Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 251 – 258

Procedia
Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

Sparse Watermarking Technique for Improving Security of Biometric System

Rohit Thanki[a]*, Komal Borisagar[b]

[a]*Faculty of Technology and Engineering, C. U. Shah University, Wadhwan City and 363030, India*
[b]*EC Department, Atmiya Institute of Technology and Science, Rajkot and 360005, India*

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 paper proposed a sparse watermarking technique based on compressive sensing (CS) theory framework for security against this kind of attack. In this proposed sparse watermarking technique, fingerprint image is taken as watermark information. This fingerprint image is converted into sparse measurements using compressive sensing (CS) theory and embeds these sparse measurements into wavelet coefficients of standard image to generate a watermarked image. The structural similarity measure index (SSIM) quality measure is used for authentication between original watermark fingerprint image and reconstructed watermark fingerprint image. The experimental results show that proposed sparse watermarking technique does not affect verification and authentication performance of a biometric system. The proposed sparse watermarking technique has a good performance compared to the existing watermarking technique in the literature.

Peer-review under responsibility of the Organizing Committee of ICECCS 2015

Keywords: Biometric System; Compressive Sensing; Fingerprint; SSIM; Sparse Biometric Watermarking.

1. Introduction

Nowadays, the biometric authentication based system is used for recognition of person automatically. This biometric system has many advantages compare to a traditional biometric system like I-card, password etc. [1]. However, this biometric system has vulnerable to various attacks like spoofing at system database, stone of

* Corresponding author. Tel.: +91-9998236991, *E-mail address:* rohitthanki9@gmail.com

Peer-review under responsibility of the Organizing Committee of ICECCS 2015
doi:10.1016/j.procs.2015.10.083

biometric templates at communication channel, modification of module with system and noise in sensor etc. [1], [2]. Digital watermarking is one of the solution for attacks like spoofing at system database, stone of biometric templates at the communication channel of biometric system [3]. Nevertheless, digital watermarking techniques have some restriction such as less payload capacity and less computational security [4]. To overcome to the limitation such as less computational security, researcher introduces a sparse domain watermarking technique based on compressive sensing theory [4]. In sparse domain watermarking technique, used sparseness property to provide by compressive sensing (CS) theory and used this theory for generating of sparse watermark information and this sparse watermark information is embedded in host medium. In the last eight years, many researchers have proposed various sparse domain watermarking techniques based on compressive sensing (CS) theory. These watermarking techniques are applied to improving payload capacity and detection of watermarked image tampering.

The concept of watermarking technique using compressive sensing (CS) theory is presented by Sheikh and its research team [5]. In this technique, $y = Af + e$ be the transform domain watermarked signal the encoding process, where f is the spread spectrum watermark sequence, A is a random measurement matrix and e is sparser 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 [6] described a watermarking technique based on a 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. Fakhr [7] described a compressive sensing based robust audio watermarking technique and gives a comparison against various attacks like MP3 audio compression and additive noise. M. Raval et al. [8] described a fragile watermarking technique using compressive sensing (CS) theory for reducing dimensions and improved security of image against tampering. Furthermore, X. Zhang et al. [9] 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 the image. M. Tagliasacchi et al. [10] described a fragile watermarking technique based on compressive sensing (CS) theory for sparse image tampering identification.

This paper 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 existed watermarking techniques in literature which is used for tamper identification of watermarked 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 paper, we have proposed a sparse biometric watermarking technique based on sparseness provided by Discrete Cosine Transform (DCT) [11], Discrete Wavelet Transform based watermarking and Compressive Sensing (CS) theory procedure [12, 13].

In this proposed sparse watermarking technique, first encrypted fingerprint biometric image 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 a watermarked image. At decoder side, extracted these sparse measurements of fingerprint image from watermarked image and then reconstructed fingerprint image from extracted sparse measurements using compressive sensing (CS) theory recovery procedure. This reconstructed fingerprint image is compared with original fingerprint image for recognition of individual based on matching results of comparison. The rest of the paper is organized such that next section gives proposed sparse watermarking technique then experimental results. Finally gives conclusions on proposed sparse watermarking technique.

2. Proposed Sparse Watermarking Technique

The proposed sparse watermarking technique is based on a combination of compressive sensing acquisition and recovery procedure [12, 13] and wavelet domain based watermarking approach. The block diagram of proposed sparse watermarking technique is shown in Figure 1. This watermarking technique is divided into five procedures such as watermark preparation using compressive sensing (CS) theory Acquisition Procedure; watermark embedding; watermark extraction; watermark reconstruction using Orthogonal Matching Pursuit (OMP) algorithm and template matching for personal recognition.

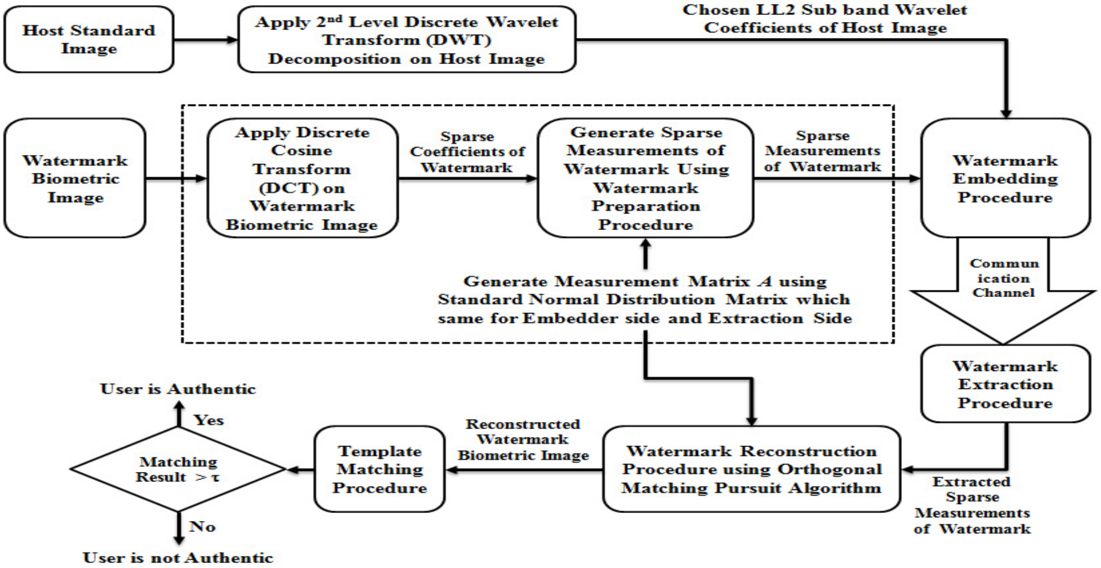
Host Standard Image
Apply 2nd Level Discrete Wavelet Transform (DWT) Decomposition on Host Image
Chosen LL2 Sub band Wavelet Coefficients of Host Image
Watermark Biometric Image
Apply Discrete Cosine Transform (DCT) on Watermark Biometric Image
Sparse Coefficients of Watermark
Generate Sparse Measurements of Watermark Using Watermark Preparation Procedure
Sparse Measurements of Watermark
Watermark Embedding Procedure
Generate Measurement Matrix A using Standard Normal Distribution Matrix which same for Embedder side and Extraction Side
Communication Channel
Watermark Extraction Procedure
Extracted Sparse Measurements of Watermark
Watermark Reconstruction Procedure using Orthogonal Matching Pursuit Algorithm
Reconstructed Watermark Biometric Image
Template Matching Procedure
Matching Result > τ
Yes
User is Authentic
No
User is not Authentic

Fig.1. Block Diagram of Proposed Sparse Watermarking Technique

2.1. Watermark Preparation Using CS Theory Acquisition Procedure

Take a watermark biometric image and apply the Discrete Cosine Transform (DCT) on it and converting watermark biometric image into DCT coefficients. These DCT coefficients of a watermark biometric image are taken as sparse coefficients and denoted as $\boldsymbol{x}$. This step is necessary because of image must sparse when compressive sensing (CS) theory is apply for it. The Measurement matrix $\boldsymbol{A}$ is generated using standard normal distribution matrix with mean = 0 and variance =1 which is same for embedder and detector. Generate sparse measurements $\boldsymbol{y}$ of the watermark biometric image by multiplication of sparse coefficients $\boldsymbol{x}$ and measurement matrix $\boldsymbol{A}$ which is described by equation 1. Then, these sparse measurements of the watermark biometric image are used as watermark information and denoted as $\boldsymbol{W_{Sparse}}$. In Figure 1, dotted box is shown watermark preparation using CS theory acquisition procedure.

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

Where y = Sparse Measurements of Watermark Biometric Image; A = Measurement Matrix; x = Sparse Coefficients.

2.2. Watermark Embedding Procedure

Take the standard image as host image and compute the size of the image. Then apply second level Discrete Wavelet Transform (DWT) on host image and convert into various sub bands such as LL2, HL2, LH2 and HH2. Here approximation wavelet coefficients (LL2) of 2nd level DWT decomposition are chosen because of the size of the LL2 sub band is equal to the size of sparse measurements watermark biometric image and easy to performed embedding process. When HL2, LH2 and HH2 subband is used for generation of watermarked image. 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 [14] which is described by equation 2. Then apply the second 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.

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

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

2.3. Watermark Extraction Procedure

Watermarked image, which may corrupt by the attacker is taken and apply 2nd level Discrete Wavelet Transform (DWT) on it and get modified wavelet coefficients of LL2 subband. Then take an original host image and apply 2nd level Discrete Wavelet Transform (DWT) on it and get original wavelet coefficients of LL2 subband. Extraction of sparse measurements of a watermark biometric image by using the reverse procedure of embedding which is described by equation 3. After extracting sparse measurements of watermark biometric image from the watermarked image, then the watermark biometric image is reconstructed from extracted sparse measurements.

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

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

2.4. Watermark Reconstruction Using Orthogonal Matching Pursuit Algorithm

Using compressive sensing (CS) theory recovery algorithm like Orthogonal Matching Pursuit (OMP) [15] is applied of extracting sparse measurements of a watermark biometric image using a measurement matrix A which generate at embedder side. The output of Orthogonal Matching Pursuit (OMP) is estimated sparse coefficients of a watermark biometric image. The Orthogonal Matching Pursuit (OMP) is working 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 the least square optimization technique. During next iteration, this residual values works as estimated sparse measurement ***y***. For each iteration, Orthogonal Matching Pursuit (OMP) has recovered one non-zero sparse coefficients. After application of Orthogonal Matching Pursuit (OMP) on extracted sparse measurements of watermark biometric image, recovered sparse coefficients which are embedded at embedder side. Then, apply inverse Discrete Cosine Transform (DCT) on these recovered sparse coefficients and get reconstructed watermark biometric image.

2.5. Template Matching Procedure

After getting reconstructed watermark biometric image, we have performed template matching between original watermark biometric image W and reconstructed watermark biometric image $\hat{W}$. In this proposed watermarking technique, the parameter like Structural Similarity Measure Index (SSIM) is used 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 [16]. For decision about used is authentic or not, create two hypotheses based on hypothesis testing, problem described by Kang [16].

- Hypothesis 1: User is authentic if $Matching\_\mathrm{Re}sult = SSIM(W,\hat{W}) > \tau_{SSIM}$
- Hypothesis 2: User is unauthentic if $Matching\_\mathrm{Re}sult = SSIM(W,\hat{W}) < \tau_{SSIM}$

3. Experimental Results

For testing and evaluation of performance of the proposed sparse watermarking technique, standard Lena image as host image and monochrome fingerprint template image [17] as watermark image is used and shown in Figure 2. FVC 2004 fingerprint template image data set are chosen for the experiment because of these fingerprint images widely used for research on biometric system. For the experiment, the size of the standard Lena image is 512 × 512 pixels and a size of the fingerprint template image is 128 × 128 pixels selected. The sparse measurements of the watermark fingerprint image are generated using compressive sensing (CS) theory procedure is given as below. First apply Discrete Cosine Transform (DCT) on the 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 equation 1. The sparse measurements of the watermark fingerprint image are shown in Figure 2 (c). These sparse measurements of the 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 2 (d). For embedding and extraction procedure, gain factor α sets a value of 2.

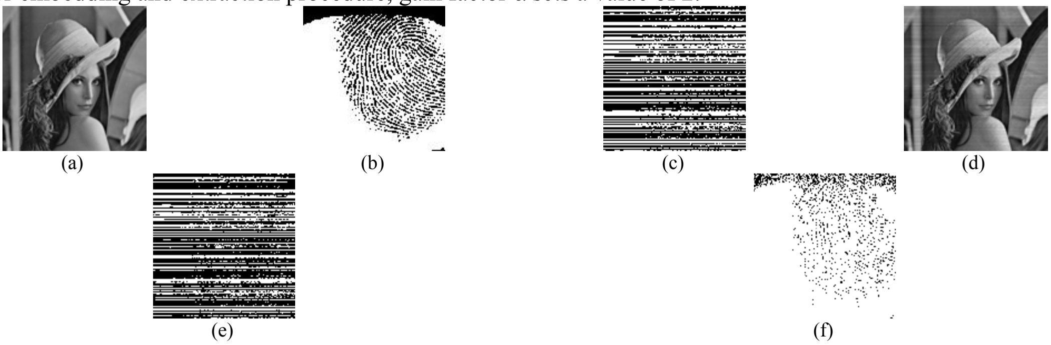

Fig.2. (a) Standard Lena Image as Host Image; (b) Fingerprint Image as Watermark; (c) Sparse Measurements of Watermark Fingerprint Image; (d) Watermarked Image; (e) Extracted Sparse Measurements of Watermark Fingerprint Image; (f) Reconstructed Watermark Fingerprint Image

For extraction of sparse measurements of watermark fingerprint image, reverse procedure of embedding is performed and extracted sparse measurements of the watermark fingerprint image is shown in Figure 2 (e). For reconstruction of watermark fingerprint image from extracted sparse measurements, apply compressive sensing (CS) theory recovery algorithm like Orthogonal Matching Pursuit (OMP) on extracted sparse measurements of a watermark fingerprint image using a measurement matrix A with size of 128 × 128 and sparsity level of 128 which depend on size of image. The output of OMP is extracted sparse coefficients of a watermark fingerprint image. Then apply Inverse Discrete Cosine Transform (IDCT) on extracted sparse coefficients to get reconstructed watermark fingerprint image which is shown in Figure 2 (f). In the proposed sparse watermarking technique, compressive sensing theory is used for additional computational security for existing biometric system based on watermarking technique. The 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.

Structural Similarity Measure Index (SSIM) [18] quality measure between watermark fingerprint images is used as matching score. The threshold for matching score is set 0.90. When watermarking attacks are applied on watermarked image, then the 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 the 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 & pepper noise and speckle noise; median, mean and Gaussian low pass filter; some geometric attacks like histogram equalization and cropping. In this paper, peak signal to noise ratio (PSNR), signal to noise ratio (SNR) and normalized cross correlation (NCC) are used perceptual quality measure between host image and watermarked image at embedder side. The quality of the reconstructed watermark fingerprint image is measure of computing similarity with the original watermark fingerprint image using SSIM quality measure [18]. 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 the 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

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

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

The quality measures are shown in Table 1 are indicated that when watermarking attacks is not applied on watermarked image, the values of quality measures are higher. But when watermarking attacks are applied on watermarked image, the values of quality measures are less. The qualitative measures like a peak signal to noise ratio (PSNR), signal to noise ratio (SNR), normalized cross correlation (NCC) and structural similarity index measure (SSIM) are used for performance evaluation of the proposed sparse watermarking technique. The PSNR, SNR and NCC quality measures are used for comparison of watermarked image and host images. 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.

In order to showcase the effect of proposed watermarking technique on the authentication performance of fingerprint recognition, fingerprint recognition algorithm is described by Jain and its research team [19, 20] is used. This algorithm gives the average distance between query fingerprint image and its matched fingerprint image in the database. For checking of the effect of the proposed sparse watermarking technique on the authentication performance of fingerprint biometric system, 50 reconstructed watermark fingerprint image, 50 authentic watermark fingerprint image and 50 fake watermark fingerprint image are stored in a database.

For the authentication performance of fingerprint biometric system, average distance between authenticated fingerprint images, fake fingerprint images and reconstructed fingerprint images using fingerprint recognition algorithm [19, 20] is calculated. Then, based on various threshold distance, calculate False Rejection Ratio (FRR) and False Acceptance Ratio (FAR) using equation defined by Giot and its research team [21]. The values of FRR and FAR is summarized in Table 2. Using the values of FRR and FAR getting for various threshold distances, a plot receiver operating characteristic (ROC) curve for the fingerprint biometric system. Based on Figure 5, a select 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 [21].

Then, the distance range between fake watermark fingerprint images and reconstructed watermark fingerprint images is calculated. The average distance range between them is 910.60 which are greater than selected threshold distance 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 the selected threshold distance value indicated that the authentication performance of the fingerprint biometric system is unaffected by proposed watermarking technique. This result indicated that the proposed sparse watermarking technique is used for security of fingerprint biometric template in the fingerprint biometric system. These results were summarized in Table 3.

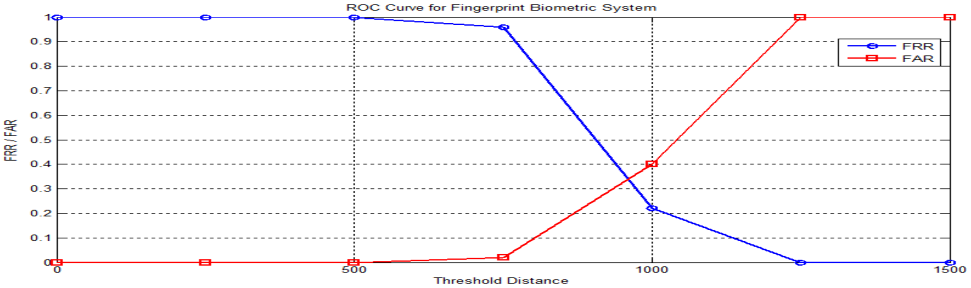

Fig.3. ROC Curve of Fingerprint Biometric System Where red line indicated graph of FAR vs. Threshold Distance and blue line indicated graph of FRR vs. Threshold Distance

Now this proposed sparse watermarking technique is compared with various wavelet domain watermarking techniques is given by Rege et al. [22], Kothari et al. [23]; Inamdar et al. [24] and Noore et al. [25]. The comparison of proposed sparse watermarking technique with these existed 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. [22]	Kothari Technique et al. [23]	Inamdar Technique et al. [24]	Noore Technique et al. [25]	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	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
5	PSNR (dB)	35.18	24.84	36.32	34.58	41.05
6	NCC	0.789	0.928	0.876	0.346	0.995

In the proposed work discussed here, approximation wavelet coefficients are 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, the 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, wherein existing watermarking techniques in the literature; biometric template is directly embedded in host medium. Also performance of proposed watermarking technique is better than existed watermarking techniques in literature because of higher PSNR and NCC values is achieved for proposed watermarking technique compared to existed watermarking techniques in the literature.

4. Conclusion

This paper shows an application of compressive sensing (CS) theory and digital watermarking techniques for biometric template security. A fragile biometric watermarking technique is proposed using Discrete Wavelet Transform (DWT), CS theory procedure, and sparseness property of Discrete Cosine Transform (DCT). This proposed sparse watermarking technique is providing security to a biometric template at communication channel in a fingerprint biometric system because of when the attack is applied on watermarked image, then embedded sparse measurements of the watermark fingerprint image is distorted and reconstruction of fingerprint image is not possible. This proposed sparse watermarking technique has also provided 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 images. It is difficult to attacker or imposter person to get this information of measurement matrix and image transform for reconstruction of watermark fingerprint images. In future, this proposed watermarking technique is applied to the other biometric template like face, iris and signature.

References

1. A. Jain and A. Kumar, “Biometric Recognition: An Overview”, *Second Generation Biometrics: The Ethical, Legal and Social Context, E. Mordini and D. Tzovaras (Eds.)*, Springer, 2012, pp. 49 – 79.
2. A. Jain, A. Ross and S. Pankanti, “Biometrics: A Tool for Information Security”, *IEEE Transactions on Information Forensics and Security,* 2006, 1, (2), pp. 125 – 143.
3. A. Jain and U. Uludag, “Hiding Fingerprint Minutiae in Images”, *Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, March 2002, pp. 97 – 102.
4. G. Langelaar, I. Setyawan and R. Lagendijk, “Watermarking Digital Image and Video Data – A State of the Art Overview”, *IEEE Signal Processing Magazine*, 2000, 17, (5), pp. 20 – 43.
5. M. Sheikh and R. Baraniuk, “Blind Error Free Detection of Transform Domain Watermarks”, *IEEE International Conference on Image Processing*, San Antonio, Texas, United States, 2007.
6. F. Tiesheng, L. Guiqiang, D. Chunyi and W. Danhua, “A Digital Image Watermarking Method Based on the Theory of Compressed Sensing”, *International Journal Automation and Control Engineering*, 2013, 2, (2), pp. 56 – 61.
7. M. Fakhr, “Robust Watermarking Using Compressed Sensing Framework with Application to MP3 Audio”, *The International Journal of Multimedia & Its Applications (IJMA)*, 2012, 4, (6), pp. 27 – 43.
8. M. Raval, M. Joshi, P. Rege and S. Parulkar, “Image Tampering Detection Using Compressive Sensing Based Watermarking Scheme”, *In Proceedings of MVIP 2011*, December 2011.
9. X. Zhang, Z. Qian, Y. Ren and G. Feng, “Watermarking with Flexible Self-recovery Quality based on Compressive Sensing and Compositive Reconstruction”, *IEEE Transactions on Information Forensics and Security*, 2011, 6, (4), pp. 1123 – 1231.
10. M. Tagliasacchi, G. Valenzise, S. Tubaro, G. Cancelli and M. Barni, “A Compressive Sensing Based Watermarking Scheme for Sparse Image Tampering Identification”, *In Proc. of ICIP 2009*, November 2009, pp. 1265 – 1268.
11. A. Jain, “Fundamentals of Digital Image Processing” (Englewood Cliffs: prentice-Hall, 1989), pp. 150 – 153.
12. E. Candès, “Compressive Sampling”, *Proceedings of the International Congress of Mathematicians*, Madrid, Spain, 2006, pp. 1433 – 1452.
13. R. Baraniuk, Lecture notes “Compressive Sensing”, *IEEE Signal Processing Magazine*, 2007, 24, (4), pp. 118 – 124.
14. I. Cox, J. Kilian, T. Shamoon and F. Leighton, “Secure Spread Spectrum Watermarking for Multimedia”, *IEEE Transactions on Image Processing,* 1997, 6, (12), pp. 1673 - 1687.
15. J. Tropp and A. Gilbert, “Signal Recovery from Random Measurements via Orthogonal Matching Pursuit”, *IEEE Transactions on Information Theory*, 2007, 53, (12), pp. 4655 – 4666.
16. W. Kang, S. Lu and C. Hsu, “Compressive Sensing based Image Hashing”, *In Proc. of ICIP 2009*, November 2009, pp. 1285 – 1288.
17. Maio, Dario, et al. "FVC2004: Third Fingerprint Verification Competition. Biometric Authentication”, *Springer Berlin Heidelberg*, 2004, pp. 1 – 7. http://bias.csr.unibo.it/fvc2002/databases.asp {Date of Access: 30/12/2014}
18. Z. Wang and A. Bovik, “A Universal Image Quality Index”, *J. IEEE Signal Processing Letters*, 2004, 9, (3), pp. 84 – 88.
19. A. Jain, S. Prabhakar, and S. Pankanti, “A Filterbank-based Representation for Classification and Matching of Fingerprints”, *International Joint Conference on Neural Networks (IJCNN)*, July 1999, pp. 3284 – 3285.
20. S. Prabhakar, “Fingerprint Classification and Matching Using a Filterbank”, *Ph.D. thesis*, Michigan State University, 2001.
21. R. Giot, M. El-Abed and C. Rosenberger, “Fast Computation of the Performance Evaluation of Biometric Systems - Application to Multibiometrics”, *Future Generation Computer Systems*, 2013, 29, (3), PP. 788 – 799.
22. V. Inamdar and P. Rege, “Dual Watermarking Technique with Multiple Biometric Watermarks”, *Sadhana © Indian Academy of Science*, 2014, 29, (1), pp. 3 – 26.
23. A. Kothari and V. Dwivedi, “Discrete Wavelet Transform Based Digital Video Watermarking – A Novel Approach to Hide Binary Watermark Behind Video”, *2011 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC 2011)*, December 2011.
24. V. Inamdar, P. Rege and M. Arya, “Offline Handwritten Signature based Blind Biometric Watermarking and Authentication Technique Using Biorthogonal Wavelet Transform”, *International Journal of Computer Applications*, 2010, 11, (1), pp. 19 – 27.
25. A. Noore, R. Singh, M. Vatsa and M. Houck, “Enhancing Security of Fingerprints through Contextual Biometric Watermarking”, *Forensic Science International*, 2007, 169, (2), pp. 188 – 194.