IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. IV (May-Jun. 2016), PP 29-39
www.iosrjournals.org

Analysis of Effect of Compressive Sensing Theory and Watermarking on Verification and Authentication Performance of Multibiometric System

Rohit Thanki[1], Ved Vyas Dwivedi[1], Komal Borisagar[2]
[1]*Research Scholar, Faculty of Technology & Engineering, C. U. Shah University, Wadhwancity, India*
[2]*Pro Vice Chancellor, C. U. Shah University, Wadhwancity, India*
[3]*E.C. Department, Atmiya Institute of Technology & Science, Rajkot, India*

Abstract: *In this paper, watermarking technique with compressive sensing theory have been analysed for security of biometric image against imposter manipulations in the multibiometric system. The compressive sensing theory is used for providing security to watermark biometric image before embedded into the host biometric image. These proposed watermarking techniques can be embedded sparse information of the watermark biometric image into transform coefficients of a host biometric image. The various watermarking techniques with sparsity property of compressive sensing theory have been designed for providing security to biometric image in multibiometric system. The proposed multibiometric system is formed by using watermarked biometric image based system and reconstructed watermark biometric image based system. The experimental results show that verification performance and authentication performance of proposed multibiometric system does not affected due to these proposed watermarking techniques. This proposed multibiometric system can be used for high security applications.*

Keywords: *Authentication, CS Theory, Multibiometric System, Verification, Watermarking*

I. Introduction

Nowadays, the biometric authentication based system is used for automatic recognition of individuals. This biometric system has many advantages compared to a traditional biometric system like I-card, password etc. [1]. However, the biometric system has vulnerable to various attacks like spoofing of the template at system database, stone or modification of biometric templates at communication channel, modification of modules of system and noise in sensor etc. [1, 2]. For the security of biometric template against attacks such as spoofing of biometric templates and stone or modification of biometric templates at communication channel, digital watermarking technique is one the solution for security against these attacks [3].

To overcome these limitations of the biometric system, the researcher is introducing a new biometric system which is known as multimodal or multibiometric system. A. Ross and A. Jain described limitations of unimodal system and give solution of this limitation by introducing multibiometric system [3]. Authors in [4–6] described operation, designing approaches, challenges in designing and application of multibiometric systems which included various applications like physical access, civil ID and criminal ID.

The multibiometric system has more advantages compared to the unimodal biometric system, but there is a problem is associated with a multibiometric system such as designing of biometric image protection and authentication technique against modification attack in multibiometric system. So the problems of biometric image security raise concerns with the wide used for multibiometric systems, various biometric watermarking techniques with compressive sensing theory and different image transform have been described for the biometric image authentication in this paper. In the last decade, many researchers have proposed various watermarking techniques for biometric template protection in multibiometric system. The various watermarking techniques [7–18] proposed by various researchers where watermark biometric information embed into other biometric feature for biometric image protection at the communication channel and system database of any biometric system available in the literature.

The existing watermarking techniques available in the literature are mostly used for copyright protection of biometric data against imposter manipulations over a communication channel. The limitation of these techniques is there are not provide security to watermark biometric data before embedded into host data. There is another limitation of these techniques is that the effect of these techniques on verification accuracy and authentication performance of multibiometric system is missing. There is few watermarking techniques are available for copyright authentication of biometric data against imposter manipulations. Still research is required to design fragile watermarking technique for biometric image authentication against imposter manipulations in multibiometric system.

The main advantages of this proposed watermarking technique are that this technique used biometric image authentication against imposter manipulations and second this technique can be used for multi-level individual authentication. The novelty of this proposed technique is that sparsity property of compressive sensing theory is used for biometric data protection before embedding into host biometric data. Also effect of this proposed watermarking technique on performance of multibiometric system is analyzed which is missing in many existing watermarking techniques available in the literature. In this paper, watermarking techniques with compressive sensing theory are proposed for biometric data protection at communication channel and biometric data authentication at the system database of multibiometric system. The major difference of the proposed watermarking technique and existing watermarking techniques is that proposed watermarking technique is embedded encrypted watermark biometric data in term of sparse measurements into host biometric data while in existing watermarking techniques, watermark biometric data is directly embedded into host biometric data. The sparse measurements of watermark biometric data are generated using compressive sensing theory.

The rest of paper organized such as: section 2 gives the proposed approach for multibiometric system. Section 3 gives experimental results and effect of proposed watermarking techniques on the performance of multibiometric system and section 4 gives the conclusion of the paper.

II. Proposed Approach for Multibiometric System

The multibiometric watermarking is based on compressive sensing (CS) theory [19–20] and transform domain watermarking approach is described in this section. This proposed watermarking technique shows that application of signal processing theory, such as compressive sensing (CS) theory for biometric data security in multibiometric system. The CS theory provides two addition procedure such as acquisition procedure and reconstruction procedure in traditional watermarking approach.

In this proposed watermarking technique, watermark biometric image is encrypted in term of sparse measurements using compressive sensing (CS) theory before embedding into host biometric image. These sparse measurements of the watermark biometric image which is embedded into transform coefficients of a host biometric image at embedder side. At detector side, extracted sparse measurements of the watermark biometric image form watermarked biometric image and then watermark biometric image is reconstructed from its extracted sparse measurements using the compressive sensing recovery procedure. The proposed watermarking technique provides two level securities and two level authentications to biometric data by using watermarked biometric data and reconstructed watermark biometric data. The block diagram of proposed multibiometric system using CS theory and watermarking is shown in Figure 1. This watermarking technique is divided into three procedures such as watermark embedding, watermark extraction and template matching procedure.

2.1 Watermark Embedding Procedure

The steps of watermark preparation and embedding procedure are given below:

- Take a watermark biometric image and calculate the size of the image.
- Then Generate basis matrix with equal size of a watermark biometric image using image transform.
- Multiply transform basis matrix with the watermark biometric image to get sparse coefficients of a watermark biometric image.

  $$x = \Psi \times IWB \times \Psi' \quad (1)$$

  Where, x = Sparse Coefficients of Watermark Biometric Image, Ψ = Transform Basis Matrix, IWB = Original Watermark Biometric Image.
- Generate measurement matrix using normal distribution which is same for embedder and detector side.
- Generate sparse measurements of a watermark biometric image by multiplication of the measurement matrix with sparse coefficients of a watermark biometric image using equation 1.

  $$y = A \times x \quad (2)$$

  Where, y = Sparse Measurements of Watermark Biometric Image, A = Measurement Matrix, x = Sparse Coefficients of Watermark Biometric Image.
- Then multiply sampling factor with sparse measurements of watermark biometric image to get sparse watermark information which is embedded in host medium. The steps 1 to 5 are indicated CS theory acquisition procedure for watermark preparation. This sampling factor is used as the secret key.

  $$W_{Sparse} = \beta \times y \quad (3)$$

  Where, W_{Sparse} = Sparse Information of Watermark Biometric Image, β = Sampling Factor, y = Sparse Measurements of Watermark Biometric Image.

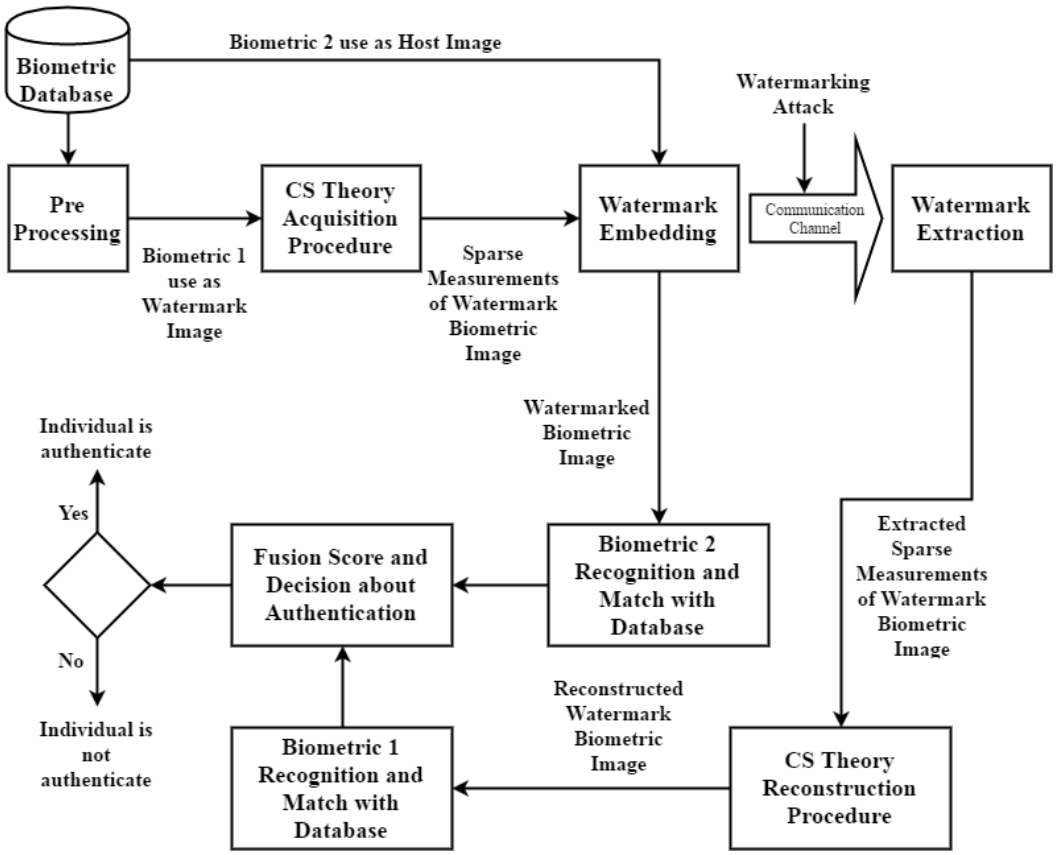

Fig. 1 Proposed Multibiometric System Using CS Theory and Watermarking

- Take another biometric image as host image and compute the size of the image. Then applied image transform on host biometric image to get transform coefficients of a host biometric image.
- The sparse information of the watermark biometric image is inserted into transform coefficients of a host biometric image using multiplicative watermarking equation [21, 22].

$$IWHB_{Transform\_Coefficients} = IHB_{Transform\_Coefficients} \times (1 + k * W_{Sparse}) \quad (4)$$

Where $IWHB_{Transform\_Coefficients}$ = Modified Transform Coefficients of Host Biometric Image, $IHB_{Transform\_Coefficients}$ = Transform Coefficients of Original Host Biometric Image, W_{Sparse} = Sparse Information of Host Biometric Image, k = Gain Factor.

- Apply an inverse image transform on modified transform coefficients to get a watermarked biometric image at embedder side.

2.2 Watermark Extraction Procedure

The steps of watermark extraction and reconstruction procedure are given below:

- Take a watermarked biometric image and applied image transform on it to get transform coefficients of a watermarked biometric image. Then select transform coefficients which are selected at watermark embedding.
- Take an original host biometric image and applied image transform on it to get transform coefficients of an original host biometric image. Then select transform coefficients which are selected at watermark embedding.
- Sparse information of the watermark biometric image is extracted using the reverse procedure of embedding.

$$W_{Extracted} = \frac{\left(\frac{IWHB_{Transform\_Coefficients}}{IHB_{Transform\_Coefficients}} - 1 \right)}{k} \quad (5)$$

Where, $IWHB_{Transform\_Coefficients}$ = Transform Coefficients of Watermarked Biometric Image, $IHB_{Transform\_Coefficients}$ = Transform Coefficients of Original Host Biometric Image, $W_{Extracted}$ = Extracted Sparse Information of Watermark Biometric Image, k = Gain Factor.

- Then sparse information of the watermark biometric image is divided by sampling factor to get actual sparse measurements of the watermark biometric image at detector side.

$$y_{Extracted} = \frac{W_{Extracted}}{\beta} \tag{6}$$

Where, $y_{Extracted}$ = Extracted Sparse Measurements of Watermark Biometric Image, $W_{Extracted}$ = Extracted Sparse Information of Watermark Biometric Image, β = Sampling Factor.

- After getting sparse measurements of the watermark biometric image, applied CS theory recovery algorithm such as orthogonal matching pursuit [28] on it to get extracted sparse coefficients of a watermark biometric image.

$$x_{Extracted} = OMP(y_{Extracted}, A, M) \tag{7}$$

Where, $x_{Extracted}$ = Extracted Sparse Coefficients of Watermark Biometric Image, $y_{Extracted}$ = Extracted Sparse Measurements of Watermark Biometric Image, OMP = Orthogonal Matching Pursuit, A = Measurement Matrix; M = Row Size of Watermark Biometric Image.

- Finally, the inverse transform basis matrix is multiplied with extracted sparse coefficients of a watermark biometric image to get reconstructed watermark biometric image at detector side.

$$IWB_{Reconstructed} = \Psi' \times x_{Extracted} \times \Psi \tag{8}$$

Where, $IWB_{Reconstructed}$ = Reconstructed Watermark Biometric Image, $x_{Extracted}$ = Extracted Sparse Coefficients of Watermark Biometric Image, Ψ = Transform Basis Matrix.

2.3 Template Matching

In this proposed multibiometric system, watermarked host biometric image based system and reconstructed watermark biometric image based system was used for two level authenticity checks.

- An original host biometric image as a query image is compared to a watermarked host biometric image which is stored in the system database and gets the matching score for watermarked host biometric image based system.
- An original watermark biometric image as a query image is compared with a reconstructed watermark biometric image which is stored in the system database and gets the matching score for reconstructed watermark biometric image based system.
- After getting the matching score for face image based system and watermark biometric image based system, applied an average sum of the matching score of watermarked host biometric image based system and reconstructed watermark biometric image based system to generate a matching score for multibiometric system.
- Individual authentication is possible if a matching score of multibiometric system is greater than selecting matching score.

III. Results and Effect of Proposed Watermarking Techniques on the Performance of Multibiometric System

3. 1 Experimental Setup and Results

For testing of proposed multibiometric system model using CS theory and watermarking, 8 bit grayscale face image with size of 128×128 pixels of 160 individuals from the Indian Face Database [23], EFI Face Database [24] taken as the Host biometric image and 8 bit grayscale fingerprint image with size of 128×128 pixels of 160 individuals from FVC 2002 DB3 Set B and FVC 2004 DB4 Set B [25] taken as the watermark biometric image. Then design various watermarking techniques with combination of CS theory which are given in Table 1. The few test images are shown in Figure 2.


H1


H2


H3


H4

W1 W2 W3 W4

Fig. 2 Test Face Images as Host Biometric Images and Test Fingerprint Images as Watermark Biometric Images

In these proposed watermarking techniques, sparsity property of various image transforms such as DCT, DWT and SVD are explored for the generation of sparse measurements of the watermark fingerprint image. Then these sparse measurements of the watermark fingerprint image are inserted into sparse coefficients of host face image to generate watermarked face image.

Table 1 Various Proposed Watermarking Techniques

Proposed Watermarking Techniques	**Transform Coefficients of Watermark Fingerprint Image Used for generation of Sparse Measurements**	**Transform Coefficients of Host Face Image Used for Watermark Embedding**
DWT Based Technique [33]	Details Wavelet Coefficients of Watermark Fingerprint Image	Approximation Wavelet Coefficients of Host Face Image
DCT Based Technique [34]	All Wavelet Coefficients of Watermark Fingerprint Image	All DCT Coefficients of Host Face Image
SVD Based Technique [35]	Singular value of All Wavelet Coefficients of Watermark Fingerprint Image	Singular value of Horizontal Wavelet Coefficients of Host Face Image
Curvelet Based Technique [36]	All DCT Coefficients of Watermark Fingerprint Image	High Frequency Curvelet Coefficients of Host Face Image

In the existing watermarking techniques, mid band frequency transform coefficients of a host biometric image is considered which is providing robustness to techniques. In these proposed watermarking techniques, low and high frequency transform coefficients of a host biometric image is considered which is provided fragility to proposed watermarking techniques. These coefficients are more vulnerable against various watermarking attacks such as signal processing, noise addition. The parameters such as gain factor k and sampling factor β are used to provide security with the addition to compressive sensing theory for watermark biometric image. These two factors are decided by the owner according to his or her requirement. In these proposed watermarking techniques, gain factor k is set to 0.2 and sampling factor β is set to 0.001.

These proposed watermarking techniques are tested by applying various standard watermarking attacks such as geometric attacks (Cropping), Signal Processing attacks (JPEG compression, addition of noise, applied different image filter) and histogram equalization attack on it. The watermarked face image quality is measured by PSNR. The reconstructed fingerprint image quality is measured by SSIM. The quality measure values for proposed watermarking techniques using H1 and W1 biometric image is summarized in Table 2.

Table 2 Quality Measures for Proposed Watermarking Techniques

Attack	**DWT Based Technique**		**DCT Based Technique**		**SVD Based Technique**		**Curvelet Based Technique**	
	PSNR (dB)	**SSIM**	**PSNR (dB)**	**SSIM**	**PSNR (dB)**	**SSIM**	**PSNR (dB)**	**SSIM**
No Attack	54.96	0.987	43.62	0.985	37.32	0.950	64.07	0.986
JPEG Compression (Q = 90)	35.44	0.987	36.54	0.676	36.55	0.142	35.17	0.012
Gaussian Noise (μ =0, σ=0.001)	38.13	0.987	36.27	0.641	34.57	0.161	37.63	0.002
Salt & Pepper Noise (Noise Density = 0.005)	40.03	0.987	35.37	0.670	33.77	0.134	36.61	0.003
Speckle Noise (Variance = 0.004)	37.97	0.987	29.09	0.676	34.51	0.174	37.50	0.002
Median Filter (size = 3 × 3)	36.75	0.987	35.60	0.671	37.91	0.165	36.28	0.008
Mean Filter (size = 3 × 3)	25.13	0.987	25.49	0.664	32.19	0.005	25.04	0.008
Gaussian Low Pass Filter (size = 3 × 3)	34.61	0.987	31.20	0.665	36.94	0.019	34.11	0.004
Histogram Equalization	19.66	0.987	19.32	0.675	19.66	0.008	19.47	0.003
Cropping	16.17	0.986	15.87	0.663	34.77	0.678	16.17	0.002

For individual authentication and decision of fragility of proposed watermarking techniques, SSIM value between the watermark and extracted watermark fingerprint images must be greater than 0.90. SSIM values in Table 2 are indicated that DWT based technique is robust against all possible watermarking techniques. While other proposed watermarking techniques such as DCT, SVD and Curvelet, SSIM value is less than 0.9 when watermarking attacks is applied on watermark face image which is indicated that these three proposed watermarking techniques are fragile against possible watermarking attacks.

When watermarking attacks is applied on watermarked face image in these DCT, SVD and Curvelet based proposed watermarking techniques, then the watermark fingerprint image can't reconstruct successfully at detector side. This is indicated that DCT, SVD and Curvelet based technique used for biometric data authentication at system database of multibiometric system.

3. 2 Effect of Proposed Watermarking Techniques on the Performance of Multibiometric System

Two procedures such as verification and authentication performance are important for any multibiometric system. When any biometric data protection technique is designed for multibiometric system, then this technique should not degrade performance of multibiometric system. In the verification mode, an individual check his / her identity and the system determine if the individual is true or false. In the authentication mode, the system recognizes an individual from the entire stored database [1, 32]. The performance of proposed watermarking technique based multibiometric system can be evaluated by Verification Performance, False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (EER). In this paper, the watermarked face based system and reconstructed fingerprint based system are made face-fingerprint based multibiometric system. The effect of proposed watermarking techniques on verification and authentication performance of face-fingerprint based multibiometric system has been analysed in this paper. In these proposed watermarking techniques, sparse measurements of the watermark fingerprint image are inserted into host face image; therefore checked that insertion of fingerprint image should not change the performance of face biometric system. Also, checked performance fingerprint biometric image should not change due to compressive sensing (CS) theory procedure.

For the verification and authentication performance of the proposed face-fingerprint based multibiometric system, individual performance of face system and fingerprint system has been calculated. Then average score approach is applied on individual performance of face based system and fingerprint based system for calculation of verification and authentication performance of multibiometric system. For performance of face and fingerprint system, LDA based face recognition algorithm developed by researchers [26, 27] and fingerprint recognition algorithm developed by Prabhakar and its research team [28, 29] is applied. We have selected these algorithms because output of these algorithms gives Euclidean distance between query biometric image and its closest match in the system database. The verification performance, FAR and FRR are calculated by the equation given by various researchers [37, 38].

For analysis of verification and authentication performance of proposed face-fingerprint based multibiometric system, 160 watermarked face images and 160 reconstructed fingerprint images are stored in the system database. Then, take 50 images from Indian face database [23] and 110 face images from FEI face Database [24] as authentic face images, 50 images from FEI face Database and 110 face images from CVL face database [30, 31] as fake face images as query images and also taken 80 images from FVC2002 DB3 setB [25] and 80 images from FVC2004 DB4 setB [25] as authentic fingerprint images, 80 images from FVC2002 DB4 setB [25] and 80 images from FVC2004 DB3 setB [25] as fake fingerprint images as query images.

Based on matching score obtained by recognition algorithms, the average distance for proposed watermarking techniques based multibiometric system is calculated. The results are summarized in Table 3.

Table 3 Average Distance between Watermarked Face, Reconstructed Fingerprint, Authentic and Fake Biometric Database (for 160 Images)

Technique	Average Distance for Face System		Average Distance for Fingerprint System		Average Distance for Multibiometric System	
	Between Authentic & Watermarked Database	Between Fake & Watermarked Database	Between Authentic & Reconstructed Database	Between Fake & Reconstructed Database	Between Authentic & Watermarked, Reconstructed Database	Between Fake & Watermarked, Reconstructed Database
DWT Based Technique	28.09	505.74	536.27	711.99	282.18	608.87
DCT Based Technique	40.61	513.13	616.10	754.20	328.36	633.67
SVD Based Technique	36.07	517.08	502.18	717.93	269.13	617.51
Curvelet Based Technique	18.06	511.63	681.80	779.19	349.93	645.41

The threshold distance selected based on this is 450. The average threshold value between fake biometric database with watermarked biometric and reconstructed biometric database is calculated. The average distance value for imposter biometric database is 626.37 which are greater than the selected threshold distance. The average distance value between genuine biometric database with watermarked biometric and reconstructed biometric database is also calculated. The average distance value for genuine biometric database is 307.4 which is less than the selected threshold distance. Since the threshold between original multibiometric data and their watermarked & reconstructed database is less than selected threshold distance, performance of multibiometric system remains unaffected due to these proposed watermarking techniques.

The verification performance of proposed watermarking technique based multibiometric system for different threshold can be calculated using equation 9 [36] and results are summarized in Table 4.

$$V(Face) = \frac{(No.ofMatchingScore) < Selected\_Threshold}{TotalNo.ofMatchingScore}$$

$$V(Fingerprint) = \frac{(No.ofMatchingScore) < Selected\_Threshold}{TotalNo.ofMatchingScore} \quad (9)$$

$$V(Multibiometric) = \frac{V(Face) + V(Fingerprint)}{2}$$

Where, *Matching Score* = Matching Results between Authenticate Biometric Image and Original Biometric Image in the Database, *V (Fingerprint)* = Verification Performance of Reconstructed Watermark Fingerprint Based System, *V (Face)* = Verification Performance of Watermarked Face Based System, *V (Multibiometric)* = Verification Performance of Proposed Face-Fingerprint based Multibiometric System.

The False Rejection Rate (FRR) and False Acceptance Rate (FAR) for proposed watermarking techniques based multibiometric system are calculated using equation 10 [37, 38]. There is a condition of any biometric system is used in high security application is that FAR value must be low compared to FRR value [32, 37, 38].

$$FRR = \frac{(No.ofMatchingScore) > Selected\_Threshold}{TotalNo.ofMatchingScore}$$

$$FAR = \frac{(No.ofMatchingScore) \leq Selected\_Threshold}{TotalNo.ofMatchingScore} \quad (10)$$

Where, *Matching Score* = Matching Results between Query Biometric Image and Its Closest Matched Biometric Image in the Database, *FAR* = False Acceptance Rate, *FRR* = False Rejection Rate.

Table 4 Verification Performance of Proposed Watermarking Techniques based Multibiometric System

Threshold	DWT Based Technique	DCT Based Technique	SVD Based Technique	Curvelet Based Technique
0.0	0.000	0.000	0.003	0.000
0.1	0.041	0.003	0.022	0.025
0.2	0.191	0.219	0.113	0.103
0.3	0.409	0.381	0.247	0.456
0.4	0.528	0.553	0.484	0.669
0.5	0.650	0.678	0.762	0.794
0.6	0.784	0.788	0.888	0.884
0.7	0.909	0.872	0.966	0.950
0.8	0.978	0.969	0.981	0.975
0.9	0.997	0.988	0.994	0.991
1.0	1.000	1.000	1.000	1.000

Based on results shows in Table 4 is indicated that verification performance of proposed watermarking techniques based multibiometric system are greater than 0.850 when selected threshold greater than 0.7. The verification performance curve for proposed watermarking techniques based multibiometric system is shown in Figure 3.

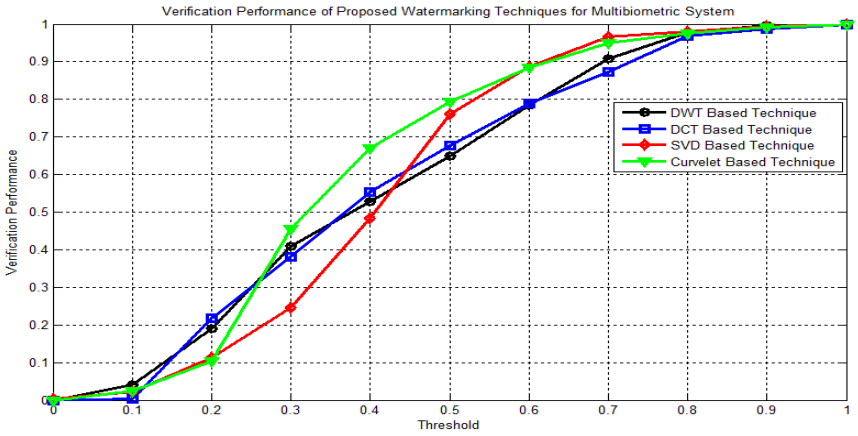

Fig. 3 Verification Performance Curve of Proposed Watermarking Techniques based Multibiometric System

For the value of FRR and FAR for different threshold values for proposed face-fingerprint based multibiometric system, we have first calculate FRR and FAR values for watermarked face based system and reconstructed watermark fingerprint based system. Then the authentication performance of face-fingerprint based multibiometric system is calculated using equation 11. The results are summarized in Table 5.

$$FRR(Multibiometric) = \frac{FRR(F)_{Selected\_Threshold} + FRR(FP)_{Selected\_Threshold}}{2}$$

$$FAR(Multibiometric) = \frac{FAR(F)_{Selected\_Threshold} + FAR(FP)_{Selected\_Threshold}}{2}$$

(11)

Where, *FRR (Multibiometric System)* = False Rejection Rate for Proposed Face-Fingerprint based Multibiometric System, *FAR (Multibiometric System)* = False Acceptance Rate for Proposed Face-Fingerprint based Multibiometric System, *FRR (F)* = False Rejection Rate for Watermarked Face based Multibiometric System, *FAR (F)* = False Acceptance Rate for Watermarked Face based Multibiometric System, *FRR (FP)* = False Rejection Rate for Reconstructed Watermark Fingerprint based Multibiometric System, *FR (FP)* = False Acceptance Rate for Reconstructed Watermark Fingerprint based Multibiometric System

Table 5 FRR and FAR values of Proposed Watermarking Techniques for Multibiometric System

Threshold	FRR DWT	FAR DWT	FRR DCT	FAR DCT	FRR SVD	FAR SVD	FRR Curvelet	FAR Curvelet
0.0	1.000	0.000	1.000	0.000	1.000	0.009	1.000	0.000
0.1	0.959	0.006	0.997	0.003	0.972	0.038	0.972	0.009
0.2	0.809	0.034	0.781	0.034	0.909	0.059	0.884	0.038
0.3	0.591	0.084	0.619	0.078	0.769	0.106	0.541	0.066
0.4	0.472	0.138	0.447	0.128	0.550	0.156	0.325	0.131
0.5	0.350	0.244	0.322	0.200	0.259	0.266	0.206	0.225
0.6	0.216	0.400	0.213	0.331	0.122	0.494	0.116	0.409
0.7	0.091	0.625	0.128	0.584	0.047	0.716	0.050	0.631
0.8	0.022	0.856	0.031	0.797	0.016	0.922	0.025	0.831
0.9	0.003	0.981	0.013	0.959	0.003	0.988	0.007	0.972
1.0	0.000	1.000	0.000	1.000	0.000	1.000	0.000	1.000

Based on values in Table 5, plot FRR/ FAR vs. Threshold curve and receiver operating characteristics (ROC) curve for watermarked face based system, reconstructed watermark fingerprint based system and proposed face-fingerprint based multibiometric system is shown in Figure 4 and 5, respectively. Equal Error Rate (EER) is a point on FRR/FAR vs. Threshold Curve shown in Figure 4 where FAR and FRR has the same value. The EER value for proposed multibiometric systems is summarized in Table 6.

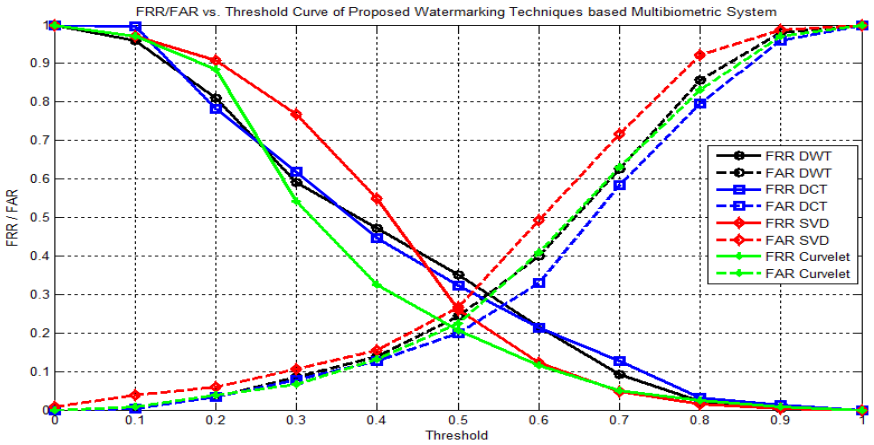

Fig. 4 FRR/FAR Vs. Threshold Curve of Proposed Watermarking Techniques based Multibiometric System

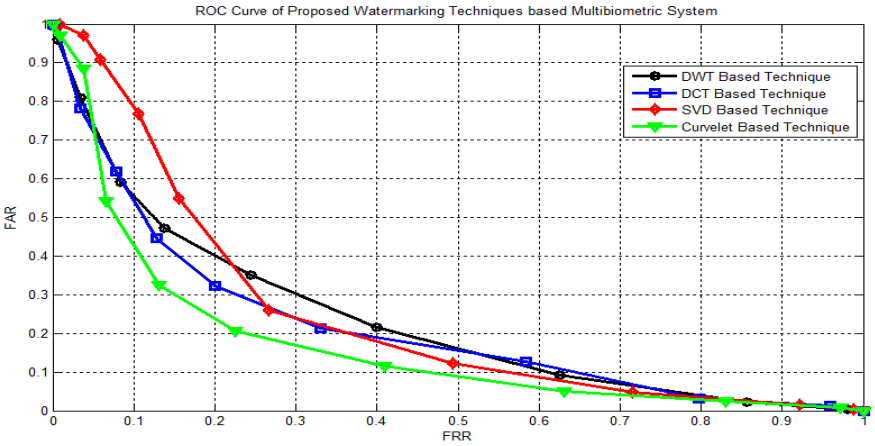

Fig. 5 Receiver Operating Characteristics (ROC) Curve of Proposed Watermarking Techniques based Multibiometric System

Table 6 Performance Evaluation of Proposed Watermarking Techniques based Multibiometric System

Proposed Technique	False Acceptance Rate (FAR)	False Rejection Rate (FRR)	Equal Error Rate (EER)
DWT Based Technique	**0.069**	**0.7**	**0.301**
DCT Based Technique	**0.075**	**0.7**	**0.267**
SVD Based Technique	**0.052**	**0.7**	**0.264**
Curvelet Based Technique	**0.041**	**0.7**	**0.217**

Based on ROC Curve shown in Figure 5, where FRR value 0.7 is chosen as common value for these three systems, measure FAR value at that point is summarized in Table 6. The results in Table 6 show that FAR values are low compared to FRR Value for these three systems, which is indicated that proposed watermarking techniques based multibiometric system used for high security applications. The EER value of the curvelet based technique is less than other proposed techniques indicated that the performance of curvelet technique based multibiometric system is better compared to other proposed techniques based multibiometric system.

IV. Conclusion

In this paper, watermarking technique with compressive sensing (CS) theory is proposed for biometric data protection at communication channel and biometric data authentication at system database against imposter manipulations in multibiometric system. There are a few observations about the advantages and limitations of these proposed watermarking techniques are mentioned below:

1. The compressive sensing theory is used to provide more security to watermark biometric image before embedding into host image.
2. These proposed watermarking techniques provides security to biometric image against modification attack because it is difficult to imposter to generate two biometric images where one biometric image which encrypted by CS theory is embedded into another biometric image.

3. These proposed watermarking techniques do not degraded the verification and authentication performance of multibiometric system.
4. The analysis of verification and authentication performance tables of proposed watermarking techniques show that these proposed watermarking technique based multibiometric system can be used in applications such as online banking transactions and physical access control where high security is required.
5. The limitations of the proposed watermarking techniques are that required correct measurement matrix generation mechanism at detector side, two additional procedures of CS theory introduces some complexity in proposed watermarking techniques.

References

Journal Papers:

[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.), pp. 49-79*, Springer, 2012.

[2] A. Ross and A. Jain, "Multimodal Biometrics: An Overview", *In Proceedings of 12th European Signal Processing Conference (EUSIPCO), September 2004*, pp. 1221-1224.

[3] A. Ross & A. K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letters, 24 (13)*, pp. 2115-2125, 2003.

[4] M. Thieme, "Multimodal Biometric Systems: Applications and Usage Scenarios", *Biometric Consortium Conference, Arlington, VA*, 2003.

[5] Teddy KO, "Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition", *Proceeding of the IEEE 34th Applied Imagery and Pattern Recognition Workshop (AIPR05)*, 2005.

[6] M. Agrawal, "Design Approaches for Multimodal Biometric System", *M. Tech. Thesis*, Department of Computer Science and Engineering, IIT, Kanpur, August 2007.

[7] P. Bedi, R. Bansal R and P. Sehgal, "Multimodal Biometric Authentication using PSO based Watermarking", *Procedia Technology 4*, pp. 612-618, 2012.

[8] S. Edward, S. Sumanthi and R. Ranihemamalini, "Person Authentication Using Multimodal Biometrics with Watermarking", In *Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN)*, pp. 100-104, 2011.

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

[10] A. Jain and U. Uludag, "Hiding Biometric Data", *IEEE Transactions on Pattern Analysis and Machine Intelligence, 25 (11)*, pp. 1494-1498, 2003.

[11] R. Motwani, "A Voice Based Biometric Watermarking Scheme for Digital Rights Management of 3D Mesh Models", *Ph.D. Thesis*, University of Nevada, Reno, 2010.

[12] A. Naik and Holambe, "Blind DCT Domain Digital Watermarking for Biometric Authentication", *International Journal of Computer Applications, 16 (1)*, pp. 11-15, 2010.

[13] A. Noore, R. Singh, M. Vasta and M. Houck, "Enhancing Security of Fingerprint through Contextual Biometric Watermarking", *In Proceedings of Forensic Sci. Int., 169*, pp. 188-194, 2007.

[14] M. Paunwala and S. Patnaik, "Biometric Template Protection with DCT Based Watermarking", *Machine Vision and Applications, 25 (1)*, pp. 263-275, 2014.

[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*, pp. 272-283, 2013.

[16] 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)*, pp. 47-60, 2012.

[17] M. Qi, Y. Lu, N. Du, Y. Zhang, C. Wang and J. Kong, "A Novel Image Hiding Approach Based on Correlation Analysis for Secure Multimodal Biometrics", *Journal of Network and Computer Applications, 33 (3)*, pp. 247-257, 2010.

[18] 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)*, pp.6-11, 2013.

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

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

[21] I. Cox, J. Kilian, T. Shamoon and F. Leighton, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing, 3 (12)*, pp. 1673-1687, 1997.

[22] F. Shih, "Digital Watermarking and Steganography – Fundamentals and Techniques", CRC Press, pp. 39-41, 2008.

[23] Indian Face Database, 2002, http://vis-www.cs.umass.edu/~vidit/IndianFaceDatabase.

[24] FEI Face Database: http://fei.edu.br/~cet/facedatabase.html

[25] Fingerprint Database: http://csr.unibo.it/fvc2004/, http://csr.unibo.it/fvc2002/

[26] J. Yang, Y. Hua and K. William, "An Efficient LDA Algorithm for Face Recognition", *In Proceedings of the International Conference on Automation, Robotics and Computer Vision (ICARCV 2000)*, pp. 34-47, 2000.

[27] J. Lu, N. Plataniotis and A. Venetsanopoulos, "Face Recognition using LDA based Algorithms", *IEEE Transactions on Neural Networks, 14 (1)*, pp. 195-200, 2003.

[28] A. Jain, S. Prabhakar and S. Pankanti, "A Filterbank based Representation for Classification and Matching of Fingerprints", *International Joint Conference on Neural Networks*, pp.3284-3285, 1999.

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

[30] P. Peter, CVL Face Database: http://www.lrv.fri.uni-lj.si/facedb.html

[31] F. Solina, P. Peer, B. Batagelj, S. Juvan and J. Kova, "Color-based face detection in the '15 seconds of fame' art installation", *Mirage 2003, Conference on Computer Vision / Computer Graphics Collaboration for Model-based Imaging, Rendering, Image Analysis and Graphical special Effects, March 10-11, 2003, INRIA Rocquencourt, France, Wilfried Philips, Rocquencourt, INRIA*, pp. 38-47, 2003.

[32] "Biometrics and Standards", ITU-T Technology Watch Report, December 2009.

[33] R. Thanki and K. Borisagar, "Discrete Wavelet Transform and Compressive Sensing Based Multibiometric Watermarking – A Novel Approach to Embed Watermark into Biometric", *Proceedings of the 2nd International Conference on Emerging Technology Trends in Electronics, Communication & Networking (ET2ECN – 2014),* pp. 102-107, December 2014.
[34] R. Thanki and K. Borisagar, "Biometric Image Protection Using Compressive Sensing and DCT based Watermarking Technique", *proceedings of RK University's First International Conference on Research & Entrepreneurship (ICRE – 2016),* pp. 1239-1248, January 2016.
[35] R. Thanki and K. Borisagar, "Multibiometric Template Security Using CS Theory-SVD Based Fragile Watermarking Technique", *WSEAS Transactions on Information Science and Applications*, vol. 12, pp. 1 – 10, April 2015.
[36] R. Thanki and K. Borisagar, "Biometric Watermarking Technique Based on CS Theory and Fast Discrete Curvelet Transform for Face and Fingerprint Protection", *Advances in Intelligent Systems and Computing Series*, vol. 425, pp. 133 – 144, December 2015.
[37] R. Giot, M. El-Abed and C. Rosenberger, "Fast Computation of the Performance Evaluation of Biometric Systems: Application to Multibiometrics", *Future Generation Computer Systems, 1*, pp. 1-30, February 2012.
[38] F. Fernandez, J. Fierrez and J. Garcia, "Quality Measures in Biometric Systems", *IEEE Security and Privacy*, pp. 52-62, December 2012.