Multibiometric Template Security Using CS Theory – SVD Based Fragile Watermarking Technique

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

Abstract: - Protection of biometric template against spoofing or modification attack at system database is major issue in multibiometric system. Hence fragile digital watermarking technique is one of the solutions for biometric template protection against these attacks. In this paper, fingerprint watermarking technique based on SVD and Compressive Sensing theory proposed for protection of biometric template at system database of multibiometric system. This technique does not embed the fingerprint directly into face image instead using the concept of compressive sensing fingerprint convert into sparse measurements. The sparse measurements is generated at time of fingerprint embedding process and extracted from watermarked face image at extraction side for reconstruction of original watermark fingerprint image. SSIM value between original watermark fingerprint image and reconstructed watermark fingerprint image is the deciding factor for cross verification of individual. The experimental results show that the proposed technique does not affect verification and authentication performance of multibiometric system.

Key-Words: - Compressive Sensing Theory, Fragile, Multibiometric, SVD, Template Protection, Watermarking

1 Introduction

In today’s world, many organization and agency are used automatic biometric recognition based system for verification and authentication of individual [1]. But this automatic biometric system having several disadvantages like noisy data, inter class variation, intra class variation, non-universality and spoof attack. For overcome these disadvantages, A. Jain and its research team proposed new biometric system which is called as multimodal or multibiometric system [2], [3]. A. Ratha and its research team are identifying several vulnerable points associated with biometric system [4]. One vulnerable point is attack on system database of biometric system. Digital watermarking technique is one of the solutions against this attack [5].

In the last decade, fragile watermarking techniques are used for content authentication. Fragile watermarking techniques are mainly used for content authentication and for security because they are identified modification [6], [7], [8]. These modifications may indicate that unauthorized user try to access secure information. In last decade, many watermarking techniques are proposed by various researchers. In these proposed techniques, Singular Value Decomposition (SVD) has new and most powerful transform used for watermarking applications. Authors in [9] proposed hybrid watermarking technique based on SVD and Discrete Wavelet Transform (DWT). In this technique, host image decomposed in various wavelet coefficients like LL, LH, HL and HH and secure information is added to Singular value of all these four wavelet coefficients of host image. This technique is suffer to less security because of original watermark information is required at detector side.

In multibiometric system, watermark biometric is used for cross verification and authentication of individual at system database. Authors in [10] proposed hybrid watermarking technique based on SVD and LSB embedding. Authors in [11] proposed multimodal biometric authentication based technique which is provides additional security to fingerprint biometric system. In this technique, face features is embed as a watermark into fingerprint images of same individual. Authors in [12] proposed non-blind watermarking technique using SVD and Complex Wavelet Transform (CWT). In this technique, singular value of appropriate sub band complex wavelet coefficients of host image is modified according to singular value of watermark and secret key. Authors in [13] described combined DWT and LSB based biometric watermarking technique for security facial features hiding into fingerprint images.

Authors in [14] proposed fragile watermarking technique based on multistage VQ and DCT for protection of fingerprint image against copy attack. Authors in [15] proposed a semi fragile fingerprint watermarking technique based on Singular Value

Decomposition (SVD) for protection of biometric template at system database and matcher subsystem. Authors in [16] proposed salient region based authentication watermarking technique for protection of biometric templates. Many of watermarking techniques and SVD based watermarking techniques for biometric template protection focus on the issue of improving robustness and security of content at communication channel. Very little attention has been given to security of biometric template at system database.

The problems of biometric template security at system database and less fragile watermarking techniques are available for biometric template protection. So by keeping security issue in concern for template protection, in this paper, a novel biometric watermarking technique in hybrid domain to support the security demand of multibiometric template protection is proposed. In this paper, we have embedded sparse measurements of watermark biometric image into host biometric image to improve computational security of proposed watermarking technique. These sparse measurements of watermark biometric image are generated using Compressive Sensing (CS) theory framework.

Compressive Sensing theory is provides dimensional reduction and computational security to data. For application of CS theory on image, the necessary step is that image must be in its sparse domain [17]. So in this paper, we have explored sparseness provides by combination of DWT and SVD transform to generated sparse measurements of watermark biometric image. Then these sparse measurements of watermark biometric image are embedding into singular value of HL wavelet coefficients of host biometric image. Sparse measurements of watermark biometric image are computed from watermark biometric features and they are embedding into host biometric image to provide protection against spoof attack. The novelty of proposed watermarking technique is that it is able to embed similar size of watermark information into host medium which is not possible in some of existed technique in literature; no required actual watermark information at detector side; provide compression and protection to watermark information simultaneously due to combination of CS theory with watermarking technique.

Section 2 and 3 explain the proposed watermarking technique and results of proposed watermarking technique respectively. Section 4 shows effect of proposed watermarking technique on performance of multibiometric system. Section 5 gives conclusion and future work.

2 Proposed Watermarking Technique

This section describes the proposed watermarking technique based on Singular Value Decomposition (SVD) plus Discrete Wavelet Transform (DWT) and compressive sensing theory framework. In this proposed technique, face image is taken as host medium and apply SVD on fourth level wavelet coefficients of face image and get Singular matrix for watermark embedding. The fingerprint image is taken as watermark and which is converted into sparse measurements using CS theory framework, Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). This proposed technique is divided into two procedures like watermark preparation & embedding and watermark extraction & reconstruction. The proposed watermark preparation & embedding procedure and watermark extraction & reconstruction procedure is shown in figure 1 and 2 respectively.

2.1 Watermark Preparation & Embedding Procedure

The proposed watermark preparation and embedding procedure steps are described below:

1. Take biometric image as watermark and compute size of biometric image.
2. Apply single level Discrete Wavelet Transform (DWT) on watermark biometric image and decomposed into approximation and details wavelet coefficients. Chosen details wavelet coefficients of watermark biometric image. Here details wavelet coefficients are chosen because it is sparser than approximation wavelet coefficients.
3. Apply Singular Value Decomposition (SVD) on details wavelet coefficients and S matrix value chosen sparse coefficients which is denoted as x in equation 1. Here S matrix is chosen as sparse coefficients because it is sparser than orthogonal matrices U and V.

   $$x = \psi \cdot f \qquad (1)$$

   In formula (1), $\boldsymbol{x}$ is the sparse coefficients, $\boldsymbol{\Psi}$ is the orthogonal or basis matrix which is depend on applied image transform, $\boldsymbol{f}$ is the original watermark biometric image.
4. Generated measurement matrix $\boldsymbol{A}$ with size M × N using random seed which is same for embedder and decoder, where N is length of sparse coefficients and M is less than value N.
5. Generated Sparse Measurements of watermark biometric image using equation 2 and denoted as $\boldsymbol{W_{Sparse}}$.

$$W_{Sparse} = A \times x \quad (2)$$

In formula (2), $\boldsymbol{W_{Sparse}}$ is the Sparse Measurements of watermark biometric image; ***A*** is the measurement matrix which is same for embedder side and decoder side, ***x*** is the sparse coefficients.

6. Now, these Sparse Measurements of watermark biometric image is used as secure watermark information.
7. Another biometric image is taken as host medium and compute size of biometric in term of row and column values.
8. Apply fourth level Discrete Wavelet Transform (DWT) decomposition on host biometric image and converts into various frequency bands like LL4, HL4, LH4 and HH4.
9. Apply SVD on HL4 component of DWT decomposition of host biometric image and chose Singular (S) matrix of host biometric image for embedding purpose.
10. Then Singular (S) matrix of host biometric image is modified according to Sparse Measurements of watermark biometric image using equation 3.

$$S_{Wat}^{HL4} = S_{Org}^{HL4} + W_{Sparse} \quad (3)$$

In formula (3), $\boldsymbol{W_{Sparse}}$ is the Sparse Measurements of watermark biometric image; $\boldsymbol{S_{Wat}}$ is modified Singular (S) matrix of HL4 wavelet coefficients of host biometric image; $\boldsymbol{S_{Org}}$ is original Singular (S) matrix of HL4 wavelet coefficients of host biometric image.

11. Apply inverse SVD on modified Singular (S) matrix with original U matrix and V matrix to generate modified HL4 component of host biometric image.
12. Apply fourth level inverse Discrete Wavelet Transform (IDWT) reconstruction on host biometric image to get watermarked biometric image.

2.2 Watermark Extraction & Reconstruction Procedure

The proposed watermark extraction and reconstruction procedure steps are described below:

1. Take watermarked biometric image, which may degrade or possibly be attacked by imposter is taken and apply fourth level Discrete Wavelet Transform (DWT) on watermarked biometric image and chose watermarked HL4 component coefficients.
2. Take original host biometric image and apply fourth level Discrete Wavelet Transform (DWT) on host biometric image and chose original HL4 component coefficients.
3. Extracted Sparse Measurements of watermark biometric image get using below equation 4.

$$W_{Extracted} = S_{Wat}^{HL4} - S_{Org}^{HL4} \quad (4)$$

In formula (4), $\boldsymbol{W_{Extracted}}$ is the Extracted Sparse Measurements of watermark biometric image; $\boldsymbol{S_{Wat}}$ is modified Singular (S) matrix of HL4 wavelet coefficients of watermarked biometric image; $\boldsymbol{S_{Org}}$ is original Singular (S) matrix of HL4 wavelet coefficients of host biometric image.

4. Then Applied CS recovery algorithm like Orthogonal Matching Pursuit (OMP) [18] using equation 5 with measurement matrix A which is generated at embedder side, level of sparsity and extracted Sparse Measurements of watermark biometric image getting from watermarked biometric image.

$$Sparse\_Coeff = OMP(W_{Extracted}, A, M) \quad (5)$$

In formula (5), ***Sparse_Coeff*** is extracted Sparse Coefficients of watermark biometric image; $\boldsymbol{W_{Extracted}}$ is the Extracted Sparse Measurements of watermark biometric image; ***M*** is level of Sparsity; ***A*** is measurement matrix which is same as generated at embedder side.

5. Apply inverse SVD on extracted Sparse Coefficients of watermark biometric image with original U and V matrix to generated details wavelet coefficients of watermark biometric image.
6. Apply inverse single level Discrete Wavelet Transform (DWT) on extracted details wavelet Coefficients and original approximation wavelet Coefficients and to get reconstructed version of watermark biometric image at detector side.

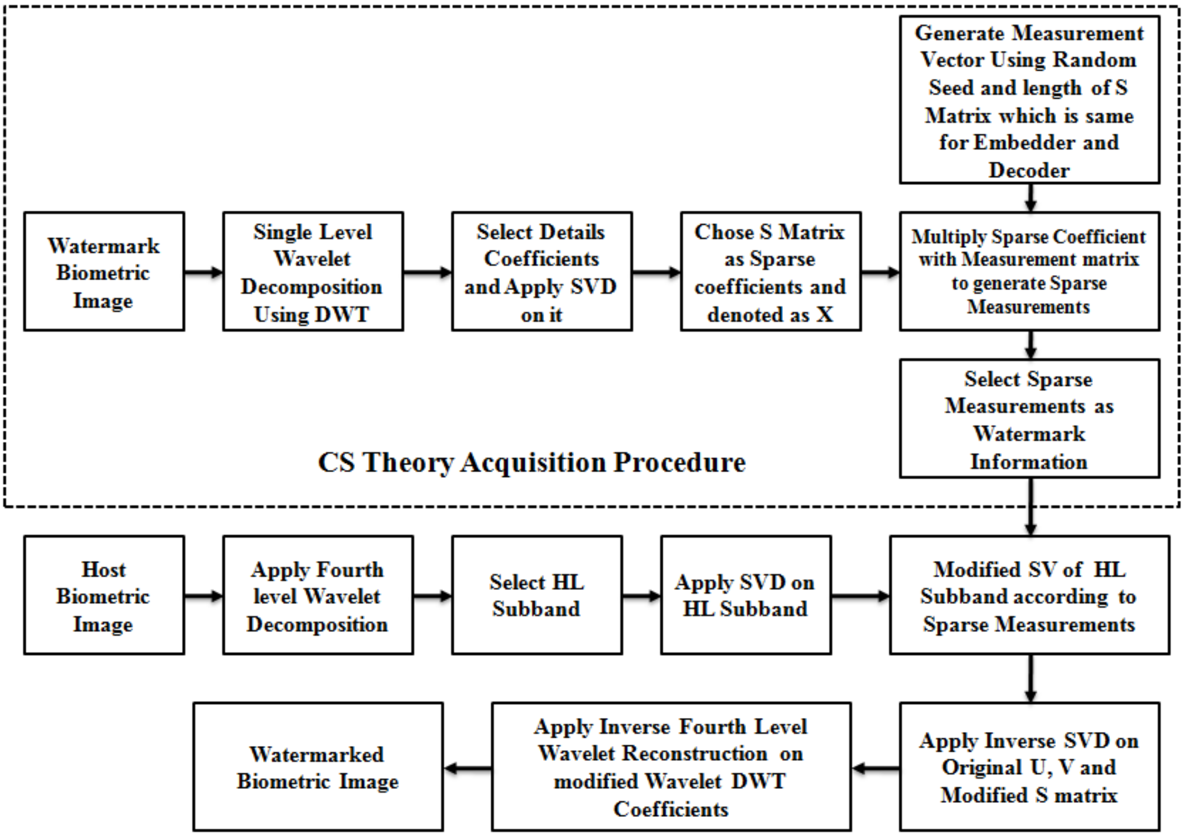

Generate Measurement Vector Using Random Seed and length of S Matrix which is same for Embedder and Decoder
Watermark Biometric Image
Single Level Wavelet Decomposition Using DWT
Select Details Coefficients and Apply SVD on it
Chose S Matrix as Sparse coefficients and denoted as X
Multiply Sparse Coefficient with Measurement matrix to generate Sparse Measurements
Select Sparse Measurements as Watermark Information
CS Theory Acquisition Procedure
Host Biometric Image
Apply Fourth level Wavelet Decomposition
Select HL Subband
Apply SVD on HL Subband
Modified SV of HL Subband according to Sparse Measurements
Watermarked Biometric Image
Apply Inverse Fourth Level Wavelet Reconstruction on modified Wavelet DWT Coefficients
Apply Inverse SVD on Original U, V and Modified S matrix

Fig.1. Watermark Preparation and Embedding Procedure

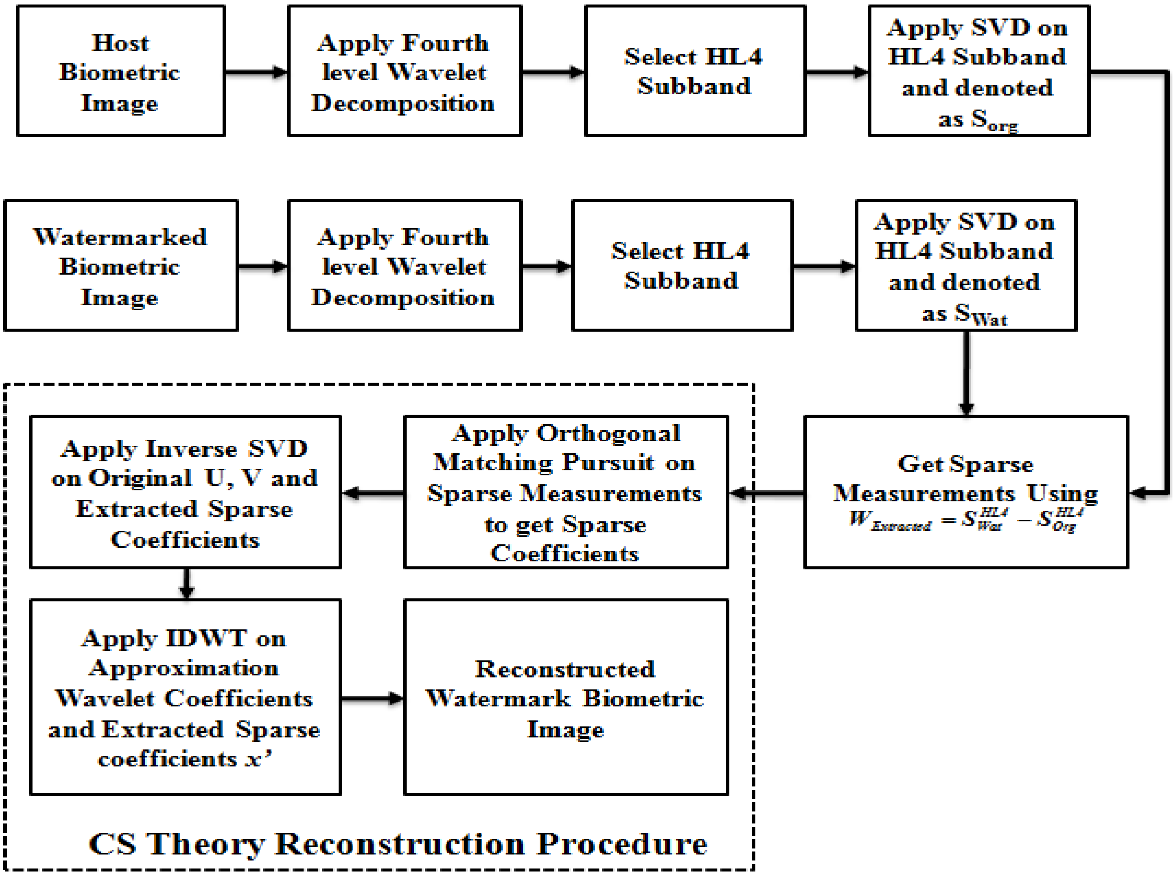

Host Biometric Image
Apply Fourth level Wavelet Decomposition
Select HL4 Subband
Apply SVD on HL4 Subband and denoted as S_{org}
Watermarked Biometric Image
Apply Fourth level Wavelet Decomposition
Select HL4 Subband
Apply SVD on HL4 Subband and denoted as S_{Wat}
Apply Inverse SVD on Original U, V and Extracted Sparse Coefficients
Apply Orthogonal Matching Pursuit on Sparse Measurements to get Sparse Coefficients
Get Sparse Measurements Using $W_{Extracted} = S_{Wat}^{HL4} - S_{Org}^{HL4}$
Apply IDWT on Approximation Wavelet Coefficients and Extracted Sparse coefficients x'
Reconstructed Watermark Biometric Image
CS Theory Reconstruction Procedure

Fig.2. Watermark Extraction and Reconstruction Procedure

3 Experimental Results

For testing of proposed watermarking technique, standard Indian face database [19] as host biometric image and standard FVC 2004 db4 database [20] as watermark biometric image taken for experiment. For experiment evaluation of proposed technique, 8 bit gray scale face image with size of 128 × 128 pixels is selected and monochromic fingerprint image with size of 128 × 128 pixels in selected.

The sparse measurements of watermark fingerprint image are generated using below procedure. First apply symmlet (sym1) discrete wavelet transform on watermark fingerprint image and take details wavelet coefficients with size of 8192 × 1. Then apply SVD on details on wavelet coefficients and decomposed into S, U and V matrix. Then Singular (S) matrix is chosen as Sparse Coefficients which is denoted as x with size of 8192 × 1. Generate measurement matrix A with size of 64 × 8192 using random seed which is same for embedder and detector. Sparse measurements of fingerprint image with size of 64 × 1 is generated using $W_{Sparse} = A_{64\times8192} \times x_{8912\times1}$. Then these sparse measurements of watermark fingerprint image are embedding into Singular (S) matrix value of HL4 wavelet coefficients of host face image to generated watermarked face image. Figure 3 shows original face image and watermarked face image using proposed watermarking technique.

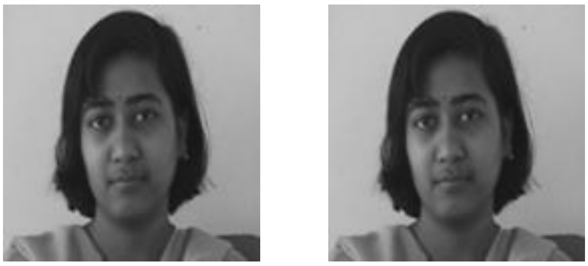


Fig.3. (a) Original Host Face Image (b) Watermarked Host Face Image

For reconstruction of watermark fingerprint image from its extracted sparse measurements, greedy algorithm like Orthogonal Matching Pursuit (OMP) [18] is used. OMP is selected because of it is easy to implement and having fast computational time compared to other CS recovery algorithms. The input of OMP algorithm is extracted Sparse Measurements of fingerprint image; correct Measurement matrix A and level of sparsity which is depend on size of fingerprint image. The output of OMP algorithm is sparse coefficients of watermark fingerprint image.

In the proposed watermarking technique, input of OMP algorithm is Sparse Measurements with size of 64 × 1; Measurement Matrix A with size of 64 × 8192; level of sparsity is 128. The output of OMP algorithm is sparse coefficients with size of 8192 × 1 for watermark fingerprint image. Then get details wavelet coefficients of watermark fingerprint image using inverse SVD on extracted sparse coefficients with original U and V after getting details wavelet coefficients of watermark fingerprint image, apply single level inverse DWT on extracted details wavelet coefficients and original approximation wavelet coefficients to get reconstructed watermark fingerprint image at detector side. Figure 4 shows original watermark fingerprint image and reconstructed watermark fingerprint image using proposed watermarking technique.

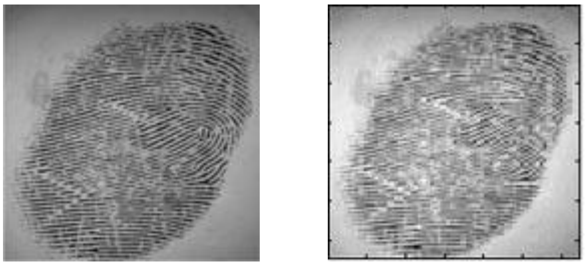


Fig.4. (a) Original Watermark Fingerprint Image (b) Reconstructed Watermark Fingerprint Image

The quality measures like PSNR, NCC and SSIM are used for calculation and evaluation for quality of watermarked face image and reconstructed watermark fingerprint image for proposed watermarking technique. In this paper, PSNR is used for compared original face image and watermarked face image; NCC is used for find correlation between original face image and watermarked face image at embedder side. The quality of watermark fingerprint image is calculated using SSIM [21] which is used to find similarity between original fingerprint image and reconstructed fingerprint image at detector side. SSIM value should be between 90 to 100 %.

For fragility test of proposed watermarking technique, various watermarking attacks like JPEG compression, addition of different noise, apply different filter and geometric attacks like cropping. Table 1 summarized the PSNR, NCC value between original host face image and watermarked host face image and SSIM value between original watermark fingerprint images and reconstructed watermark fingerprint image under consideration of above attacks. This proposed watermarking technique is fragile against all possible watermarking attacks based on SSIM values. Because of when watermarking attacks apply on watermarked face image, then SSIM value between original fingerprint image and reconstructed fingerprint image is less than 50 percentages which is shown in table 1.

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

Attacks	**NCC**	**PSNR (dB)**	**SSIM (%)**
No Attacks	1.00	99.00	99.71
JPEG Compression (Q = 90)	1.00	44.52	49.98
Gaussian Noise (μ =0, σ=0.001)	0.99	29.93	3.75
Salt & Pepper Noise (Noise Density = 0.005)	0.99	28.04	3.72
Speckle Noise (Variance = 0.004)	0.99	29.44	4.45
Median Filter (Size = 3 × 3)	1.00	45.34	44.00
Mean Filter (Size = 3 × 3)	0.98	27.53	0.30
Gaussian Low Pass Filter (Size = 3 × 3)	1.00	37.27	0.12
Histogram Equalization	0.98	22.07	0.63
Cropping	0.85	17.60	1.71

4 Proposed Watermarking Technique Effect over Multibiometric System

This proposed watermarking technique is used to secure biometric template at system database in multibiometric system. Fingerprint image is used as watermark and embed into face image for cross authentication of individual, therefore it is essential that insertion of fingerprint should not change performance of face system of multibiometric system. In proposed watermarking technique, fingerprint image is compressed and encrypted by CS theory. So that cs theory should not change performance of fingerprint system of multibiometric system. Here we have check verification and authentication performance of face and fingerprint system of multibiometric system for proposed watermarking technique.

In order to showcase the effect of watermark fingerprint on host face image, we have used face matching algorithm developed in [22, 23]. In order to showcase the effect on cs theory on watermark fingerprint, we have used fingerprint matching algorithm developed in [24, 25]. We have selected these two algorithms because output of these algorithms gives distance between query biometric image and its closest match in the database.

For effect of proposed watermarking technique on verification and authentication performance of multibiometric system, we have analyzed affect of proposed watermarking technique on individually verification and authentication performance of face and fingerprint system of multibiometric system.

4.1 Effect of Proposed Watermarking Technique on Face System of Multibiometric System

For calculation of verification and authentication performance of face system, we have stored 160 watermarked face image; 160 authentic face image and 160 fake face image. For verification performance of face system, we have calculated verification accuracy of original host face image and verification accuracy of watermarked face image using equation described in [26]. The verification accuracy of face recognition (using [22, 23]) is 96.25 % on original test faces. In proposed watermarking technique, the verification accuracy of face recognition is 95.00 % (after watermarking). The results verification accuracy of proposed watermarking technique for face system is summarized in table 2.

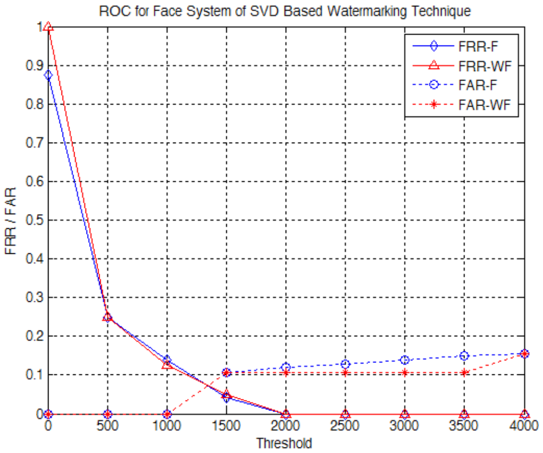
Table 2. Verification Accuracy of Proposed Watermarking Technique on Face System of Multibiometric System

$V_{OriginalFace}$	$V_{WatermarkedFace}$	$V_{HostFaceTemplate}$
96.25 %	95.00 %	99.35 %

From the result obtained using matching algorithm [22, 23] based on various thresholds, we have calculated four probabilities with named like FRR-F, FRR-WF, FAR-F and FAR-WF and based on this value, plot receiver operating characteristics (ROC) curve for face system of proposed watermarking technique as shown in figure 5. Based on figure 5, we have selected threshold distance 1500. Distance between fake face images compute with watermarked face images in stored database. The average distance is 6707.56 which are greater than selected threshold value. Also compute the distance between authentic face images with watermarked face images stored in database. The average distance between them is 385.40. Since the distance between authentic face images and their watermarked version database is less than selected threshold shows that face system of multibiometric system unaffected by proposed watermarking technique. These results are summarized in table 3.

Table 3. Average Distance between Watermarked, Authentic and Fake Face Images (for 160 Images)

Average Distance between Watermarked and Authentic Face Image	Average Distance between Watermarked and Fake Face Image	Selected Threshold
385.40	6707.56	1500



Where, FRR-F = FRR without Watermarking, FRR-WF = FRR with Watermarking, FAR-F = FAR without Watermarking, FAR-WF = FAR with Watermarking

Fig.5. ROC Curve of Proposed Watermarking Technique for Face System of Multibiometric System

4.2 Effect of Proposed Watermarking Technique on Face System of Multibiometric System

For calculation of verification and authentication performance of fingerprint system, we have stored 160 reconstructed watermark fingerprint image; 160 authentic fingerprint image and 160 fake fingerprint image. For verification performance of fingerprint system, we have calculated verification accuracy of original watermark fingerprint image and verification accuracy of reconstructed fingerprint image using equation described in [26]. The verification accuracy of fingerprint recognition (using [24, 25]) is 99.38 % on original test faces. In proposed watermarking technique, the verification accuracy of fingerprint recognition is unchanged after reconstruction of watermark fingerprint image forms its extracted sparse measurements using CS theory recovery process. The results verification accuracy of proposed watermarking technique for fingerprint system is summarized in table 4.

Table 4. Verification Accuracy of Proposed Watermarking Technique on Fingerprint System of Multibiometric System

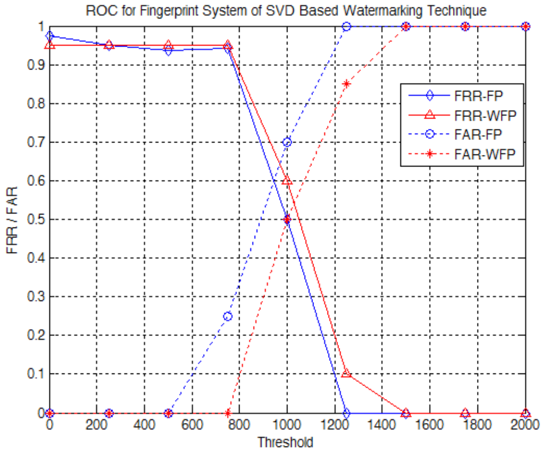
$V_{OriginalFingerprint}$	$V_{WatermarkReconstructedFingerprint}$	$V_{WatermarkFingerprintTemplate}$
99.38 %	99.38 %	99.38 %

From the result obtained using matching algorithm [24, 25] based on various thresholds, we have calculated four probabilities with named like FRR-FP, FRR-WFP, FAR-FP and FAR-WFP and based on this value, plot receiver operating characteristics (ROC) curve for fingerprint system of proposed watermarking technique as shown in figure 6. Based on figure 6, we have selected threshold distance 1000. Distance between fake fingerprints images compute with reconstructed watermark images in stored database. The average distance is 1034.82 which are greater than selected threshold value. Also compute the distance between authentic fingerprint images with reconstructed watermark fingerprint images stored in database. The average distance between them is 993.44. Since the distance between authentic watermark fingerprint images and their reconstructed watermark version database is less than selected threshold shows that fingerprint system of multibiometric system unaffected by proposed watermarking technique. These results are summarized in table 5.

Table 5. Average Distance between Reconstructed, Authentic and Fake Fingerprint Images (for 160 Images)

Average Distance between Reconstructed Watermark and Authentic Fingerprint Image	Average Distance between Reconstructed Watermark and Fake Fingerprint Image	Selected Threshold
993.44	1034.82	1000

Based on this analysis, a verification accuracy of 99.37 % was achieved for proposed watermarking technique based multibiometric system with enhancement in template security. Equal Error Rate (EER) difference for face system based on ROC curve shown in figure 5 is 0.3 % using watermarking and without watermarking. EER difference for fingerprint system based on ROC curve shown in figure 6 is 6.0 % using watermarking and without watermarking. Based on results shows in figure 5 and 6 that ROC curve of FAR and FRR values of face and fingerprint systems with watermarking is same as ROC curve of FAR and FRR values of face and fingerprint systems without watermarking which is indicated that proposed watermarking technique fulfilled the criteria of template protection technique.



Where, FRR-FP = FRR without Watermarking, FRR-WFP = FRR with Watermarking, FAR-FP = FAR without Watermarking, FAR-WFP = FAR with Watermarking

Fig.6. ROC Curve of Proposed Watermarking Technique for Fingerprint System of Multibiometric System

6 Conclusion & Future Work

A novel fragile biometric watermarking technique is proposed in hybrid domain using CS theory framework. This technique is not robust against JPEG compression, median filtering and noise addition like Gaussian noise, salt & pepper noise and speckle noise, histogram equalization and cropping attacks. This technique has been proposed for spoof detection of biometric template against spoofing attack at system database of multibiometric system. This technique is provide security against spoofing attack because it is difficult to generated two biometric modalities by imposter because of one is encrypted by CS theory framework and embed into other biometric modalities of same individual. A verification accuracy of 99.37 % was achieved for proposed watermarking technique based multibiometric system with enhancement in template security. The performance of the proposed watermarking technique has been compared with various existed watermarking techniques based on SVD in literature in term of PSNR value and performance of proposed watermarking techniques is better than existed watermarking techniques which are shown in table 6. In future, we have apply this proposed technique on other biometric modalities like iris, voice and palm print and take analysis for these biometric modalities.

Table 6. Values of Quality Measure like PSNR obtained by Proposed Watermarking Technique compared with Existed Watermarking Techniques in Literature

Techniques	PSNR (dB)
Mansouri Technique et al. [12]	68.33
Joshi Technique et al. [15]	93.29
Inamdar Technique et al. [27]	44.36
Kothari Technique et al. [28]	30.64
Jahan Technique et al. [29]	40.16
Chaudhary Technique et al. [30]	46.04
Sreedhanya Technique et al. [31]	61.15
Gupta Technique et al. [32]	50.67
Rege et al. [33]	44.08
Proposed Technique	99.00

7 Acknowledgment

We would like to thank Vidit Jain and his research team to provided standard Indian face image database.

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 and K. Nandakumar, “Biometric Authentication: System Security and User Privacy”, *IEEE Computer Society*, 2012, pp. 87-92.

[3] A. Jain, A. Ross and S. Pankanti, “Biometrics: A Tool for Information Security”, *IEEE Transactions on Information Forensics and Security*, 1(2), 2006, pp. 125-143.

[4] N. Ratha, J. Connell and R.Bolle, “Enhancing Security and Privacy in Biometric Based Authentication Systems”, *IBM Systems Journal*, 40 (3), 2001, 614-634.

[5] A. Jain and U. Uludag, “Hiding Fingerprint Minutiae in Images”, *Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2002, 97-102.

[6] P. S. L. M. Barreto, H.Y. Kim, and V. Rijmen, “Toward secure public-key block wise fragile authentication watermarking”, *Proc. IEEE*, 149 (2), 2002, pp. 57-62.

[7] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, “Hierarchical watermarking for secure

image authentication with localization", *IEEE Trans. Image Process.*, 11(6), 2002, pp. 585-595.

[8] L. Jaejin and S. W. Chee, "A watermarking sequence using parities of error control coding for image authentication and correction", *IEEE Trans. Consum. Electron*, 46 (2), 2000, pp. 313-317.

[9] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain watermarking: Embedding data in all frequencies", *in Proc. Workshop Multimedia Security*, Magdeburg, Germany, 2004, pp. 166-174.

[10] W. De-song, L. Jian-ping and W. Xiao-yang, "Biometric Image Integrity Authentication Based on SVD and Fragile Watermarking", *IEEE Congress on Image and Signal Processing*, 2008. *CISP '08*, 5, 2008, pp. 679-682.

[11] L. M. El Bakrawy, N. Ghali, A. Hassanien and J. Peters, "Strict Authentication of Multimodal Biometric Images Using Near Sets", *Soft Computing in Industrial Applications: Advances in Intelligent and Soft Computing by Springer*, 96, 2011, pp. 249-258.

[12] A. Mansouri, A. Mahmoudi Aznaveh and F. Torkamani Azar, "SVD Based Digital Image Watermarking Using Complex Wavelet Transform", *Sadhana © Indian Academy of Science, published by Springer – Verlag*, 34 (3), 2011, pp. 393-406.

[13] M. Vasta, R. Singh and A. Noore, M. Houck and K. Morris, "Robust Biometric Image Watermarking for Fingerprint and Face Template Protection", *IEICE Electronics Express*, 3(2), 2006, pp. 23-28.

[14] V. Joshi, M. Raval, P. Rege, S. Parulkar, "Multistage VQ Based Exact Authentication for biometric Images", *Computer Society of India (CSI) Journal of Computing*, 2(1-2), 2013, pp. 25-29.

[15] M. Joshi, V. Joshi and M. Raval, "Multilevel semi-fragile watermarking technique for improving biometric fingerprint system security", *in Intelligent Interactive Technologies and Multimedia*, Anupam Agrawal, R. C. Tripathi, Ellen Yi-Luen Do and M. D. Tiwari Eds., Springer – Verlag Berlin Heidelberg, 2011, pp. 272-283.

[16] C. Li, B. Ma, Y. Wang and Z. Zhang, "Protecting Biometric Templates Using Authentication Watermarking", *PCM 2010, Part I, LNCS 6297, Springer-Verlag Berlin Heidelberg*, 2010, pp. 709-718.

[17] E. Candès, "Compressive Sampling", *Proceedings of the International Congress of Mathematicians*, Madrid, Spain, 2006.

[18] J. Tropp and A. Gilbert, "Signal Recovery from Random Measurements via Orthogonal Matching Pursuit", *IEEE Transactions on Information Theory*, 53 (12), 2007, pp. 4655-4666.

[19] V. Jain, A. Mukherjee, 2002. The Indian Face Database,
http://vis-www.cs.umass.edu/~vidit/IndianFaceDatabase.

[20] For Fingerprint template Database: http://bias.csr.unibo.it/fvc2004/databases.asp

[21] Z. Wang and A. Bovik, "A Universal Image Quality Index", *J. IEEE Signal Processing Letters*, 9(3), 2004, pp. 84-88.

[22] M. Turk and A. Pentland, "Face Recognition Using Eigenfaces", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Maui, Hawaii, USA*, 1991, pp. 586-591.

[23] H. Moon and P. Phillips, "Computational and Performance aspects of PCA-based Face Recognition Algorithms", *Perception*, 30, 2001, pp. 303-321.

[24] A. Jain, S. Prabhakar and S. Pankanti, "A Filterbank based Representation for Classification and Matching of Fingerprint", *International Joint Conference on Neural Networks (IJCNN), Washington DC*, 1999, pp. 3284-3285.

[25] S. Prabhakar, "Fingerprint Classification and Matching Using a Filterbank", *Ph.D. Thesis*, Michigan State University, USA, 2001.

[26] M. Vasta, R. Singh and A. Noore, "Improving Biometric Recognition Accuracy and Robustness Using DWT and SVM Watermarking", *IEICE Electronics Express*, 1 (12), 2005, pp. 363-367.

[27] V. Inamdar and P. Rege, "Dual Watermarking Technique with Multiple Biometric Watermarks", *Sadhana © Indian Academy of Science, published by Springer – Verlag*, 29 (1), 2014, pp. 3-26.

[28] A. Kothari, "Design, Implementation and Performance Analysis of Digital Watermarking for Video", *Ph.D. Thesis*, JJTU, India, 2013.

[29] R. Jahan, "Efficient and Secure Digital Image Watermarking Scheme using DWT SVD and Optimized Genetic Algorithm Based Chaotic Encryption", *International Journal of Science, Engineering and Technology Research (IJSETR)*, 2(10), 2013, pp. 1943-1946.

[30] N. Chaudhary, D. Singh and D. Hussain, “Enhancing Security of Multimodal Biometric Authentication System by Implementing Watermarking Utilizing DWT and DCT”, *IOSR Journal of Computer Engineering*, 15(1), 2013, pp. 6-11.

[31] A. Sreedhanya and K. Soman, “Ensuring Security to the Compressed Sensing Data Using a Steganographic Approach”, *Bonfring International Journal of Advances in Image Processing*, 3(1), 2013, pp. 1-7.

[32] A. Gupta and M. Raval, “A Robust and Secure Watermarking Scheme Based on Singular Value Replacement”, *Sadhana © Indian Academy of Science, published by Springer – Verlag*, 37(4), 2012, pp. 425-440.

[33] V. Inamdar and P. Rege, “Face Features Based Biometric Watermarking of Digital Image Using Singular Value Decomposition for Fingerprinting”, *International Journal of Security and Its Applications*, 6(2), 2012.