Robust and Secure Watermarking Using Sparse Information of Watermark for Biometric Data Protection

Rohit M. Thanki, *Student Member, IEEE,* Ved Vyas Dwivedi, and Komal R. Borisagar

***Abstract*—Biometric based system is used for security purpose and identity of the person in many organizations in the present world. This biometric based system has several vulnerable points. Two of vulnerable points are the security of biometric data at database and security of biometric data at communication channel between two modules of biometric based system. In this paper proposed a robust watermarking scheme using the sparse information of watermark biometric. This scheme is proposed for the protection of biometric templates at the communication channel of biometric based system. The sparse information of watermark biometric data is generated using detail wavelet coefficients and compressive sensing. Then sparse information of watermark biometric data is embedded into DCT coefficients of host biometric data. This proposed scheme is robust to common signal processing and geometric attacks such as JPEG compression, adding noise, filtering, and cropping, histogram equalization. This proposed scheme has more advantages and high quality measures compared to existing schemes in the literature.**

***Index Terms*—Compressive Sensing, Multimodal Biometric, Robustness, Sparse Domain Watermarking, Spoofing Attack.**

I. Introduction

THE biometric based system has been used rapidly in many organizations for person authentication. This system is provided security against entering the unauthenticated person into the system. This biometric based system is mainly used at airport, laboratory and office for security purpose. This biometric based system having more advantages as compared to a traditional person recognition system. This biometric based system is used biometric characteristics of a person which is unique for every person [1]. But this biometric based system has several issues to deal with [2]. There are main two issues associated with biometric based system such biometric data tempering at the database and at communication channel between two modules of the system [1, 2]. There are other issues such as sensor noise, inter-class variations, distinctiveness and non-universality of the template also associated with the biometric based system.

Then researchers have introduced a new biometric based system around 2003. This system is called as multimodal biometric based systm [3].This system has taken takes two or more biometric template characteristics of the person for authentication purpose. There are two issues associated with this multimodal biometric based system is the generation of multimodal biometric data and protection of this data [3]. For these two issues, one of the solutions is a digital watermarking technique which can be used for generating as well as provided protection multimodal biometric data against an attack on the communication channel of biometric based system.

There are many schemes proposed and described by researchers in the last decade. These schemes for proposed for biometric template protection at communication channel between two modules. These proposed schemes are faced problems such as less quality of the template, less computational security and less payload capacity. Some of these schemes are briefly reviewed related to the proposed work in the following.

A. K. Jain and his research team proposed the application of digital watermarking scheme in biometric based system. Authors in [4] proposed multimedia content protection framework which is based on biometric data of the person. Authors in [5] described watermarking scheme based on correlation approach of PN sequences and DCT for embedding iris image feature into face image. This scheme is provided two levels of privacy where the face image is used as verification and extracted iris features for cross verification of individuals. Authors in [6] proposed a robust watermarking scheme for embeds fingerprint data into a region of interest of another fingerprint image by using a segmentation technique. This proposed scheme is provided robustness against noise, geometric and filter attack.

Authors in [7] proposed Particle Swarm Optimization based watermarking approach for multimodal biometric data security. They have described that PSO algorithm is used to find best DCT coefficient for face image for watermark embedding. The fingerprint image and demographic data which is watermark information are embedded into these coefficients using quantization. They have also claimed that this scheme provided more security and reliable system for personal recognition. Authors in [8] proposed a watermarking scheme for improvement of the capacity of multimodal biometric templates. In this scheme, a watermark biometric data are embedded into low frequency AC coefficient of 8×8 DCT blocks of standard test images. Authors in [9] proposed multimodal biometric watermarking scheme using DCT and Phase Congruency Model for improved recognition and authentication of a person. In this scheme, the facial features are embedded into the fingerprint

Rohit M. Thanki is Ph.D. Research Scholar of the Department of Electronics and Communication Engineering, C. U. Shah University, Wadhwancity, Gujarat, India, E-mail: rohitthanki9@gmail.com.

Ved Vyas Dwivedi is Pro vice Chancellor, C. U. Shah University, Wadhwancity, Gujarat, India, E-mail: vedvyasdwivediphd@gmail.com.

Komal R. Borisagar is Associate Professor,E. C. Department, Atmiya Institute of Technology and Science, Rajkot, India, E-mail: krborisagar@aits.edu.in.

image for e-passport and e-identification card.

The motivation of the present work arises from developing a sparse watermarking algorithm which embedded offline fingerprint as a watermark biometric data for security of biometric data in the multibiometric system. the fingerprint of every person is a unique and accepted trait for authentication purposed in worldwide [1]. In this paper, transform domain based scheme with compressive sensing (CS) procedure is proposed. In this scheme, the sparse information of a watermark biometric image of the individual as a watermark is embedded into highest AC coefficients of DCT of host biometric image. The sparse information of a watermark biometric image is generate using CS theory framework. The watermarking idea borrowed from papers [10, 11, 12, and 13] with significant modifications and improvements in implementation. The work also goes a step further where compression as well as protection of biometric data taken place simultaneously.

II. Used Hypothesis

First review few basics of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) which are used for embedding watermark biometric into host medium and for generation of sparse measurements of watermark biometric image, respectively. The compressive sensing theory framework is used for generates sparse measurement vector form watermark biometric image at embedder side. The watermark biometric image is reconstructed from its extracted sparse measurement vector at detector side.

A. Discrete Cosine Transform (DCT)

The discrete cosine transform is used for converting images into its frequency domain. The advantage of cosine transform is decomposed the image into the same size into the frequency domain. The DCT decomposition of any image in different frequency coefficients is shown in Figure 1. The DC coefficients have lower band frequency coefficients which are perfect for watermark embedding but creates a problem of perception and vice-versa is true for high frequency AC coefficients [8,14].

Fig. 1. Energy Distribution of DCT of Image

As a trade-off, in the proposed scheme, sparse information of watermark biometric is embedded into highest AC coefficients of DCT of host biometric image. Embedding of sparse information of watermark biometric is done by modulating highest AC coefficients of DCT according to gain factor and values of sparse measurement vector.

B. Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform is used for a computational tool for various applications of signal and image processing (e.g., The FBI uses wavelet transforms for compressing digitally scanned fingerprint images) [33]. The Discrete Wavelet Transform (DWT) is decomposed the image into various coefficients of frequency such as approximation coefficients and detail coefficients. Where approximation coefficients have a low frequency of the components and detail coefficients have a higher frequency of the components. The Discrete Wavelet Transform has a property such as the introduction of sparseness in wavelet coefficients of the image. Sparseness is defined as how many coefficients having non-zero values in signal or image [17]. The DWT decomposition of any image vector in various frequency coefficients is shown in figure 2. Figure 2 shows that detail wavelet coefficients have sparser than approximation wavelet coefficients.

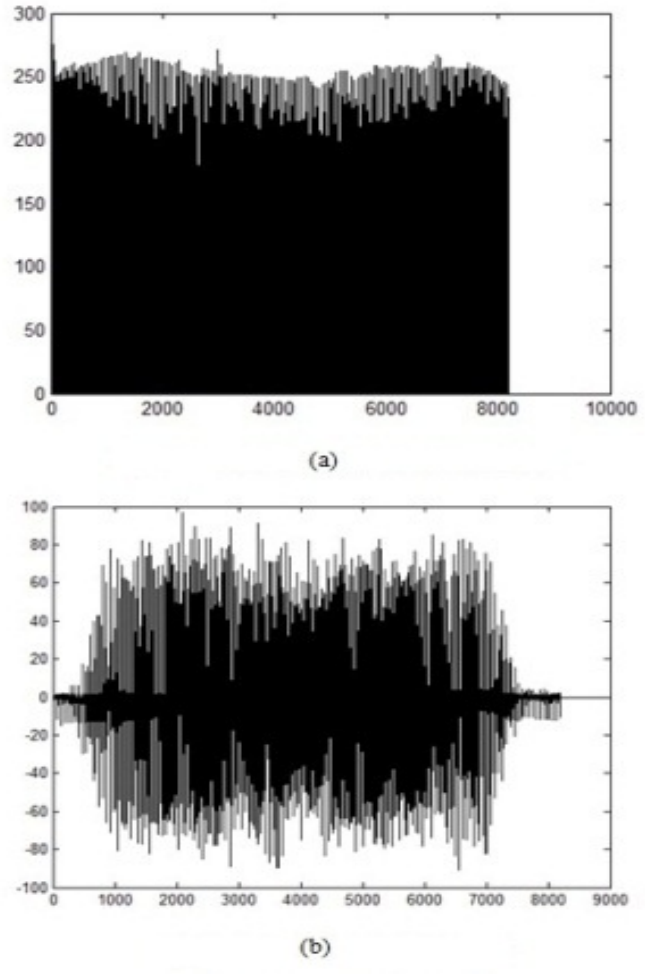

Fig. 2. Wavelet Coefficients of Image (a) Approximation Coefficients (b) Detail Coefficients

As a trade-off, in the proposed scheme, sparse information of watermark biometric image is generated using Compressive sensing procedure. This is a necessary condition for application of CS theory on image is that the image must be sparse on its own basis [15, 16]. So in this paper, detail coefficients

of a watermark biometric image are used for generation of sparse measurements of watermark biometric image.

C. Compressive Sensing (CS) Theory

A compressive sensing theory is a new signal processing theory which is provided a signal or image acquisition in its sparse domain. This theory is introduced by Donoho and Candes in 2006. They are mathematically proven that the signal or image can be recovered using few Fourier coefficients but a necessary condition is that signal or image is in the sparse domain [15, 16]. The compressive sensing theory is provided image acquisition as well as compression simultaneously. The compressive sensing theory is divided into two steps where the first step is generating sparse information from the original image or signal. The second step is reconstructed image or signal from its sparse information using a CS reconstruction algorithm. An image has a size of M×N is represented by M×1 size of sparse measurement using below formula [16].

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

$$x = \Psi(f) \tag{2}$$

In the above equation, y is a sparse measurement of image, A is a measurement matrix which is same for encoder and decoder side, Ψ is a basis transformation matrix of image which can be generated using any image transform like Fourier, Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) and f is an original image.

The different cs theory reconstruction algorithms are described by researchers in the last decade for reconstruction of original images from its sparse measurement vector. These algorithms are based on linear algebra and convex optimization [16, 17]. These reconstruction algorithms mainly divided into two types such as linear optimization based and greedy techniques, respectively [18]. As a trade off, Discrete Wavelet Transform (DWT) is used for generation of sparse information of watermark biometric image at embedded side. The orthogonal matching pursuing (OMP) algorithm [20] is used for reconstruction of watermark biometric image from its extracted sparse measurement vector at detector side.

III. Proposed Watermarking Scheme

This section describes proposed watermarking scheme, where Discrete Cosine Transform (DCT) is applied to the host biometric image and Discrete Wavelet Transform (DWT) is applied to watermark biometric image. A watermark biometric image is converted into its sparse information using compressive sensing theory. The sparse information of the watermark biometric image is generated before embedding into host biometric image using properties of the sparseness of Discrete Wavelet Transform. The proposed scheme is carried out in two phases, watermark preparation and embedding procedure; watermark extraction and reconstruction procedure.

A. Watermark Embedding Procedure

The steps for watermark preparation and embedding are given below:

1) Take a biometric image as a watermark data and calculate the size of the image. Then convert the watermark biometric image into vector.
2) 1st level Discrete Wavelet Transform (DWT) is applied to watermark data vector and decomposed into an approximation and detail coefficients of the wavelet.
3) Then chosen detail wavelet coefficients as sparse coefficients which are denoted as *x*. The reason behind details wavelet coefficients chosen as sparse coefficients is that detail coefficients is sparser than approximation coefficients.

$$[cA, cD] = DWT(W_B, ' wavename') \tag{3}$$

$$cD = x \tag{4}$$

Where cA = Approximation Wavelet Coefficients, cD = Details Wavelet Coefficients, W_B = Watermark Biometric Image in term of the vector, x = Sparse Coefficients of Watermark Biometric Image.

4) Generate measurement matrix A with the size of M×N using standard Gaussian distribution. This measurement matrix A is same for embedder and decoder side.
5) Then sparse measurements of a watermark biometric image is generated using below equation.

$$y = A \times x \tag{5}$$

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

6) Then the sparse measurement of a watermark biometric image is multiplied by sampling factor to get sparse watermark information and which is denoted as W_{Sparse}. The sampling factor is same for embedder and detector side.

$$W_{Sparse} = \beta \times y \tag{6}$$

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

7) Take a host biometric image and calculate the size of the image.
8) Discrete Cosine Transform (DCT) is applied to a host biometric image and converted into AC DCT and DC DCT coefficients. Then find largest AC DCT coefficients of a host biometric image for embedding sparse watermark information.
9) Then sparse watermark information insertion into DCT coefficients of a host biometric image using standard watermarking equation [10] which is given below:

$$I_W(u, v) = I(u, v) \times (1 + k \times W_{Sparse}) \tag{7}$$

Where u, v is highest AC coefficients of DCT, I_W is watermarked biometric image, I is a host biometric image, W_{Sparse} is sparse watermark information, k is a gain factor.

10) Inverse Discrete Cosine Transform (IDCT) is applied to modified DCT coefficients of a host biometric image to get a watermarked biometric image.

B. Watermark Extraction and Reconstruction Procedure

The steps for extraction of sparse watermark information and reconstruction of watermark biometric image from its extracted sparse watermark information are given below:

1) Discrete Cosine Transform (DCT) is applied to watermarked biometric image and converted into AC DCT and DC DCT coefficients. Then find largest AC coefficients of DCT of watermarked image which is used at embedder side.
2) Discrete Cosine Transform (DCT) is applied to a host biometric image and converted into AC DCT and DC DCT coefficients. Then find largest AC DCT coefficients of a host biometric image which is used at embedder side.
3) Extraction of sparse watermark information by using the watermark embedding reverse procedure:

$$W_{Extracted} = \frac{\frac{I_W(u,v)}{I(u,v)} - 1}{k} \tag{8}$$

Where u, v is highest AC coefficients of DCT, I_W is watermarked biometric image, I is a host biometric image, $W_{Extracted}$ is extracted sparse watermark information, k is a gain factor.

4) Then extracted sparse watermark information is divided by sampling factor to get actual sparse measurements of the watermark biometric image.

$$Recover_y = \frac{W_{Extracted}}{\beta} \tag{9}$$

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

5) The orthogonal matching pursuit (OMP) [20] algorithm is applied to extracted sparse measurements of the watermark biometric image along with measurement matrix. The output of OMP algorithm is sparse coefficients of a watermark biometric image. Here sparse coefficients are detail wavelet coefficients of a watermark biometric image.

$$x_{Extracted} = OMP(Recover_y, A, M) \tag{10}$$

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

6) Finally, inverse 1st level Discrete Wavelet Transform (DWT) is applied to extracted detail wavelet coefficients with original approximation wavelet coefficients to get the actual values of watermark biometric image in term of the vector. Then reshape the vector to generate reconstructed watermark biometric image at the detector side.

$$R = IDWT(cA, x'_{Extracted}, 'wavename') \tag{11}$$

$$W_{Reconstructed} = Reshape(R, M, N) \tag{12}$$

Where $W_{Reconstructed}$ = Reconstructed Watermark Biometric Image at Detector Side, $x'_{Extracted}$ = Extracted Sparse Coefficients of a Watermark Biometric Image, R = Extracted actual values of a Watermark Biometric Image in term of vector, cA = Original Approximation Wavelet Coefficients of a Watermark Biometric Image, M = Row Size of a Watermark Biometric Image, N = Column Size of a Watermark Biometric Image.

IV. Experimental Results

The proposed watermarking scheme is tested and performed by using standard Indian face database [21] and standard FVC 2004 fingerprint database [22]. The size of the test image is 128×128 pixels. This proposed watermarking scheme is tested using 50 host face images and 50 watermark fingerprint images. The few of host face images and watermark fingerprint images are shown in Figure 3 and 4, respectively.

For a generation of sparse information of watermark fingerprint image, detail coefficients of a watermark fingerprint image are getting used by 1st level haar wavelet decomposition and get sparse coefficients x with a size of 8192×1. Then generate measurement matrix A with the size of 64×8192 using a random seed. Then generate sparse measurements of watermark fingerprint image with a size of 64×1 using $y_{64\times1} = A_{64\times8192} \times x_{8192\times1}$. Then sampling factor is multiplied with sparse measurements to generate sparse watermark information is denoted as W_{Sparse}. For embedding, the gain factor is chosen 2 and sampling factor 0.001. MATLAB 13 has been used for the implementation of the scheme. The watermarked face image and recovered watermark fingerprint image is shown in figure 5 (a) and (b), respectively.

The watermarked face image, sparse information of watermark fingerprint image, extracted sparse information of watermark fingerprint image and reconstructed watermark fingerprint image using OMP from extracted sparse measurements is shown in figure 5, respectively.

The Quality measures such as PSNR and SSIM are used for calculation of quality of watermarked and recovered watermark images. The quality of the watermark image is calculated using Structural Similarity Index Measure (SSIM) which is used to find similarity between two images [28]. SSIM defined as follows:

$$SSIM(x, y) = \frac{(2xy + c_1)(2\sigma_{xy} + c_2)}{(x\hat{}2 + y\hat{}2 + 1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{13}$$

Where x and y are corresponding windows of the same size of the original watermark biometric and reconstructed

Fig. 3. Host Face Images (a) H1 (b) H2 (c) H3 (d) H4

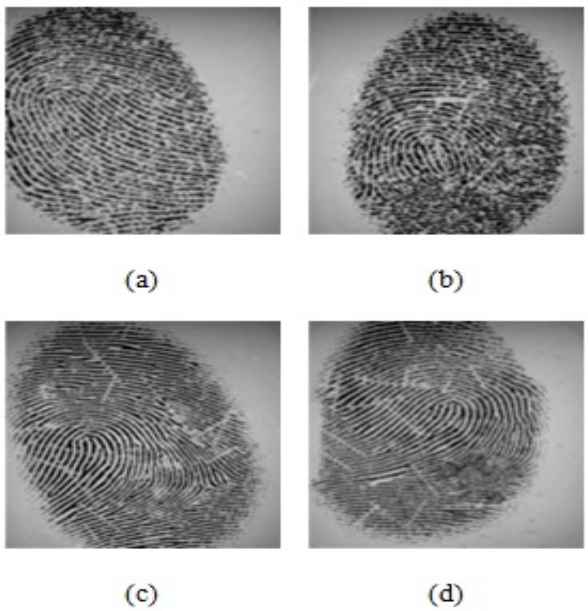

Fig. 4. Watermark Fingerprint Images (a) W1 (b) W2 (c) W3 (d) W4

watermark biometric images, $x^{\wedge}$ and $y^{\wedge}$ are the corresponding averages of x and y respectively, $\sigma_x{}^2$ and $\sigma_y{}^2$ are the corresponding variances of x and y. σ_{xy} is the covariance of x and y and c_1 and c_2 are appropriate constants.

In this paper, SSIM1 is used for finding similarity between watermarked face image and original face image. Also, SSIM2 is used for finding similarity between reconstructed watermark fingerprint image and original watermark fingerprint image.

The robustness of the watermarked image is represented by Normalized Cross Correlation (NCC). This is used as the quantitative measure to compared the original host image and

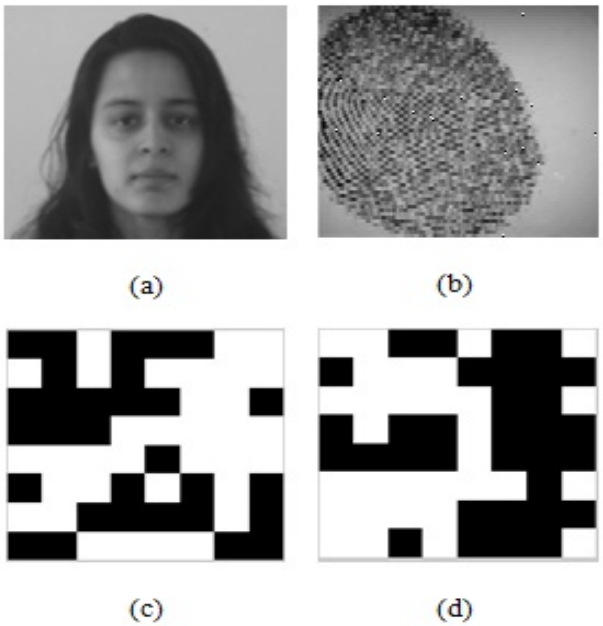

Fig. 5. Fig. 5. (a) Watermarked Face Image, (b) Reconstructed Watermark Fingerprint Image (c) Sparse Information of Watermark Fingerprint Image (d) Extracted Sparse Information of Watermark Fingerprint Image

watermarked host image [7]. It is defined as:

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} I(x,y) \times I^{'}(x,y)}{\sum_{x=1}^{M}\sum_{y=1}^{N} I^{2}(x,y)} \tag{14}$$

Where I(x,y) represent the original watermark image and $I^{'}$(x,y) represents extracted watermark image.

The NCC value can be anywhere between 0 and 1. The closer the NCC value is to 1, the possibly increase the accuracy of reconstructed watermark image [7]. In this paper, NCC is used for finding a correlation between original watermark fingerprint image and reconstructed watermark fingerprint image. The quality measures for proposed scheme under various watermarking attack is summarized in Table 1. These results are generated using host biometric image H1 and watermark biometric image W1. The results shows that this proposed scheme is robust against watermarking attacks.

TABLE I
VALUES OF QUALITY MEASURES FOR PROPOSED SCHEME

Attacks	PSNR(dB)	SSIM1	NCC	SSIM2
No Attack	48.89	1.000	0.950	0.995
JPEG (Q=90)	44.48	0.999	0.952	0.995
Gaussian Noise	29.99	0.998	0.920	0.992
SaltPepper Noise	28.07	0.997	0.904	0.994
Speckle Noise	29.65	0.998	0.927	0.993
Median Filter	46.32	1.000	0.952	0.995
Mean Filter	28.10	0.997	0.531	0.909
Histogram Equ.	20.97	0.992	0.214	0.608
Cropping	18.07	0.973	0.094	0.330

The scheme has been proposed for the purpose of achieving high computational security and protection of biometric data at the communication channel of biometric based system. The higher value of quality measures of proposed scheme shows that the effectiveness of the proposed scheme is maintaining higher imperceptibility and good watermarked image quality. This proposed scheme is increasing the payload capacity of the watermarking scheme because of the same size of watermark information can be embedded in the host data by application of CS theory on watermark data before embedding. The performance of the proposed watermarking scheme has been compared with existed watermarking schemes [7, 9, 23, 24, 25, 26 and 27] using images show in Figure 3 and 4. The results have been summarized in Table 2 and 3. The results show that proposed watermarking scheme is performed better than existed watermarking schemes.

TABLE II
PSNR OBTAINED BY PROPOSED SCHEME COMPARED WITH EXISTED SCHEMES IN LITERATURE

Host Image	H1	H2	H3	H4
Scheme in [7]	40.89	40.95	39.93	41.34
Scheme in [9]	45.63	44.81	45.50	44.51
Scheme in [23]	38.95	39.42	37.58	39.24
Scheme in [24]	37.62	38.82	37.58	39.33
Scheme in [25]	32.18	33.15	31.72	33.92
Scheme in [26]	36.42	35.82	34.45	36.96
Scheme in [27]	37.32	37.76	36.17	38.08
Proposed Scheme	48.89	49.42	45.49	63.26

TABLE III
SSIM OBTAINED BY PROPOSED SCHEME COMPARED WITH EXISTED SCHEMES IN LITERATURE

Host Image	H1	H2	H3	H4
Scheme in [7]	0.953	0.961	0.942	0.964
Scheme in [9]	0.981	0.975	0.982	0.975
Scheme in [23]	0.938	0.941	0.923	0.944
Scheme in [24]	0.936	0.939	0.907	0.942
Scheme in [25]	0.928	0.931	0.899	0.929
Scheme in [26]	0.932	0.918	0.905	0.912
Scheme in [27]	0.932	0.938	0.920	0.926
Proposed Scheme	0.995	1.000	0.999	0.994

In order to showcase the effect of watermarking on the multibiometric system, face matching algorithm described in [29, 30] used for face recognition which gives the Euclidean distance between query face image and its closest match in the database. Also, fingerprint matching algorithm described in [31, 32] used for query fingerprint recognition which gives the Euclidean distance between fingerprint image and its closest match in the database. The advantage of this proposed watermarking scheme is that query face image recognized and fully authenticate with the enrolled watermarked face image at embedder side using a face recognition algorithm [29, 30]. At detector side, query fingerprint image recognized and fully authenticate with reconstructed watermark fingerprint data using fingerprint recognition algorithm [31, 32].

In the proposed watermarking scheme, the accuracy of face recognition and fingerprint recognition is 97.40 % (after watermarking) and 92.45 % (after extraction and reconstruction) respectively. The verification accuracy of multibiometric system using the proposed watermarking scheme is 94.93 % with enhancement in the security of biometric data.

V. CONCLUSION

A novel watermarking scheme using compressive sensing (CS) framework for hiding multimodal biometric data protection has been presented in this paper. The scheme has been proposed for the protection of biometric data against different attacks at communication channel between two modules of the multibiometric system. The presented scheme has been applied compressive sensing theory framework on a watermark biometric image before embedding into the host biometric image. This step would be provided more computational security against modification of biometric data because of it is difficult to get correct measurement matrix and sparse coefficients by an imposter or attacker.

This scheme is non-blind detection scheme. This scheme is robust against various watermarking attacks. This scheme has less imperceptibility, less robust against histogram Equalization and cropping attack. The performance of the proposed scheme has been better than existed schemes in the literature in term of PSNR and SSIM values. The theoretical payload capacity of the proposed scheme is 100 percentage because of the same size of watermark information are embedded into host data.

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, pp. 49-79, 2012.

[2] N. Ratha, J. Connell and R. Bolle, *Enhancing Security and Privacy in Biometric Based Authentication Systems*, IBM Systems Journal, vol. 40, no. 3,2001.

[3] A. Jain, A. Ross and S.Prabhakar, *An Introduction to Biometric Recognition*, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, vol. 14, no. 1, January 2004.

[4] A. Jain and U. Uludag, *Hiding Biometric Data*, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, November 2003.

[5] M. Vasta, R. Singh, P. Mitra and A. Noore, *Digital Watermarking based Secure Multimodal Biometric System*, In Proceedings of the 2004 IEEE International Conference in Systems, Man and Cybernetics, vol. 3, pp. 2983-2987, 2004.

[6] K. Zebbiche and F. Khelifi, *Region Based Watermarking of Biometric Images: Case Study in Fingerprint Images*, International Journal of Digital Multimedia Broadcasting, Hindawai Publishing Corporation, 2008.

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

[8] M. Paunwala and S. Patnaik, *DCT Watermarking Approach for Security Enhancement of Multimodal System*, ISRN Signal Processing 2012, 2012.

[9] B. Behera and V. Govindan, *Improved Multimodal Biometric Watermarking in Authentication Systems Based on DCT and Phase Congruency Model*, International Journal of Computer Science and Network, vol. 2, issue 3, June 2013.

[10] I. Cox, J. Kilian, T. Shamoon and F. Leighton, *Secure Spread Spectrum Watermarking for Multimedia*, IEEE Transactions on Image Processing, Vol. 6, No. 12, December 1997.
[11] G. Langelaar, I. Setyawan and R. Lagnedijk, *Watermarking of Digital Image and Video Data A State of Art Review*, IEEE Signal Processing Magazine, pp. 20-46, September 2000.
[12] R. Wolfgang, C. Podilchuk, and E. Dalp, *Perceptual Watermarks for Digital Images and Video*, Proceedings of IEEE, vol. 87, no. 7, pp. 1108-1126, 1999.
[13] M. Bami, F. Bartolini, V. Cappellini and A. Piya, *A DCT Domain System for Robust Image Watermarking*, Signal Processing, vol. 66, no. 3, pp. 357-372, 1998.
[14] A. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall Inc., New Jersey, pp. 150-153, 1999.
[15] E. Candes, *Compressive Sampling*, Proceedings of the International Congress of Mathematicians, Madrid, Spain 2006.
[16] D. Donoho *Compressed Sensing*, IEEE Trans. Inform. Theory, vol. 52, no. 4, pp. 1289-1306, April 2006.
[17] R. Baraniuk, *Lecture notes on Compressive Sensing*, IEEE Signal Processing Magazine, Vol. 24, pp. 118-124, July 2007.
[18] S. Mazari and K. Belloulata, *Signal and Image Recovery from Random Linear Measurements in Compressive Sensing*, International Journal of Computer Science and Electronics Engineering, vol. 1, pp. 158-162, February 2013.
[19] 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, Vol. 2, Issue 2, May 2013.
[20] J. Tropp and A. Gilbert, *Signal Recovery from Random Measurements via Orthogonal Matching Pursuit*, 2007.
[21] Vidit Jain, Amitabha Mukherjee, *The Indian Face Database*, 2002. http://vis-www.cs.umass.edu/ vidit/IndiaFaceDatabase
[22] For Fingerprint Database: http://bias.csr.unibo.it/fvc2004/databases.asp
[23] B. Ma, C. Li, Y. Wang and Z. Zhang, *Block Pyramid Based Adaptive Quantization Watermarking for Multimodal Biometric Authentication*, In Proceedings of 20th IEEE International Conference on Pattern Recognition (ICPR), pp. 1277-1280, 2010.
[24] S. Edward and M. Sumanthi, *Multimodal Biometrics for authentication using DRM technique*, International Journal of Technology and Engineering Systems (IJTES), vol. 2, issue 2, pp. 200-205, 2011.
[25] A. Naik and R. Holambe, *Blind DCT Domain Digital Watermarking for Biometric Authentication*, International Journal of Computer Applications (IJCA), vol. 1, issue 16, pp. 11-15, 2010.
[26] D. Shinfeng, S. Shie and J. Guo, *Improving the robustness of DCT based Image Watermarking against JPEG Compression*, J. Computer Standards and Interfaces, vol. 32, pp. 60-67, 2010.
[27] M. Rohani and A. Avanaki, *A Watermarking Method based on Optimizing SSIM Index using PSO in DCT Domain*, CSICC, 2009, pp. 418-423, 2009.
[28] Z. Wang and A. Bovik, *A Universal Image Quality Index*, J. IEEE Signal Processing Letters, vol. 9, issue 3, pp. 84-88, 2002.
[29] M. Turk and A. Pentland, *Face Recognition Using Eigenfaces*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 586 591, Maui, Hawaii, USA, June 1991.
[30] H. Moon and P. Phillips, *Computational and Performance aspects of PCA-based Face Recognition Algorithms*, Perception, Vol. 30, pp. 303-321, 2001.
[31] 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, pp. 3284-3285, July 1999.
[32] S. Prabhakar, *Fingerprint Classification and Matching Using a Filterbank*, A Ph.D. Thesis, Michigan State University, 2001.
[33] I. Selesnick, *Wavelet Transforms A Quick Study*, Physics Today Magazine, October 2007.

Rohit M. Thanki is currently pursuing Ph.D. in Electronics and Communication Engineering at C. U. Shah University, Wadhwan city, Gujarat, India. He obtained his Bachelor of Electronics and Communication Engineering from Atmiya Institute of Technology and Science, Saurashtra University, Rajkot in 2008. He received his Master degree in Communication Engineering from G H Patel College of Engineering and Technology, Sardar Patel University, Vallabh Vidyanagar in 2010. His area of interests are Biometric Security, Digital Watermarking, Compressive Sensing, Pattern Recognition, Image Processing, Signal Processing and Digital VLSI Design.

Ved Vyas Dwivedi is a Pro Vice Chancellor, C U Shah University, Wadhwan city, India. He supervised many Ph.D. Thesis and Master Dissertation during his professional career. He has published more 100 research papers. His area of interests are Wireless-Optical-Mobile-Satellite Communication, Radar-Microwave-Electron Magnetic-Antenna-RF Engineering, Meta Materials, Image Processing and Signal Processing.

Komal R. Borisagar is a Associate Professor, Electronics and Communication Department, Atmiya Institute of Technology and Science, Rajkot, India. She was awarded Ph.D. in Electronics and Communication Engineering from JJTU, India in 2012. Her area of interests are Wireless Communication, Speech Processing, Image Processing and Signal Processing.