Sparse Watermarking Technique for Improving Security of Fingerprint Biometric System

ROHIT THANKI[1], KOMAL BORISAGAR[2]
[1]Research Scholar, Faculty of Technology & Engineering, C U Shah University, Wadhwan
[2]HOD & Associate Professor, EC Department, Atmiya Institute of Technology & Science, Rajkot
INDIA
rohitthanki9@gmail.com[1], krborisagar@aits.edu.in[2]

Abstract: - Any biometric system is vulnerable against various attacks. One of the attacks is on the communication channel between the system database and matcher module of the biometric system. Therefore, this study proposed a fragile sparse biometric watermarking technique based on compressive sensing theory for security against this kind of attack. In this proposed sparse watermarking technique, watermark fingerprint template is converting into sparse measurements using compressive sensing theory and embeds these sparse measurements of fingerprint template into standard image. The structural similarity measure index (SSIM) quantity measure is used for authentication between original watermark fingerprint image and reconstructed watermark fingerprint image. The experimental results show that proposed sparse biometric watermarking technique does not affect verification and authentication performance of fingerprint biometric system. The results also show that proposed sparse biometric watermarking technique having a good performance compare to the existing watermarking techniques in the literature.

Key-Words: - Biometric System, Compressive Sensing, DWT, FAR, Fingerprint, FRR, SSIM, Sparse Biometric Watermarking.

1 Introduction

Nowadays, biometric authentication based system is used for recognition of person automatically. This biometric system having many advantages compare to traditional biometric system like I-card, password etc. (Jain & Kumar, 2012). However, this biometric system has vulnerable in various attacks like spoofing at system database, stone of biometric template at communication channel, modification of module of system and noise in sensor etc. (Jain & Kumar, 2012; Jain, Ross & Kumar, 2006). Digital watermarking is one of the solution for attacks like spoofing at system database, stone of biometric template at communication channel of biometric system (Jain & Uludag, 2003).

However, digital watermarking techniques have some limitation such as less payload capacity and less computational security (Langelaar, Setyawan & Lagnedijk, 2000). To overcome to the limitation such as less computational security, researcher introduces sparse domain watermarking technique based on compressive sensing theory (Sheikh and Baraniuk, 2007). In sparse domain watermarking technique, used sparseness property provide by compressive sensing (CS) theory and used this theory for generation of sparse watermark information and this sparse watermark information is embedded into host medium. In last eight years, many researchers are proposed various sparse domain watermarking techniques based on compressive sensing (CS) theory (Raval et al., 2011). These watermarking techniques are used for improving payload capacity and detection of image tampering.

The concept of watermarking technique using compressive sensing (CS) theory is given by Sheikh and its research team (Sheikh & Baraniuk, 2007). In this technique, $y = Af + e$ be the transform domain watermarked signal is generated during encoding process, where f is the spread spectrum watermark sequence, A is a random measurement matrix and e is the sparse transform domain vector for the host signal. For decoding process, first detect, sparse transform domain signal e which is subtracted from y and the result of this operation is multiplied by the inverse of A to get the watermark.

Meanwhile F. Tiesheng et al. (2013) as described a watermarking technique based on compressive sensing theory which includes compressive sensing acquisition and compressive sensing reconstruction process. This technique is found more robust and secure against different attacks. M. Waleed Fakhr (2012) as described a compressive sensing based robust audio watermarking technique and gives

comparison against various attacks like MP3 audio compression and additive noise. Besides M. Raval et al. (2011) as described a fragile watermarking technique using compressive sensing (CS) theory for reducing dimension and improved security of image against tampering.

Furthermore X. Zhang et al. (2011) as described a watermarking technique with flexible self-recovery quality based on compressive sensing and Discrete Cosine Transform (DCT). In this technique, extracted watermark data is used for tamper identification of image. Besides M. Tagliasacchi et al. (2009) as described a fragile watermarking technique based on compressive sensing (CS) theory for sparse image tampering identification.

Furthermore various watermarking techniques are described by researchers for protection of biometric templates. V. Inamdar and P. Rege (2014) as described a dual watermarking technique using multiple biometric watermarks for copyright ownership using compressed speech signal and Gabor features of face embedded into standard host image. This proposed technique is found robust under various watermarking attacks. A. Kothari and V. Dwivedi (2011) as described a watermarking techniques using correlation properties of PN sequence and discrete wavelet transform for copyright protection of videos.

V. Inamdar et al. (2010) (Inamdar, Rege & Arya, 2010) as described a blind biometric watermarking scheme for handwritten signature using Biorthogonal wavelet transform where second level details coefficients of wavelet transform of host image is modified accord to watermark image bit. The authors also described signature template matching procedure for authentication of extracted signature watermark data with signature data base. A. Noore et al. (2007) as described digital watermarking technique based on discrete wavelet transform for embedding selected facial image and corresponding texture information into selected texture region of fingerprint image. The authors claim that watermarking technique is improved visual capacity and security of automatic fingerprint identification system because retrieving two information like facial and texture information.

This study has proposed sparse biometric watermarking technique for biometric template tamper identification and improving security of biometric template using compressive sensing (CS) theory because of in existing watermarking techniques in literature which is used for tamper identification of standard image and in these watermarking techniques, direct biometric template is embedded into host image without any preprocessing which create problem of security of biometric template against spoofing or modification attack at communication channel. Therefore in this study, we have proposed a fragile sparse biometric watermarking technique based on sparseness provided by Discrete Cosine Transform (DCT) (Jain, 1989), Discrete Wavelet Transform based watermarking (Raval & Rege, 2002) and Compressive Sensing (CS) theory procedure (Candès, 2006; Baraniuk, 2007).

In this proposed sparse watermarking technique, we have encrypted fingerprint biometric template into sparse measurements using compressive sensing (CS) theory acquisition procedure. These sparse measurements of fingerprint template are generated using Discrete Cosine Transform (DCT) and random measurement matrix. Then these sparse measurements of fingerprint template are embedding into approximation wavelet coefficients of standard image to generate watermarked image. At decoder side, we have extracted these sparse measurements of fingerprint template from watermarked image and reconstructed fingerprint template image from extracted sparse measurements using compressive sensing (CS) theory recovery procedure. This reconstructed fingerprint template image is compared with original fingerprint image for recognition of person based on matching results of comparison.

The rest of paper is organized such that next section gives proposed sparse watermarking technique then dataset preparation information, and experimental results. Finally gives conclusions on proposed sparse watermarking technique.

2 Proposed Sparse Watermarking Technique

Proposed sparse watermarking technique is based on combination of compressive sensing acquisition and recovery procedure (Candès, 2006; Baraniuk, 2007) and wavelet domain based watermarking approach. The block diagram of proposed sparse watermarking technique is given in Figure 1. This watermarking technique is dividing into five procedures such as watermark preparation using compressive sensing (CS) theory, watermark embedding, watermark extraction, watermark reconstruction using recovery process of compressive sensing (CS) theory and template matching for personal recognition.

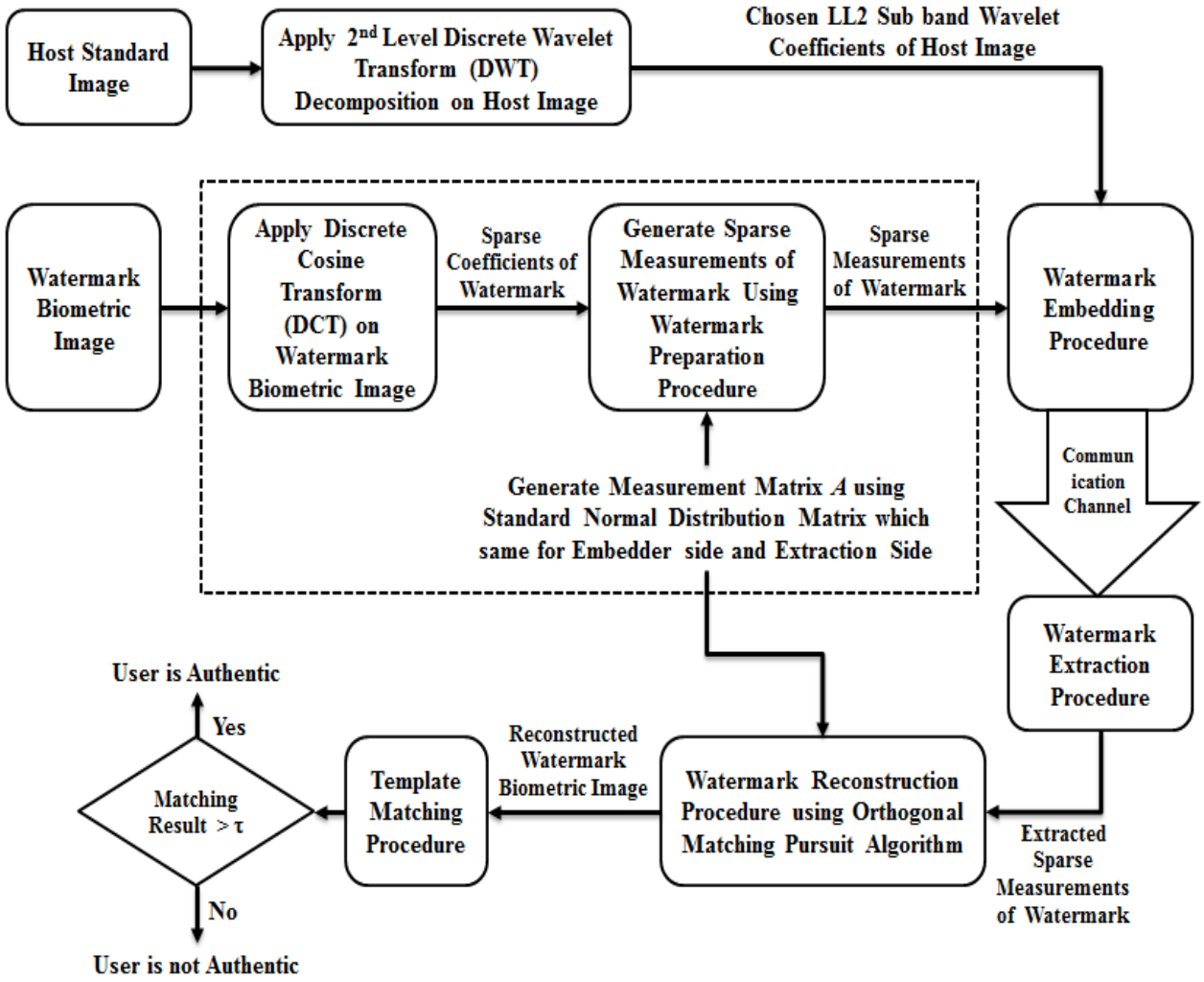


Fig.1. Block Diagram of Proposed Sparse Watermarking Technique

2.1 Watermark Preparation Using CS Theory

The watermark preparation using compressive sensing (CS) theory acquisition procedure steps are described below. In Figure 1, dotted box is shows procedure for watermark preparation using CS theory.

1. Take watermark biometric image and apply the Discrete Cosine Transform (DCT) on it and converting watermark biometric image into DCT coefficients.
2. Then, these DCT coefficients of watermark biometric image is taken as sparse coefficients and denoted as x. This step is necessary because of image must sparse when compressive sensing (CS) theory is apply on it.
3. Measurement matrix A is generated using standard normal distribution matrix with mean = 0 and variance =1 which is same for embedder and detector.
4. Generate sparse measurements y of watermark biometric image by multiplication of sparse coefficients x and measurement matrix A.

$$y = A \times x \tag{1}$$

In equation 1, y = *S*parse Measurements of Watermark Biometric Image; A = Measurement Matrix; x = Sparse Coefficients
5. Then, these sparse measurements of watermark biometric image are used as watermark information and denoted as W_{Sparse}.

2.2 Watermark Embedding Procedure

The proposed watermark embedding steps are given below:

1. Take standard image as host image and compute size of image.
2. Apply 2nd level Discrete Wavelet Transform (DWT) on host image and convert into various sub bands such as LL2, HL2, LH2 and HH2. Here we have chosen approximation wavelet coefficients (LL2) of 2nd level DWT decomposition because of size of LL2 sub band

is equal to size of sparse measurements watermark biometric image and easy to perform embedding process. The used of HL2, LH2 and HH2 subband is for generation of watermarked image.

3. Then LL2 sub band wavelet coefficients of host image is modified according to sparse measurements of watermark biometric image with gain factor α using Cox equation (Cox, Shamoon & Leighton, 1997) which is given below:

$$\hat{I}_{LL2}(x,y) = I_{LL2}(x,y) * (1 + \alpha * W_{Sparse}(x,y)) \quad (2)$$

Where $W_{Sparse}(x,y)$ = the (x, y)th value of sparse measurements of watermark biometric image, $I_{LL2}(x,y)$ = the original wavelet coefficients at (x, y) th location in LL2 subband, α is gain factor which is varied between 2 to 5, $\hat{I}_{LL2}(x,y)$ = the modified wavelet coefficients at (x, y) th location in LL2 subband.

4. Then apply 2nd level Inverse Discrete Wavelet Transform (IDWT) on modified LL2 sub band with original sub bands such as HL2, LH2, and HH2 to generate the watermarked image at embedder side.

2.3 Watermark Extraction Procedure

The proposed watermark extraction steps are given below:

1. Watermarked image, which may corrupt by attacker is taken and apply 2nd level Discrete Wavelet Transform (DWT) on it and get modified wavelet coefficients of LL2 subband.
2. Take original host image and apply 2nd level Discrete Wavelet Transform (DWT) on it and get original wavelet coefficients of LL2 subband.
3. For the size of sparse measurements of watermark biometric image repeat the step 4.
4. Extraction of sparse measurements of watermark biometric image by using reverse procedure of embedding which is given below:

$$W_{Extracted}(x,y) = \frac{\left(\frac{\hat{I}_{LL2}(x,y)}{I_{LL2}(x,y)} - 1\right)}{\alpha} \quad (3)$$

Where $W_{Extracted}(x,y)$ = the (x, y) th value of extracted sparse measurements of watermark biometric image, $I_{LL2}(x,y)$ = the original wavelet coefficients at (x, y) th location in LL2 subband, $\hat{I}_{LL2}(x,y)$ = the modified wavelet coefficients at (x, y) th location in LL2 subband.

5. After extracting sparse measurements of watermark biometric image and then watermark biometric image is reconstructed from extracted sparse measurements.

2.4 Watermark Reconstruction Procedure

The proposed watermark reconstruction procedure using compressive sensing (CS) theory recovery process steps are given below:

1. Using compressive sensing (CS) theory recovery algorithm like Orthogonal Matching Pursuit (OMP) (Tropp & Gilbert, 2007) is apply of extracted sparse measurements of watermark biometric image using measurement matrix *A* which generate at embedder side.
2. The output of Orthogonal Matching Pursuit (OMP) is estimated sparse coefficients of watermark biometric image. The Orthogonal Matching Pursuit (OMP) is worked on three basic steps where are find best matching column between sparse measurements *y* value and measurement matrix *A* and then find orthogonal projection between these columns. Then finally find residual between these columns using least square optimization technique. In next iteration, this residual values work as estimated sparse measurement *y*. For each iteration, Orthogonal Matching Pursuit (OMP) is recover one non-zero sparse coefficients.
3. After application of Orthogonal Matching Pursuit (OMP) on extracted sparse measurements of watermark biometric image, we have got recovered sparse coefficients which are embedded at embedder side.
4. Then, apply inverse Discrete Cosine Transform (DCT) on these recovered sparse coefficients and get reconstructed watermark biometric image.

2.5 Template Matching Procedure

The template matching procedure steps are described below.

1. After getting reconstructed watermark biometric image, we have performed template matching between original watermark biometric image and reconstructed watermark biometric image.
2. In this proposed technique, we have used parameter like Structural Similarity Measure Index (SSIM) for template matching between original watermark biometric image and reconstructed watermark biometric image. The matching score value is decided based on similarity between original and reconstructed watermark biometric images which should be

greater than some fixed threshold value (Kang, Lu & Hsu, 2009).

3. For decision about used is authentic or not, we have create two hypothesis based on hypothesis testing problem described by Kang (Kang, Lu & Hsu, 2009).
   - Hypothesis 1: User is authentic if
     $$Matching\_\text{Re}sult = SSIM(W,\hat{W}) > \tau_{SSIM}$$
   - Hypothesis 2: User is authentic if
     $$Matching\_\text{Re}sult = SSIM(W,\hat{W}) < \tau_{SSIM}$$

   Where W is original watermark biometric image, $\hat{W}$ is reconstructed watermark biometric image.

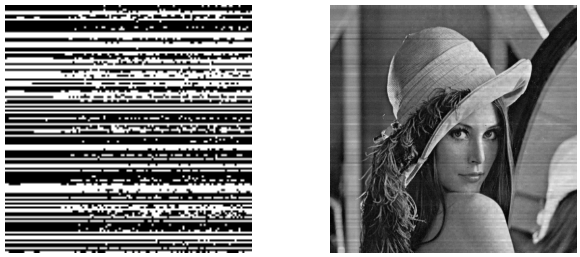
3 Dataset Preparation

For testing and evaluation of performance of the proposed sparse watermarking technique, standard Lena image as host image and monochromic fingerprint template image (FVC, 2004) as watermark image is used and shown in Figure 2. We have chosen FVC 2004 fingerprint template images dataset for experiment because of these fingerprint images widely used for research on biometric system and we have compared our experimental results which existing watermarking techniques results easily using this dataset. For experiment, the size of standard Lena image is 512 × 512 pixels and size of fingerprint template image is 128 × 128 pixels selected.

(a) (b)

Fig.2. (a) Standard Lena Image as Host Image (b) Monochromic Fingerprint Image as Watermark

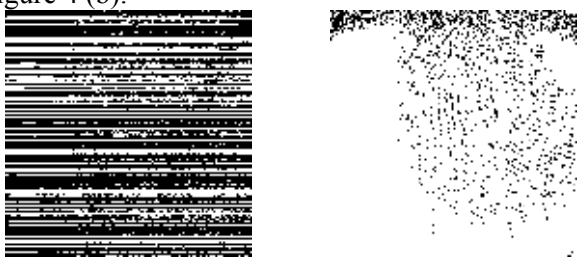
The sparse measurements of watermark fingerprint image is generated using compressive sensing (CS) theory procedure is given as below. First apply Discrete Cosine Transform (DCT) on watermark fingerprint image and convert into its DCT coefficients. These DCT coefficients are taken as sparse coefficients x with size of 128 × 128. Then generate measurement matrix A with size of 128 × 128 using standard normal distribution matrix with mean = 0 and variance =1. Then generate sparse measurements of watermark fingerprint image with size of 128 × 128 using $y_{128\times128} = A_{128\times128} \times x_{128\times128}$. The sparse measurements of watermark fingerprint image are shown in Figure 3 (a). These sparse measurements of watermark fingerprint image are embedding into wavelet coefficients of LL2 subband of host image which size of 128 × 128 using equation 2 and generate watermarked image after embedding procedure which is shown in Figure 3 (b). For embedding and extraction procedure, gain factor α is set value of 2.



(a) (b)

Fig.3. (a) Sparse Measurements of Watermark Fingerprint Image (b) Watermarked Image

For extraction of sparse measurements of watermark fingerprint image, reverse procedure of embedding is performed and extracted sparse measurements of watermark fingerprint image is shown in Figure 4 (a). For reconstruction of watermark fingerprint image from extracted sparse measurements, apply compressive sensing (CS) theory recovery algorithm like Orthogonal Matching Pursuit (OMP) (Tropp & Gilbert, 2007) on extracted sparse measurements of watermark fingerprint image using measurement matrix A with size of 128 × 128 and sparsity lelvel of 128 which depend of size of image. The output of OMP is extracted sparse coefficients of watermark fingerprint image. Then apply Discrete Cosine Transform (DCT) on extracted sparse coefficients to get reconstructed watermark fingerprint image which is shown in Figure 4 (b).



(a) (b)

Fig.4. (a) Extracted Sparse Measurements of Watermark Fingerprint Image (b) Reconstructed Watermark Fingerprint Image

In the proposed sparse watermarking technique, compressive sensing theory is used for additional

computational security for existing biometric system based on watermarking technique. Reconstructed watermark fingerprint image is used for user authentication at template matching procedure so that it is essential that compressive sensing (CS) theory procedure could not cause significant change in authentication performance of fingerprint recognition.

In order to showcase the effect of compressive sensing (CS) theory on authentication performance of fingerprint recognition, we have used fingerprint recognition algorithm is described by Jain and its research team (Jain & Prabhakar, 1999; Prabhakar, 2001). This algorithm is give average distance between query fingerprint image and its matched fingerprint image in the database. For checking of effect of proposed sparse watermarking technique on authentication performance of fingerprint biometric system, we have stored 50 reconstructed watermark fingerprint image, 50 authentic watermark fingerprint image and 50 fake watermark fingerprint image in a database.

4 Experimental Results

Structural Similarity Measure Index (SSIM) quality measure between watermark fingerprint images is used as matching score. The threshold for matching score is set 0.90. When watermarking attacks is applied on watermarked image, then similarity value between original fingerprint image and reconstructed fingerprint image which is chosen as matching score is less than selected threshold 0.9 percentages which is indicated in Table 1. This situation indicated that proposed sparse watermarking technique is fragile against all possible watermarking attacks.

For fragility test of proposed sparse watermarking technique, various attacks like JPEG compression; Additive noise like Gaussian noise, salt & peeper noise and speckle noise; median, mean and Gaussian low pass filter; some geometric attacks like histogram equalization and cropping. In this paper, PSNR, NCC and SNR are used perceptual quality measure between host image and watermarked image at embedder side. The quality of reconstructed watermark fingerprint image is measure by computing similarity with original watermark fingerprint image using SSIM quality measure (Wang & Bovik et al., 2004). Table 1 summarized the PSNR, SNR, NCC value between host image and watermarked image and SSIM value between watermark biometric image and extracted watermark biometric image at detector side under consideration of watermarking attacks.

Table 1. Values of Quality Measures for Proposed Sparse Watermarking Technique under Various Watermarking Attacks

Attacks	PSNR (dB)	SNR (dB)	NCC	SSIM
No Attack	41.05	26.85	0.995	0.934
JPEG Compression (Q = 90)	40.25	25.32	0.994	0.927
Gaussian Noise (μ = 0, σ = 0.01)	38.34	21.46	0.984	0.686
Salt & Pepper Noise (Noise Density = 0.005)	37.77	20.32	0.979	0.562
Speckle Noise (Variance = 0.004)	38.64	22.05	0.986	0.873
Median Filter (size = 3 × 3)	40.26	25.27	0.993	0.876
Mean Filter (size = 3 × 3)	38.80	22.37	0.987	0.625
Gaussian Low Pass Filter (size = 3 × 3)	39.66	26.06	0.994	0.887
Histogram Equalization	32.44	12.01	0.987	0.112
Cropping	38.43	21.62	0.985	0.364

The quality measures shows in Table 1 is indicated that when watermarking attacks is not applied on watermarked image, the values of quality measures are high. But when watermarking attacks is applied on watermarked image, the values of quality measures are less. The qualitative measures like PSNR, SNR, NCC and SSIM are used for performance evaluation of proposed sparse watermarking technique. The PSNR, SNR and NCC quality measures are used for comparison of watermarked image and host image. The high value of these quality measures indicated that performance of proposed sparse watermarking technique is better when watermarking attacks is not applied on watermarked image.

Now we have given study of effect of this proposed sparse watermarking technique on authentication performance of fingerprint biometric system. For authentication performance of fingerprint biometric system, we have get average distance between authenticated fingerprint images, fake fingerprint images and reconstructed fingerprint images using fingerprint recognition algorithm (Jain & Prabhakar, 1999; Prabhakar, 2001). Then based on various thresholds, we have calculated False Rejection Ratio (FRR) and False Acceptance Ratio (FAR) using equation defined by

Giot and its research team (Giot, El-Abed & Rosenberger, 2012).

False Acceptance Ratio (FAR) describes the probability that a biometric system will incorrectly authenticate an individual or will fail to reject an imposter and False Rejection Ratio (FRR) describes the probability that a biometric system incorrectly declares failure of match between input sample and matching template (Giot, El-Abed & Rosenberger, 2012).The values of FRR and FAR is summarized in Table 2.

Table 2. Values of FRR and FAR for Fingerprint Biometric System based on Recognition Performance

Threshold Distance	False Rejection Ratio (FRR)	False Acceptance Ratio (FAR)
0	1.00	0.00
250	1.00	0.00
500	1.00	0.00
750	0.96	0.02
1000	0.00	1.00
1250	0.00	1.00
1500	0.00	1.00

Using the values of FRR and FAR getting for various threshold distances, we have plot receiver operating characteristics (ROC) curve for fingerprint biometric system. Based on Figure 5, we have selected threshold distance is 875 because of on this value, FRR graph line and FAR graph line having equal value and this value is referred as Equal Error Rate (EER) for fingerprint biometric system (Giot, El-Abed & Rosenberger, 2012).

Then, the distance range between fake watermark fingerprints images compute with reconstructed watermark fingerprint images in stored database. The average distance range between them is 910.60 which are greater than selected threshold value. Also compute the distance between authentic watermark fingerprint images and reconstructed watermark fingerprint images stored in database. The average distance range between them is 845.77. Since the distance range between authentic fingerprint image and their reconstructed version database is less than selected threshold value indicated that authentication performance of fingerprint biometric system is unaffected by compressive sensing theory recovery procedure, so that propose sparse watermarking technique is used for security of biometric template in biometric system. These results are summarized in Table 3.

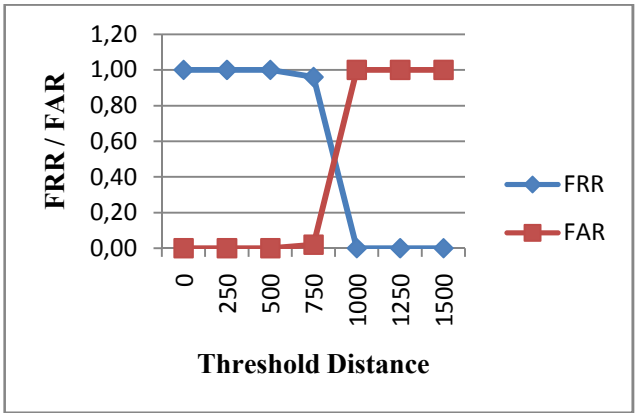


Fig.5. ROC Curve of Fingerprint Biometric System Where red line indicated graph of FAR vs. Threshold and black line indicated graph of FRR vs. Threshold

Table 3. Average Distance between Reconstructed, Authentic and Fake Fingerprint Image (for 50 Images)

Average Distance between Reconstructed Watermark and Authentic Fingerprint Image	Average Distance between Reconstructed Watermark and Fake Fingerprint Image	Selected Threshold Distance
845.77	910.60	875

Now this proposed sparse watermarking technique is compared with various wavelet domain watermarking techniques is given by Rege et al. (2014), Kothari et al. (2011); Inamdar et al. (2010) and Noore et al. (2007). The comparison of proposed sparse watermarking technique with these existing techniques with various features and parameters is summarized in Table 4.

Table 4. Comparison of Proposed Sparse Watermarking Technique with Existed Watermarking Technique in Literature

Sr. No.	Features & Parameters	Rege Technique et al. (2014)	Kothari Technique et al. (2011)	Inamdar Technique et al. (2010)	Noore Technique et al. (2007)	Proposed Sparse Watermarking Technique
1	Type of Watermarking Technique	Robust	Robust	Robust	Robust	Fragile
2	Used Host Medium	Standard Image	Standard Video	Standard Image	Fingerprint Image	Standard Image

3	Used Watermark Information	LPC of Speech, Gabor Coefficients of Face, Offline Signature	Standard Image	Offline Signature	Face Image + Text Information	Sparse Measurements of Fingerprint Image
4	Used Wavelet Coefficients	LH Sub band of Different Level	HL Sub band of 1st Level	LH, HL and HH Sub band of 2nd Level	LH, HL and HH Sub band of 2nd Level	LL Sub band of 2nd Level
5	Computational Security Achieved	Gain Factor	Gain Factor + PN Sequence	Gain Factor + PN Sequence	Selected Texture Regions of Wavelet Coefficients of Fingerprint Image	Compressive Sensing Theory Procedure
6	Authentication Through Template Matching	Possible	No such scope	Possible	Possible	Possible
7	PSNR (dB)	35.18	24.84	36.32	34.58	41.05
8	SNR (dB)	12.10	20.43	27.46	11.13	26.85
9	NCC	0.789	0.928	0.876	0.346	0.995
10	SSIM	0.977	0.994	0.891	0.951	0.934

In the proposed work discussed here, approximation wavelet coefficients is used for embedding while in existing watermarking techniques in literature, horizontal, vertical and diagonal wavelet coefficients is used for embedding. In the proposed watermarking technique, compressive sensing theory procedure is used for more computational security compared to gain factor and Correlation properties of PN sequence used for security parameter in existing watermarking technique in literature. In the proposed watermarking technique, biometric template is secure before embedding into host medium, where in existing watermarking techniques in literature, biometric template is directly embedding into host medium. Also performance of proposed watermarking technique is better than existing watermarking techniques in literature because of higher PSNR and NCC values is achieved for proposed watermarking technique compared to existing watermarking techniques in literature.

5 Conclusions

A fragile biometric watermarking technique is proposed using Discrete Wavelet Transform (DWT), CS theory procedure, and sparseness property of Discrete Cosine Transform (DCT). This technique is robust against JPEG compression attack because when this attack is applied on watermarked image, watermark fingerprint image authentication is possible because of SSIM value between original watermark fingerprint image and reconstructed watermark fingerprint image is higher than selected matching score which is indicated in Table 1. This proposed sparse watermarking technique is providing security to biometric template at communication channel in fingerprint biometric system because of when attack is applied on watermarked image then embedded sparse measurements of watermark fingerprint image is distorted and reconstruction of fingerprint image is not possible.

This proposed sparse watermarking technique is also provide security against spoof or modification attack because of at reconstruction of watermark fingerprint image, required correct measurement matrix and correct image transform information to reconstruction of watermark fingerprint image. It is difficult to attacker or unauthenticated person to get this information of measurement matrix and image transform for reconstruction of watermark fingerprint image. In future, this proposed watermarking technique is applied on other biometric template like face, iris and signature.

References:

[1] Jain, A., & Kumar, A., (2012). Biometric Recognition: An Overview. *Second Generation Biometrics: The Ethical, Legal and Social Context, E. Mordini and D. Tzovaras (Eds.), Springer,* 49 – 79.

[2] Jain, A., Ross, A., & Pankanti, S. (2006). Biometrics: A Tool for Information

Security. *Information Forensics and Security, IEEE Transactions on*, *1*(2), 125 – 143.

[3] Jain, A., & Uludag, U. (2002, March). Hiding fingerprint minutiae in images. *In Proceedings of 3rd Workshop on Automatic Identification Advanced Technologies*, 97 – 102.

[4] Sheikh, M., & Baraniuk, R., (2007, September). Blind Error-Free Detection of Transform-Domain watermarks. *In Image Processing, 2007. ICIP 2007. IEEE International Conference on* (Vol. 5, pp. V-453).

[5] Tiesheng, F., Guiqiang, L., Chunyi, D., & Danhua, W. (May, 2013). A Digital Image Watermarking Method Based on the Theory of Compressed Sensing. *International Journal Automation and Control Engineering*, *2*(2), 56-61.

[6] Fakhr, M. W. (December, 2012). Robust Watermarking Using Compressed Sensing Framework with Application to MP3 Audio. *The International Journal of Multimedia & Its Applications*, *4*(6), 27 – 43.

[7] Raval, M., Joshi, M., Rege, P., & Parulkar, S. (December, 2011). Image Tampering Detection Using Compressive Sensing Based Watermarking Scheme. *Proceedings of MVIP 2011.*

[8] Zhang, X., Qian, Z., Ren, Y., & Feng, G. (2011). Watermarking with Flexible Self-recovery Quality based on Compressive Sensing and Compositive Reconstruction. *Information Forensics and Security, IEEE Transactions on*, *6*(4), 1223-1232.

[9] Valenzise, G., Tagliasacchi, M., Tubaro, S., Cancelli, G., & Barni, M. (November, 2009). A Compressive-Sensing based Watermarking Scheme for Sparse Image Tampering Identification. In *Image Processing (ICIP), 2009 16th IEEE International Conference on*, 1265 – 1268.

[10] Candès, E. J. (2006). Compressive Sampling. In *Proceedings of the International Congress of Mathematicians: Madrid, August 22-30, 2006: invited lectures* (pp. 1433-1452).

[11] Baraniuk, R. (July, 2007). Compressive Sensing. *IEEE signal processing magazine*, *24*(4), 118 - 124.

[12] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (December, 1997). Secure Spread Spectrum Watermarking for Multimedia. *Image Processing, IEEE Transactions on*, *6*(12), 1673-1687.

[13] Tropp, J. A., & Gilbert, A. C. (December, 2007). Signal Recovery from Random Measurements via Orthogonal Matching Pursuit. *Information Theory, IEEE Transactions on*, *53*(12), 4655-4666.

[14] Maio, Dario, et al. "FVC2004: Third Fingerprint Verification Competition. *Biometric Authentication*. Springer Berlin Heidelberg, 2004, 1 – 7.

[15] http://bias.csr.unibo.it/fvc2002/databases.asp {Date of Access: 30/12/2014}

[16] Wang, Z., & Bovik, A. C. (2002). A Universal Image Quality Index. *Signal Processing Letters, IEEE*, *9*(3), 81 – 84.

[17] Jain, A. K., Prabhakar, S., & Pankanti, S. (1999). A Filterbank-based Representation for Classification and Matching of Fingerprints. In *Neural Networks, 1999. IJCNN'99. International Joint Conference on* (Vol. 5, pp. 3284 – 3285).

[18] Prabhakar, S. (2001). *Fingerprint Classification and Matching Using a Filterbank* (Doctoral dissertation, Michigan State University).

[19] Inamdar, V. S., & Rege, P. P. (2014). Dual Watermarking Technique with Multiple Biometric Watermarks. *Sadhana*, *39*(1), 3 – 26.

[20] Kothari, A., & Dwivedi, V., (December, 2011). Discrete Wavelet Transform Based Digital Video Watermarking – A Novel Approach to Hide Binary Watermark Behind Video. *Proceedings of 2011 IEEE International Conference on Computational Intelligence and Computing Research.*

[21] Inamdar, V., Rege, P., & Arya, M. (2010). Offline Handwritten Signature based Blind Biometric Watermarking and Authentication Technique using Biorthogonal Wavelet Transform. *International Journal of Computer Applications*, *11*(1), 19 – 27.

[22] Noore, A., Singh, R., Vatsa, M., & Houck, M. M. (2007). Enhancing Security of Fingerprints through Contextual Biometric Watermarking. *Forensic Science International*, *169*(2), 188-194.

[23] Jain, A. K. (1989). *Fundamentals of digital image processing* (Vol. 3). Englewood Cliffs: prentice-Hall, 150 – 153.

[24] Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). Watermarking Digital Image and Video Data. A State-of-the-Art Overview. *IEEE Signal Processing Magazine, 17 (5)*, 20 – 43.

[25] Raval, M. S., & Rege, P. P. (October, 2003). Discrete Wavelet Transform based Multiple

Watermarking Scheme. In *TENCON 2003. Conference on Convergent Technologies for the Asia-Pacific Region* (Vol. 3, pp. 935-938).

[26] Kang, L. W., Lu, C. S., & Hsu, C. Y. (November, 2009). Compressive Sensing-based Image Hashing. In *Image Processing (ICIP), 2009 16th IEEE International Conference on* (pp. 1285 – 1288).

[27] Giot, R., El-Abed, M., & Rosenberger, C. (2013). Fast Computation of the Performance Evaluation of Biometric Systems: Application to Multibiometrics. *Future Generation Computer Systems*, *29*(3), 788-799.