Discrete wavelet transform
Fingerprint watermarking
PN sequence

ABSTRACT

In this manuscript, a wavelet-based blind watermarking scheme has been proposed as a means to provide protection against false matching of a possibly tampered fingerprint by embedding a binary name label of the fingerprint owner in the fingerprint itself. Embedding watermarks in the detail regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. It has been experimentally shown that when a binary watermark is embedded into detail coefficients of an indexed fingerprint image in a spread spectrum fashion, the perceptual invisibility and robustness have anticlinal response to change in amplification factor "K" and smaller watermarks have better transparency than the larger ones. The DWT-based technique has been found to give better robustness against noises, geometrical distortions, filtering and JPEG compression attack than other frequency domain watermarking techniques.

Corresponding Author:
Rajlaxmi Chouhan,
Departement of Electronics and Electrical Communication Engineering,
Indian Institute of Technology Kharagpur
Kharagpur WB India 721302
Email: rajlaxmi.chouhan@gmail.com

1. INTRODUCTION

Fingerprints are unique biometrics mainly used for the establishment of instant personal identity but they are susceptible to accidental/intentional attacks. Protection of biometric data is one of the most important concerns these days and therefore it is gaining interest among researchers. 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. Thus, a defensive scheme is needed which will preserve fidelity and prevent modifications [3-5].

Digital watermarking is a process of embedding an invisible structure, called digital watermark, into a host signal to mark its ownership [4-5]. In such an application a serial number is embedded into the signal to protect, and also to identify the copyright holder. The objective of the scheme is to perform an authenticity check.

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]. 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].

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]. Here, if due to some incidental/intentional tampering, the received fingerprint is falsely matched to someone

else, the extracted watermark plays the role of a scrutinizer that can be used to check whether the fingerprint received is of the same person whose label it holds or not. The present work addresses the issue of watermarking of fingerprints and proposes a robust watermarking scheme for the same.

Digital watermarking research, at present, primarily involves the identification of effective signal processing strategies to discreetly, robustly, and unambiguously hide the watermark information into multimedia signals [6-7]. The general process involves the use of a key which must be used to successfully embed and extract the hidden information. 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. In a blind watermarking scheme, the original signal is not required during the detection process of the watermark. The key or the seed, which is typically used to generate some random sequence used during the embedding process, is required solely. Blind watermarking schemes can be applied in biometric data communication where the host image is the main biometric data to be transmitted and the watermark can be some identification of the owner of that biometric data. The majority of the frequency domain watermarking schemes modifies the transformed coefficients based on the bits of watermark image.

Early work on digital watermarking for still images focused on information hiding in the spatial domain [8]. Recent efforts are mostly based on frequency-domain techniques [9-11]. Discrete Cosine Transform (DCT) based technique proposed by Lin et al. [9] addresses the watermark embedded at low frequency. The weighted correction is also used to improve the imperceptibility of the watermark. In particular, digital image watermarking algorithms which are based on the discrete wavelet transform have been widely recognized to be more prevalent than others. A wavelet based technique proposed by Abu-Errub et al. [10] uses optimization and genetic algorithm for spread spectrum watermarking. A combined Discrete Wavelet Transform (DWT) and DCT technique proposed by Al-Haj [11] performs multilevel wavelet decomposition followed by DCT of second level details.

With its suitability to model the Human Visual System [12-13] behavior and its multiresolution properties, the DWT has gained interest among watermarking researchers, as it is witnessed by the number of algorithms following this approach that have been proposed over the last few years [14-17]. A wavelet based watermarking technique exhibiting unobtrusiveness and robustness has been discussed for Intellectual Property Rights protection [14]. This is due to the wavelets' excellent spatial localization, frequency spread, and multi-resolution characteristics, which are very much similar to the theoretical models of the human visual system.

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, a wavelet-based, blind and robust digital watermarking technique for fingerprints authentication has been presented in this manuscript. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. This motivation had led us to the extension of our earlier work on fingerprint watermarking [18].

2. DISCRETE WAVELET TRANSFORM

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple “scale” wavelet decomposition [13, 16].

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 [17]. 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 [9, 15].

Most of earlier watermarking work concentrated in the cosine domain. However, DWT offers many advantages over DCT due to absence of the annoying blocking artefacts associated with the DCT as it is a block-based transform [17]. It also provides better energy compaction than both the FFT and DCT in the

sense that it is closer to the optimal Karhunen-Love transform. Taking into account the advantages of DWT to ensure robust data hiding, it has been explored in this manuscript for embedding of binary labels.

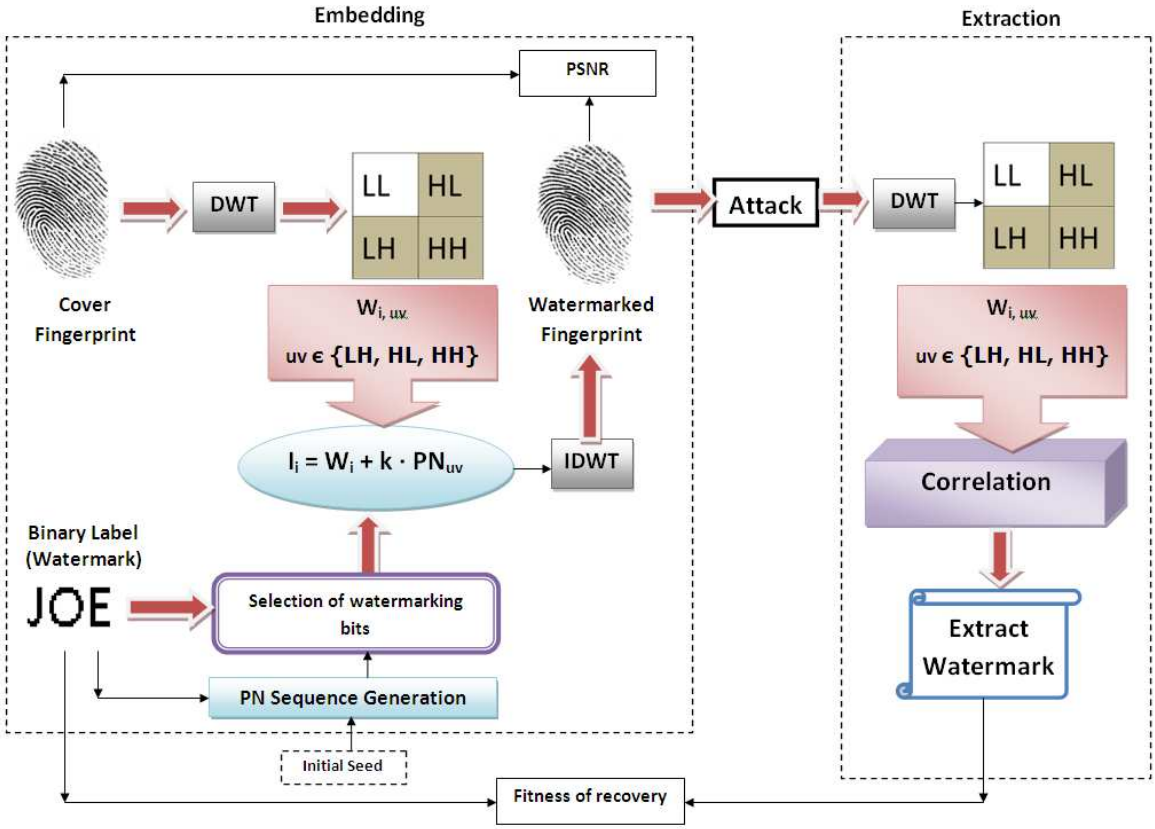


Figure 1 Watermark embedding and extraction algorithm

3. PROPOSED WATERMARKING SCHEME

The proposed watermarking scheme has been shown in Figure 1. The scheme has been divided into two sections: Embedding and Extraction.

3.1. Embedding procedure

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: A uniformly distributed, highly uncorrelated, zero-mean, two-dimensional pseudorandom sequence (PN) [8, 15] of the size of sub-band matrix is generated for each bit of the watermark image. This pseudorandom sequence is used to embed the zero watermark bit in the selected sub-band.

Step 3: Embed the PN sequence in the selected DWT sub-band with 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 Wi as coefficients matrix of the selected subband, then the embedding is done according to the equations (1) and (2).

If the watermark bit is 0, then

$$I_{i,uv} = W_{i,uv} + K.\, PN_{uv} \quad where\ uv\ \varepsilon\ \{LH,HL,HH\} \tag{1}$$

otherwise,

$$I_{i,uv} = W_{i,uv} \tag{2}$$

Step 4: 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 quality of a watermarked image [16]. PSNR is calculated as a performance metric which determines perceptual transparency of the watermarked image with respect to the original host image (in decibels).

$$PSNR = \frac{MN \max_{x,y} P_{x,y}^2}{\sum_{x,y} \left(P_{x,y} - \overline{P}_{x,y}\right)^2} \quad (3)$$

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

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

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

3.2. Extraction procedure

Step 1: Apply 1-level DWT to the watermarked image. For performance evaluation of the scheme, this step can be preceded by attack on the image. This attack can be JPEG, geometrical, and Gaussian noise or other kinds of noises.

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 value is greater than twice 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 here has been defined as [17, 19]

$$Fitness\ of\ recovery = 100 \times Correlation\ factor \quad (4)$$

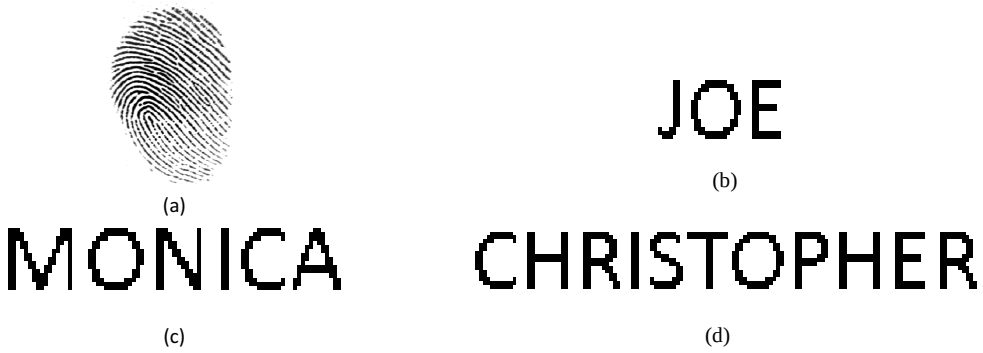
where correlation factor is the correlation between original watermark and extracted watermark.

4. EXPERIMENTAL SETUP

The outputs of the proposed watermarking scheme have been shown here for varying parameters. The value of amplification or gain factor, "K" is changed linearly. For different values of K, the variations in transparency of watermarked image and robustness to attack are analyzed. 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; Fitness of recovery of extracted watermark (with and without attack) and time elapsed in computations. Their values have been recorded and analyzed.

The host image is a 388 × 374 indexed fingerprint image. The watermarks used are binary labels of variable length and fixed width (20 pixels) carrying names. In a real-world application, this could be the identification name/number of the person whose fingerprint the host image is. Initial seed used a 35 ×1 vector. This scheme has been tested against a database of eighty fingerprint images [20] and twelve watermarks (name labels) of variable lengths. The best output results for three binary name labels have been included here for extraction, before and after noise attacks. The watermarked images are subjected to three kinds of attacks – Noise (Gaussian, Speckle and Salt & Pepper), Geometrical Distortion (cropping and scaling), JPEG Compression, and Low-pass filtering attack (LPF). The output parameters for best results have been mentioned along with the output images. The values have been recorded corresponding to the "Haar" wavelet as it is the first and the simplest in the wavelet families.

One of the host (cover) fingerprint image and watermark labels – small, medium and large size (input images) have been shown in Figure 2.



(a) (b) (c) (d)

Figure 2 Input Images (a) Original host fingerprint image (388 × 374) (b) Small Binary Watermark Label (38 × 20 pixels) (c) Medium-sized Binary Watermark Label (88 × 20 pixels) (d) Large-size Binary Watermark Label (140 × 20 pixels)

5. WATERMARK EMBEDDING RESULTS

The watermarked images for all values of K (1 to 4) have been displayed in Table 1. Table 2 shows watermarked fingerprints for four other cover fingerprints along with their respective PSNR values.

Table 1. Watermarked images with corresponding *PSNR* values for different watermark labels

K	1	2	3	4
Watermarked Image for 38 × 20 Binary Label	*PSNR* = 983.7737	*PSNR* = 245.9434	*PSNR* = 109.3082	*PSNR* = 61.5
Watermarked Image for 88 × 20 Binary Label	*PSNR* = 431.2972	*PSNR*= 107.8243	*PSNR*= 47.9219	*PSNR*= 26.9561
Watermarked Image for 140 × 20 Binary Label	*PSNR*= 247.4106	*PSNR* = 61.8527	*PSNR* = 27.4901	*PSNR* = 15.4632

Table 2. Different watermarked fingerprints with corresponding PSNR values for medium sized watermark label (88×20) and K=3

Input Fingerprint				
Watermarked Fingerprint				
***PSNR* (dB)**	76.57	65.55	70.32	69.63

6. WATERMARK EXTRACTION RESULTS

Figure 3 shows watermark extraction results when no noise attacked the watermarked image. It is apparent that watermark recovery without noise attack is 100%.

(a) (b) (c)

Figure 3 Recovered Watermarks (without attack) for three binary labels (a) Small (38 × 20) (b) Medium-sized (88 × 20) (c) Large-sized (140 × 20)

6.1. Watermark Extraction Results (for all values of K)

Table 3 shows experimentally calculated fitness values of extracted watermark for various values of "K" and noise, geometric distortion (cropping, scaling), JPEG compression and filtering attacks.

6.2. Discussion

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

- K=1does not give perfect extraction even for low degrees of noise. Lesser correlation values are obtained for K=1 on cropping and JPEG compression attacks also.
- K=2 gives fair recovery for attacks but not perfect.
- K=3 and 4 gives very good fitness of recovered watermark for all kinds of attacks. For noise attacks, the extraction is 100%. For cropping attack, up to area of 25% perfect extraction of watermark is observed for smaller watermarks while nearly perfect recovery for larger watermarks. Good robustness is observed against JPEG compression, scaling and low pass filtering attack too. It is apparent that values of K=3 and K=4 are candidates for being the optimum amplification values as lower values of K give lesser fitness of correlation for all sized name labels.

Table 3. Fitness of recovery of extracted watermark for attacked watermarked images for different degrees of attacks and values of K

K	Noise Type	38 × 20 Watermark	88 × 20 Watermark	140 × 20 Watermark
1	Salt and Pepper density=0.01	99.6302	98.8589	98.8616
	Speckle Noise var= 0.04	99.2623	77.4866	81.2594
	Gaussian Noise SNR= 50	95.6966	92.5596	93.1007
	JPEG (Quality 5)	95.3984	94.3588	94.3102
	Cropping (25%)	97.3234	97.2356	95.7724
	Scaling (2:1:2)	98.3234	97.9738	97.3912
	LPF (3 × 3)	98.1037	97.2934	97.0124
2	Salt and Pepper density=0.02	100.0000	100.0000	100.0000
	Speckle Noise var= 0.04	99.2623	99.3562	98.4705
	Gaussian Noise SNR= 50	100.0000	99.8382	99.7137
	JPEG (Quality 5)	96.3254	95.3425	95.0285
	Cropping (25%)	99.2355	99.1264	99.2345
	Scaling (2:1:2)	95.5354	95.0545	94.2019
	LPF (3 × 3)	99.9102	99.0293	98.0013
3	Salt and Pepper density 0.05	**100.0000**	**100.0000**	**99.9999**
	Speckle Noise var= 0.04	**100.0000**	**100.0000**	**99.9999**
	Gaussian Noise SNR = 30	**100.0000**	**100.0000**	**100.0000**
	JPEG (Quality 5)	**98.9889**	**97.6128**	**97.7550**
	Cropping (25%)	**100.0000**	**100.0000**	**99.9998**
	Scaling (2:1:2)	**96.6222**	**95.8354**	**95.0345**
	LPF (3 × 3)	**100.00**	**99.9984**	**98.1553**
4	Salt and pepper density= 0.10	100.0000	100.0000	99.9999
	Speckle noise var=0.08	100.0000	100.0000	99.9999
	Gaussian noise SNR=20	100.0000	100.0000	100.0000
	JPEG (Quality 5)	99.4565	98.1245	98.8385
	Cropping (25%)	100.0000	100.0000	100.0000
	Scaling (2:1:2)	100.0000	100.0000	99.9989
	LPF (3 × 3)	100.0000	100.0000	100.0000

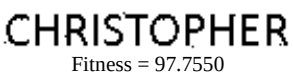
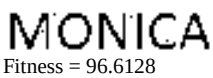
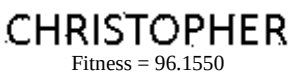
- Although it might be reckoned that K=3 gives PSNR values quite low (109.3 for smallest name label to 27.49 for longest label) the purpose of its use in fingerprint watermarking does not get defeated because the objective is authenticity check. The verification/identification processes are invariably followed by binarization which can eliminate the effect of watermarking up to K=3. K=4 is not chosen as the optimum value due to unacceptably low PSNR. This leaves K=3 as the optimum value for transparency-robustness trade-off. This is validated by results shows in Table 2.
- It is also apparent from Table 3 that the PSNR values (perceptual quality) deteriorate as the size of binary label is increased for all values of amplification factor K.

6.3. Watermark Extraction Results (Best outputs for K=3)

Recovered watermarks for best and optimum results (for K=3) have been shown in the Table 4. For K=3, the watermarking scheme gives 100% recovery of watermark when subjected to salt and pepper noise attack up to density 0.05 for all name labels of length 3-11 letters or 38-140 pixels. It also gives 100% recovery for speckle noise variance up to 0.04, additive white Gaussian noise with SNR above 30 and cropping attacks. Good results are obtained even in scaling by factor 2 and low pass filtering attacks.

Hence, as per the experimental results, optimum value of amplification factor (watermarking weight) is found to be K=3 for binary labels of all lengths.

Table 4 Extracted watermarks and their corresponding fitness of recovery for K=3 (optimum outputs)

Noise Type	38 × 20 Watermark	88 × 20 Watermark	140 × 20 Watermark
Salt and Pepper Density = 0.05	 Fitness = 100	 Fitness= 100	 Fitness = 99.99
Speckle Noise Variance=0.04	 Fitness = 100	 Fitness= 100	 Fitness= 99.99
Gaussian Noise SNR = 30	 Fitness = 100	 Fitness= 100	 Fitness = 100
JPEG Compression (Quality = 5)	 Fitness= 98.9899	 Fitness = 97.6128	 Fitness = 97.7550
Cropping (25%)	 Fitness = 100	 Fitness= 100	 Fitness = 99.99
Scaling (2:1:2)	 Fitness= 97.9899	 Fitness = 96.6128	 Fitness = 96.1550
Low pass mean filtering (3 × 3)	 Fitness = 100	 Fitness= 100	 Fitness = 99.99

7. QUANTITATIVE PERFORMANCE EVALUATION

Figure 4 shows variation of PSNR for three watermarks as K is increased. Tables 5-6 and Figure 5-6 show computation times for various embedding and extraction under noise attack for values of K varying from 1 to 4 respectively. The contrast between time of computation for small and large watermarks for all processes is clearly visible. The points which are apparent from the experimental results are summarized here.

7.1. Time complexity

- Smaller watermarks are processed in times much less than what is required for larger watermarks.
- Extraction process is found to take almost similar or less than the time required for embedding.

7.2. Response to Amplification factor

- All images show perceptibility degradation with increase in K. However, for larger watermarks, this change is very gradual and mild even though the values of PSNR for smaller logo changes more abruptly (Figure 4).
- Without any noise attacks perfect extraction of watermark was observed for all values of K.
- The optimum value of amplification or gain factor, K was found to be 3 for salt and pepper noise density up to 0.05, speckle noise variance up to 0.04 and Gaussian noise attack for SNR greater than or equal to 30. The scheme can be optimized for robustness-transparency trade-off for K=3 as it is found to be give good recovery with all noise attacks.

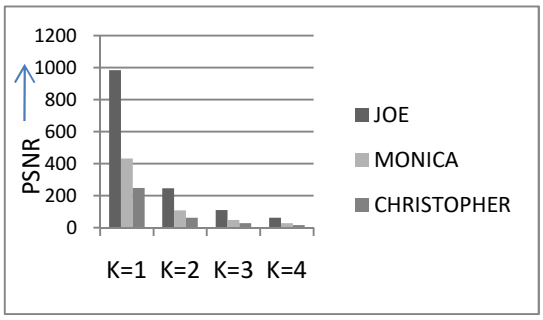


Figure. 4 Relationship between PSNR and K

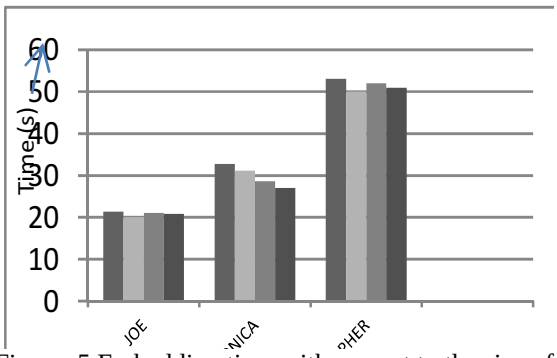


Figure. 5 Embedding time with respect to the size of watermark for each value of K

Table 5 Average Embedding Time for Different Watermarks and K

Watermark name label	Average time taken for embedding (seconds)			
	K=1	K=2	K=3	K=4
JOE	21.4	20.1	21	20.9
MONICA	32.7	31.2	28.6	27
CHRISTOPHER	53.1	50	52	51

Table 6. Extraction time with respect to different types of noises for each watermarks

Watermark name label	Average time taken for extraction (seconds)			
	Without noise	Salt and pepper noise attack	Cropping	JPEG Compression
JOE	16	17	19	15
MONICA	26.2	30	31	28
CHRISTOPHER	43.1	42	44	42

8. COMPARATIVE PERFORMANCE

The response of the proposed technique was tested for all the fingerprints of the database [20] and compared with existing DCT-based and hybrid transform DWT-DCT based watermarking techniques [9, 11]. Table 7 shows the fitness of recovery values obtained (on medium-sized binary label) using the proposed technique in comparison with those obtained using existing frequency domain techniques [9, 11]. It is observed that the performance of the DWT-based technique is better than the plain DCT-based technique.

The fitness obtained using the proposed technique is comparable to that obtained using hybrid DWT-DCT. Due to its multiresolution property, DWT 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. Since the computational cost of DWT is lower than that of DCT or hybrid DCT, the DWT-based fingerprint watermarking technique can be considered suitable to give noteworthy robustness.

Table 7. Comparison of fitness of recovery of proposed technique with other frequency domain watermarking techniques for various attacks

Noise Type	Proposed Technique	DCT [9]	DWT-DCT [11]
Salt and Pepper Density 0.05	100.00	95.34	100.00
Speckle Noise Variance =0.04	100.00	96.76	99.99
Gaussian Noise SNR = 30	100.00	95.68	100.00
JPEG Compression (Quality = 5)	97.62	84.78	97.52
Cropping (25%)	100.00	89.63	99.95
Scaling (2:1:2)	96.62	92.36	97.00
Low pass mean filtering (3 × 3)	100.00	90.08	98.97

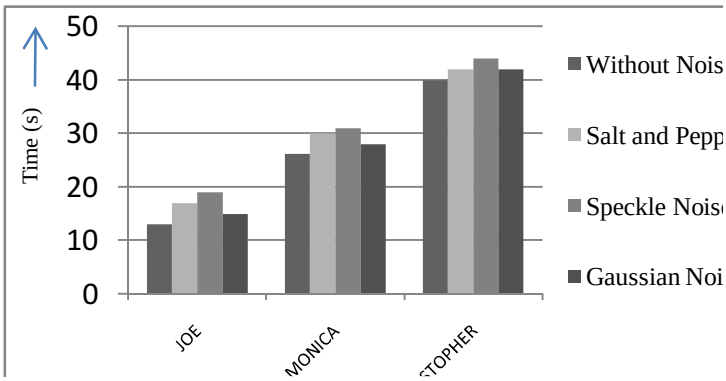


Figure 6. Extraction time with respect to different noise attacks for each watermark

9. CONCLUSIONS

The presented digital watermarking scheme which is based on wavelet is found to be an efficient for authentication of fingerprint images. It is found to give equally good results for all fingerprints in the database for all possible cases – recovery under normal extraction and with noise attacks of varying degrees (gaussian, speckle, salt & pepper), geometrical distortion (cropping, scaling), JPEG compression, and filtering (mean) attacks. Since extracted watermark holds the identity of the fingerprint owner, it can be used to check whether the fingerprint received belongs to him/her or not by matching the extracted name label with the identity of the person. Hence, the purpose of this watermarking scheme of detecting a false match due to a tampered fingerprint is met with good efficiency. Comparison with existing techniques validates the performance of the proposed technique, which is better than DCT based and comparable with hybrid DWT-DCT technique. This technique may be considered suitable for fingerprint watermarking using binary labels having dimensions from (38-140) × 20. This scheme can be further extended for watermarking of various other identification codes like minutiae details of fingerprints.

REFERENCES

[1] S. Jain, "Digital watermarking techniques: A case study in fingerprints & faces" (2010), Proc. Indian Conference on Computer Vision, Graphics and Image Processing ICVGIP (2000), pp. 139-144.
[2] D. Mathivadhani, C. Meena, "A Comparative Study on Fingerprint Protection Using Watermarking Techniques," (2010) Global Journal of Computer Science and Technology, vol. 9, no. 5, pp. 98-102.
[3] M. Vatsa, R. Singh, A. Noore, M. H. Houck, K. Morris, "Robust biometric image watermarking for fingerprint and face template protection", (2006) IEICE Electronic Express vol. 3, no. 2, pp. 23-28.
[4] K. Zebbiche, F. Khelifi, "Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images", (2008) International Journal of Digital Multimedia Broadcasting 492942.
[5] K. Hui, L. Jing, Z. Xiao-dong, Z. Xiao-xu, "Study on Implementation of a Fingerprint Watermark", (2008) Proc. International Conference on Computer Science and Software Engineering, vol. 3, pp. 725-728.

[6] V. Potdar, S. Han, E. Chang, “A Survey of Digital Image Watermarking Techniques”, (2005) Proc. IEEE International Conference on Industrial Informatics, pp. 709-716.
[7] H. Fu, “Literature Survey on Digital Image Watermarking”, Lectures notes on EE381K Multidimensional Signal Processing, 1998.
[8] J. Cox, J. Kilian, T. Leighton, T.G. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia”, (1997) Proc. International Conference on Image Processing (ICIP 1997), vol. 6, pp. 1673- 1687.
[9] 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.
[10] Abu-Errub, 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.
[11] Al-Haj, "Combined DWT-DCT Digital Image Watermarking", (2007) Journal of Computer Science, vol. 3, no. 9, pp. 740-746.
[12] J. Delaigle, C. De Vleeschouwer, B. Macq, “Psychovisual Approach to Digital Picture Watermarking”, (1998) Journal of Electronic Imaging, vol. 7, no. 3, pp. 628-640.
[13] R.C. Gonzalez, R.E. Woods, Digital Image Processing. New Jersey: Prentice Hall, Upper Saddle River, 2002.
[14] C.V. Serdean, M. Tomlinson, J. Wade, A.M. Ambroze, “Protecting Intellectual Rights: Digital Watermarking in the wavelet domain,” (2002) IEEE Int. Workshop Trends and Recent Achievements in IT, pp. 16-18.
[15] Furht, D. Kirovski, Encryption and Authentications: Techniques and Applications. USA: Auerbach, 2006.
[16] Graphs, “An Introduction to Wavelets,” (1995) IEEE Computational Science and Engineering, vol. 2, no. 2, pp. 50-61.
[17] R. Safabakhsh, S. Zaboli, A. Tabibiazar, “Digital Watermarking on Still Images Using Wavelet Transform,” (2004) Proc. IEEE International Conference on Information Technology: Coding and Computing ITCC’04, vol.1, pp. 671-675.
[18] R. Chouhan, A. Mishra, P. Khanna, “Wavelet-based robust digital watermarking scheme for fingerprint authentication”, (2011) Proc. International Conference on Intelligent Computational Systems (ICICS), pp. 29-33.
[19] F.A.P. Petitcolas, “Watermarking Schemes Evaluation”, (2000) IEEE Signal Processing Magazine, vol. 17, pp. 58-64.
[20] 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.

BIOGRAPHIES OF AUTHORS

Rajlaxmi Chouhan received her Bachelor's degree in Electronics & Communication Engineering (ECE) from Rajiv Gandhi Technical University Bhopal (India) in 2009, and Master in Technology in ECE from Indian Institute of Information Technology, Design & Manufacturing Jabalpur in 2011. She is currently a research scholar at the Indian Insitute of Technology Kharagpur. Her research interests include image enhancement, image watermarking and stochastic resonance-based image processing applications. Miss Chouhan has 15 research publications in international conferences and journals. She is a graduate student member of the IEEE Signal Processing Society and IEEE Women in Engineering.

Agya Mishra received her B.E in Electronics and Communication Engineering, from Government Engineering college Ujjain, India, M.Tech. in Digital Communication from Maulana Azad National Institute of Technology, Bhopal, India and pursuing PhD from MANIT Bhopal India. She is Assistant Professor in Jabalpur Engineering College, Jabalpur, India. She has over 20 publications in international journals and conferences. Her fields of interest are Statistical signal and Digital signal processing, Digital image processing, computational intelligence.

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.