I.J. Image, Graphics and Signal Processing, **2015, 1, 53-60**
Published Online December 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2015.01.07

Compressive Sensing Based Multiple Watermarking Technique for Biometric Template Protection

Rohit M. Thanki
PhD Research Scholar, EC Department, Faculty of Technology & Engineering, C U Shah University, Wadhwan, India
Email: rohitthanki9@gmail.com

Komal R. Borisagar
Assistant Professor, EC Department, Atmiya Institute of Technology & Science, Rajkot, India
Email: krborisagar@aits.edu.in

Abstract—Biometric authentication system is having several security issues. Two security issues are template protection at system database and at communication channel between system database and matcher subsystem of biometric system. In this paper, two level watermarking technique based on CS Theory framework in wavelet domain is proposed for security and authentication of biometric template at these two vulnerable points. In the proposed technique, generate sparse measurement information of fingerprint and iris biometric template using CS theory framework. This sparse measurement information is used as secure watermark information which is embedding into a face image of same individual for generation of multimodal biometric template. Sparse watermark information is computed using Discrete Wavelet transform (DWT) and random seed. The proposed watermarking technique not only provide protection to biometric templates, it also gives computational security against spoofing attack because of it is difficult for imposter to get three secure biometric template information where two encoded biometric template is embed in term of sparse measurement information into third biometric template. Similarity value between original watermark image and reconstructed watermark image is the measuring factor for identification and authentication. The experimental results show that the technique is robust against various attacks.

Index Terms—Compressive Sensing, Discrete Wavelet Transform (DWT), Fingerprint, Face, Iris, Multimodalities, Sparsity, Watermarking.

I. INTRODUCTION

In Recent world, automatic biometric authentication system is used for human identification [1, 2]. This biometric authentication system matches decision between query biometric feature and enrolled biometric feature and based on matching result human can authentication or not [1, 2]. But this biometric authentication system have disadvantage like noise in sensor, interclass variations, Distinctiveness, Nonuniversality and Spoof attacks [3]. Also this biometric authentication system have vulnerable against various attacks which identified by N. Ratha and its research team in 2001 [4, 5]. These attacks are divided into eight groups which are first is attack on sensor, second is attack on communication channel between sensor and feature extractor modules, third is attack on feature extractor modules where changing some feature of biometric template by attacker, fourth is attack on communication channel between feature extractor and matcher module, fifth is attack on matcher modules by modifying matching score, sixth is attack on system database where tampering or modified biometric template by attacker, seventh is attack on communication channel between system database and matcher module, eight is attack on decision module [4, 5]. These attacks on biometric authentication system are shown in figure 1.

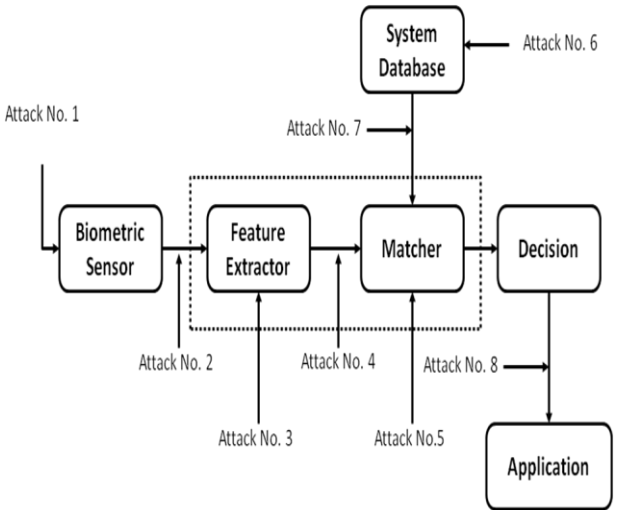


Fig. 1. Attacks on Biometric Authentication System (taken from [4, 5])

For overcome of these disadvantages of biometric system, A. Jain and its research team is introduced new biometric authentication system which is known as

Copyright © 2015 MECS

multimodal biometric system in 2003. In multimodal biometric system, two or more biometric modalities of individual are used for enrollment, verification and authentication [6]. In this biometric system, one biometric modality feature is embed or fused into other biometric modality of same individual for generation of multimodal biometric template [6]. This biometric system can be operated in three different modes like serial, parallel and hierarchical. Multimodal biometric system is also vulnerable against spoofing attack and due to this attack, authenticate individual cannot enter into the system. Digital watermarking technique is best solution against spoofing attacks in biometric system because it embeds secure biometric information into other host medium.

In this paper, new watermarking technique using DWT and CS theory framework proposed for protection of biometric template at system database, on communication channel between system database and matcher modules of biometric system. The rest of paper is organized as follows: section 2 describes the literature review of related work. Section 3 describes the compressive sensing theory which is used for generation of sparse measurement information of the fingerprint and iris image. Section 4 describes the proposed watermarking technique. Section 5 shows experimental results and analysis of technique. Finally, section 7 concludes the paper.

II. Literature Review of Related Work

In last decade many researcher are proposed and described various watermarking techniques for protection of biometric template. Few watermarking techniques are reviewed which is related to proposed work is described below:

Author in [7] proposed signature based biometric watermarking technique where details coefficient of host standard image are modified according to PN sequence and signature watermark bit. Also author proposed new signature recognition algorithm using Hough transform and PCA. This proposed technique is robust against JPEG compression, filtering and adding noise attacks. Author in [8] proposed human speech based biometric watermarking technique where speech signal is embed into wavelet coefficients of standard test image which is used for copyright protection.

Author in [9] is give study of DWT based fingerprint watermarking technique and claim that verification of fingerprint image can possible after extraction from watermarked image. Author in [10] proposed redundant discrete wavelet transform based biometric technique combined with phase congruency model for speech signal and color face image. In this proposed technique, Mel frequency cepstral coefficients (MFCC) is embed into red and blue channel of color face image for improve robustness and security of multimodal biometric system. Author in [11] proposed biometric watermarking technique based on LSB and DWT for embedding face features into fingerprint image for multimodal biometric system. Author in [12] proposed biometric technique based on multi resolution DWT and support vector machine (SVM) for embedding face image into fingerprint and claimed that this technique improved 10 % of face recognition under different attack. Author in [13] proposed biometric watermarking technique based on wavelet transform where embed voice and iris feature into wavelet coefficient of fingerprint image using block processing and then compression applied on watermarked version of multimodal biometric template for improve storage capacity of system.

Author in [14] proposed CS theory based watermarking technique with description on cs acquisition and recover process for standard image. Author in [15] proposed CS theory and SVD based image watermarking technique for improving security. Author in [16] proposed CS theory based watermarking technique for audio signals and this technique is robust against different attacks like MP3 audio compression and additive noise. Author in [17] proposed CS theory based watermarking technique using wavelet transform for tamper identification in standard images. Author in [18] proposed first watermarking technique using CS theory framework in transform domain. In this technique, transform coefficients of host image are modified according to encoded watermark where encoded watermark is generated using measurement matrix which is generated by random seed. For detection of watermark, cs recovery process L1 minimization is used.

III. Brief Description of Compressive Sensing Theory

D. Donoho and E. Candès et al. [19, 20] are proved mathematically that the original signal can be reconstructed accurately from part of its transform coefficients. Based on this theory, E. Candès et al. [20] gives new signal processing theory called "Compressive Sensing or Sampling Theory". Compressive Sensing theory having more advantages compare to existed compression technique in literature and its break limitation of Shannon – Nyquist Theorem's sampling theory [21].

The linear measurement vector of signal or image generates using compressive sensing theory is given by below formula [21]:

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

$$y = A \times \Psi \times f \tag{2}$$

Where y = linear measurement vector of signal or image, A = measurement matrix which is generated using random seed only to embedder and decoder, Ψ = orthonormal or basis matrix, x = transform coefficients of signal or image, f = original signal or image.

Compressive sensing theory is performing two processes on signal or image where first process is CS acquisition process which is related to generation of

linear measurement vector and second process is CS recovery process which is related to recovery of transform coefficients x from linear measurement vector y. The CS acquisition process of any signal or image is achieved using equation 1 and 2 and graphical shown in figure 2.

For CS recovery process, consider few questions which are related to measurement matrix and linear measurement vector. First question is how measurement matrix A satisfies that measurement process is correct? Second question is how transform coefficients of signal or image get from the measurement vector?

The answer to first question is restricted Isometry property which is given by Candès and Tao [31]. The measurement matrix A of size M × N obeys the Restricted Isometry Property of order K (K ≤ m) if A approximately preserves the squared magnitude of any K – sparse vector y using below equation [21, 22, 31 and 32]:

$$(1-\delta)\|x\|_2^2 \le \|Ax\|_2^2 \le (1+\delta)\|x\|_2^2, \delta \in (0,1) \qquad (3)$$

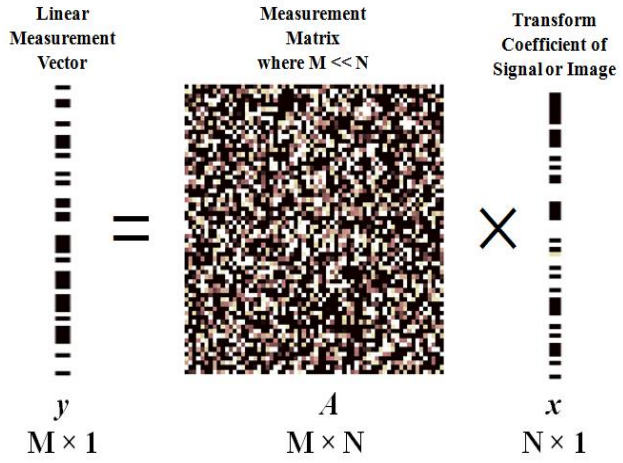


Fig. 2. CS Acquisition Process (taken from [21, 22])

Holds for all x and $\|x\|_0 := |\sup(x)| \le K$. In word, measurement matrix A acts as an approximate Isometry on the set of vectors that are K-sparse. A necessary and sufficient condition for extract recovery of sparse signal or compressible images is to satisfying Restricted Isometry property (RIP) [21, 22 and 32].

The answer to second question about recovery of transform coefficients of signal or image is Basis Pursuit. The coefficients of the signal or image x in A and hence the coefficients of signal or image x can be recovered by solving the following constrained minimization problem.

$$\hat{x} = \arg\min_x \|x\|, s.t. Ax = y \qquad (4)$$

Provided that A satisfies the RIP of order 2K with $\delta \le \sqrt{2}-1$, BP is guaranteed to recover x exactly [21, 22, 31 and 32]. For recovery of transform coefficients of signal or image, various recovery algorithms is proposed and described by various researchers in last five years. Few examples of CS recovery algorithms are L1 minimization technique, COSAMP, OMP, SP and IHT.

Other important property of compressive sensing theory is given unique solution to recovery of sparse signal or image based on measurement matrix values and sparsity level. Example like that if we want to recover transforms coefficients x of signal or image from measurement vector y then we required correct measurement matrix A which is generated at CS acquisition process otherwise we cannot get correct transform coefficients of signal or image.

In this paper, Discrete Wavelet Transform like daubechies is used at CS acquisition process for generation of linear measurement vector and used two CS recovery algorithm like orthogonal matching pursuit (OMP) [23] and subspace pursuit (SP [24] for recovery of transform coefficients from linear measurement vector.

IV. Proposed Watermarking Technique

This section describes the proposed two level watermarking technique based on CS theory and discrete wavelet transform. In the proposed technique, multi resolution DWT is applied on fingerprint image of individual which is taken as host image and high frequency wavelet coefficients of host image is chosen for watermark embedding because less information of host image is content in high frequency wavelet coefficients.

Single level wavelet decomposition is applied on face and iris image of same individual and converting into sparse measurement information using CS theory which is taken as watermark information. The proposed technique is divided into two parts like watermark embedding procedure and watermark extraction and reconstruction procedure.

A. Watermark Embedding Procedure

The watermark embedding steps are described below:

1. Iris biometric template is taken as watermark image 1 and compute size of iris image.
2. Apply 1D DWT on iris image and taken details wavelet coefficients of iris image as transform coefficients.
3. Generate measurement matrix using length of transform coefficients and random seed which is same for embedder and detector side.
4. Repeat step 2 and 3 for row size of iris image and convert into linear measurement vector by multiplying measurement matrix and transform coefficients using equation 1 and 2.
5. Steps 2 to 4 give CS theory acquisition process and after these steps get sparse measurement information which is used secure watermark information.
6. This sparse measurement information of iris image is reshaping into matrix which is denoted as watermark

W_1. This watermark information is used for reference data for cross verification of iris biometric template and decision about modification at system database.

7. Applied Third level Discrete Wavelet Transform (DWT) is applied on host fingerprint image and converts into various coefficients like LL_3, HL_3, LH_3 and HH_3.
8. Replace HH_3 wavelet coefficients of host fingerprint image with watermark W_1 which is sparse measurement information of iris image.
9. Now take face biometric template as watermark image 2 and compute size of image.
10. Apply 1D DWT on face image and taken details wavelet coefficients of face image as transform coefficients.
11. Generate measurement matrix using length of transform coefficients and random seed which is same for embedder and detector side.
12. Repeat step 10 and 11 for row size of face image and convert into linear measurement vector by multiplying measurement matrix and transform coefficients using equation 1 and 2.
13. This sparse measurement information of face image is reshaping into matrix which is denoted as watermark W_2. This watermark information is used for reference data for cross verification of face biometric template and decision about modification at matcher system.
14. Applied Discrete Wavelet Transform (DWT) is applied on host fingerprint image and converts into various coefficients like LL_4, HL_4, LH_4 and HH_4.
15. Replace HH_4 wavelet coefficients of fingerprint image with watermark W_2 which is sparse measurement information of face image.
16. Take inverse fourth level of Discrete Wavelet Transform (DWT) of fingerprint image and generated Watermarked version of fingerprint image.

B. Watermark Extraction and Reconstruction Procedure

The watermark extraction and reconstruction steps are described below:

1. Watermarked fingerprint image is verified with enrolled fingerprint image and a result of verification is less than threshold value then below step is follows.
2. Take watermarked fingerprint image and apply third level DWT on watermarked fingerprint image.
3. Take HH_3 wavelet coefficients of watermarked fingerprint image as watermark information $W_{Extracted1}$ which in term of sparse measurement matrix.
4. Reshape $W_{Extracted1}$ into linear measurement vector $y_{Extracted1}$ for reconstruction of iris watermark image using step 5.
5. Used compressive sensing recovery algorithm Orthogonal Matching Pursuit (OMP) [23] using below equation with correct measurement matrix A_1which is same as used at embedder side and extracted linear measurement vector $y_{Extracted1}$.

$$Ext\_Wavcof\_Iris = OMP(y_{Extracted1}, A_1, M_1) \quad (5)$$

Where *Ext_Wavcof_Iris* is extracted transform coefficients of iris biometric image, $Y_{Extracted1}$ is extracted linear measurement vector, M_1 is level of sparsity, A_1 is measurement matrix which same as generated at embedder side.

6. After getting transform coefficients of iris image and applied inverse 1D DWT to get reconstructed iris watermark image.
7. This reconstructed iris image is used for comparison with enrolled iris image and takes decision about modification of template at system database.
8. Then again apply third level Discrete Wavelet Transform (DWT) on watermarked fingerprint image.
9. Take HH_4 wavelet coefficients of watermarked fingerprint image as watermark information WExtracted2 which in term of sparse measurement matrix.
10. Reshape WExtracted2 into sparse measurement vector yExtracted2 for reconstruction of face watermark image using step 11.
11. Used compressive sensing recovery algorithm Subspace Pursuit (SP) [24] using below equation with correct measurement matrix A_2 which is same as used at embedder side and extracted sparse measurement vector $y_{Extracted2}$.

$$Ext\_Wavcof\_Face = SP(y_{Extracted2}, A_2, M_2) \quad (6)$$

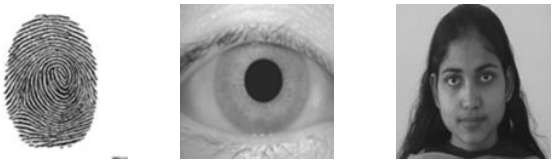
Where *Ext_Wavcof_Face* is extracted transform coefficients of face biometric image, $Y_{Extracted2}$ is extracted linear measurement vector, M_2 is level of sparsity, A_2 is measurement matrix which same as generated at embedder side.

12. After getting transform coefficients of face image and applied inverse 1D DWT to get reconstructed face watermark image.
13. This reconstructed face image is used for comparison with enrolled face image and takes decision about modification of template at matcher module.

V. Results and Discussion

Performance of the proposed watermarking technique is evaluate using 8 bit gray scale fingerprint image with size of 128 × 128 pixels taken from fingerprint samples from FVC 2004 [26] used as host image, 8 bit gray scale face image with size of 128 × 182 pixels taken from Indian face database [25] and 8 bit gray scale iris image with size of 512 ×512 pixels taken from CASIA database [27] used as watermark images which is shown in figure 3.

Copyright © 2015 MECS



(a) Fingerprint Image as Host Medium (b) Iris Image as Watermark 1 (c) Face Image as Watermark 2

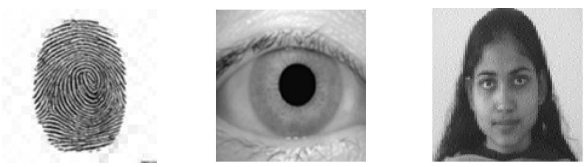
Fig. 3. Various Biometric Templates

For generation of sparse measurement vector of iris watermark image, applied 1D daubechies wavelet transform on iris image and get transform coefficients with size of 131072 × 1. Then generate measurement matrix with size of 256 × 131072 using random seed. Then generate sparse measurement information of iris image with size of 256 × 1 by multiplying transform coefficients and measurement matrix and reshape into 16 × 16 size of matrix which is used as watermark information and denoted as watermark W_1.

For generation of sparse measurement vector of face watermark image, applied 1D daubechies wavelet transform on face image and get transform coefficients with size of 16384 × 1. Then generate measurement matrix with size of 64 × 16384 using random seed. Then generate sparse measurement information of face image with size of 64 × 1 by multiple of transform coefficients and measurement matrix and reshape into 8 × 8 size of matrix which is used as watermark information and denoted as watermark W_2.

Then applied fourth level daubechies wavelet decomposition on host fingerprint image and decompose into various wavelet coefficients of fingerprint image. Then replace fourth level HH wavelet coefficients with watermark W_2 information and third level HH wavelet coefficients with watermark W_1 information. The watermarked fingerprint image is shown in figure 4(a).

In the decoder side, the sparse measurement information is extracted using watermark extraction algorithm. The reconstruction of the extracted biometric watermark image is done with Orthogonal Matching Pursuit [23] and Subspace Pursuit [24] algorithm. The input of these two CS recovery algorithm is extracted sparse measurements of watermark information; correct measurement matrix which is generated at embedder side; sparsity level which is depend on size of watermark image. The output of these algorithms is sparse coefficients of watermark biometric image. The extracted & reconstructed biometric image is shown in figure 4 (b & c).



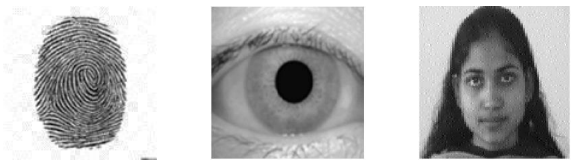
(a) Watermarked Fingerprint Image (b) Reconstruct Iris Image at system database as Watermark 1 (c) Reconstruct Face Image at matcher module as Watermark 2

Fig. 4. Watermarked and Extracted Watermark Biometric Image

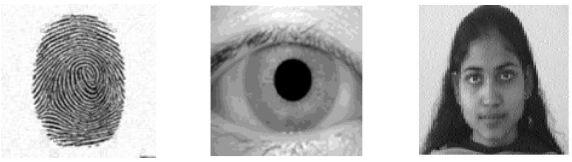
The robustness of the watermarking technique is measure by Peak Signal to Noise Ration (PSNR) which is used to compare the original host image and watermarked host image [28, 29 and 30]. The quality measure like Normalized Cross Correlation (NCC) is used to find correlation between original host image and watermarked host image. The closer NCC value is to 1, the possibly increase robustness of watermarking technique. In this paper, PSNR value is used for measurement of robustness and imperceptibility of watermarked fingerprint image. NCC is used to find correlation between original host fingerprint image and watermarked fingerprint image.

The quality of reconstructed watermark iris and face image is calculated using Structural Similarity Index Measure (SSIM) which is used to find similarity between two images [28]. In this paper, SSIM is used to find similarity between original watermark image and reconstructed watermark image.

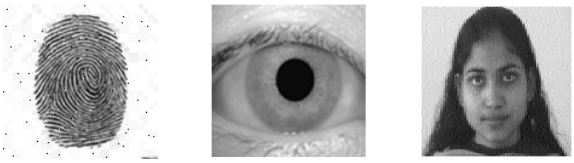
This proposed watermarking technique is also tested against various watermarking attacks like JPEG compression, addition of different noise like Gaussian, Speckle and Salt & Pepper, application of different filter like mean, median and Gaussian low pass filter, and geometric attack like cropping. Experiment results shown in figure 5. Table 1 shows the quality measure value of MSE, PSNR and NCC between host fingerprint image and watermarked fingerprint image.



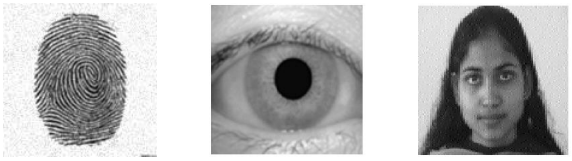
(a) JPEG Compression Attack, Q =90



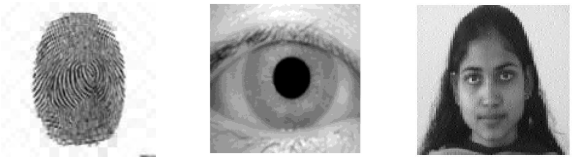
(b) Gaussian Noise Attack, $\mu = 0$, $\sigma = 0.001$



(c) Salt & Pepper Noise Attack, Noise Density = 0.005

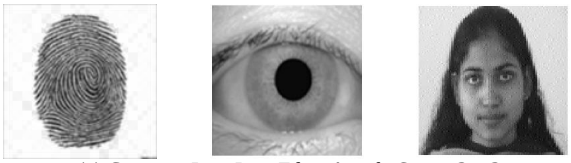


(d) Speckle Noise Attack, Variance = 0.004

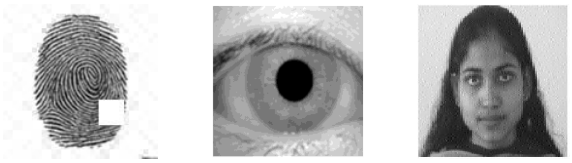


(e) Median Filter Attack, Size = 3 × 3

(f) Mean Filter Attack, Size = 3 ×3



(g) Gaussian Low Pass Filter Attack, Size = 3 ×3



(h) Cropping Attack

Fig. 5. Watermarked and Extracted Watermark Biometric Image Under Various Watermarking Attacks

Table 1. Quality Measures for Proposed Technique

Results	**No Attack**	**JPEG Comp. Attack**	**Gaussian Noise Attack**	**Salt & Pepper Noise Attack**	**Speckle Noise Attack**	**Median Filter Attack**	**Mean Filter Attack**	**Gaussian Low Pass Filter Attack**	**Cropping Attack**
		Q = 90	μ = 0, σ = 0.001	Density = 0.005	Variance = 0.004	Size= 3 ×3	Size= 3 ×3	Size= 3 ×3	
NCC	0.99	0.99	0.99	0.98	0.99	0.97	0.93	0.99	0.94
MSE	54.15	54.70	107.35	243.21	168.66	295.78	679.58	125.75	610.42
PSNR (dB)	30.79	30.75	27.82	24.27	25.86	23.42	19.81	27.14	20.27

After applying various attacks on watermarked fingerprint image prove that the proposed watermarking technique is robust against various watermarking attack. The SSIM or similarity value between the original watermark image and extracted & reconstructed watermark image can be taken as measuring factor for identification and authentication of individual. However there are various pattern recognition algorithms could be applied for identification and authentication.

As shown in table 2 similarity value between original and extracted & reconstructed watermark image is 1.00 (100 %) and 0.998 (99.80 %) for iris biometric template and face biometric template respectively for all possible attacks indicate that identification and authentication of individual doesn't affected by proposed watermarking technique.

The proposed watermarking technique has be evaluated and compared with various existed watermarking techniques in literature using for biometric template protection give in [7 and 8] and CS theory based watermarking technique in [15 and 16] using images shown in figure 3 and results have been summarized in table 3. The good PSNR value indicated that proposed watermarked technique is provide more invisibility and good quality of biometric template.

Table 2. Similarity between the original and extracted iris and face image after various attacks

Attacks	Similarity between original iris and reconstructed iris image (%)	Similarity between original Face and reconstructed face image (%)
No attack	100	99.80
JPEG Compression	100	99.80
Gaussian Noise	100	99.80
Salt & Pepper	100	99.80
Speckle Noise	100	99.80
Median Filter	100	99.80
Mean Filter	100	99.80
Gaussian LPF	100	99.80
Cropping	100	99.80

Table 3. PSNR Value obtained by Proposed Technique Compared with Existed Watermarking Technique in Literature

Technique	PSNR value in dB
Inamdar et al. [7]	30.00
Jundale et al. [8]	30.69
Sreedhanya et al. [15]	7.12
Fakhr et al. [16]	28.00
Proposed Technique	30.79

Copyright © 2015 MECS

Using CS theory framework in this proposed technique, watermark image is embed into one fourth size of host image. This shows that high payload capacity of watermarking technique is achieved compare to existed watermarking technique in literature. Compression of watermark biometric image is achieved before embedding shows that proposed technique can be used for large scale biometric system.

VI. Conclusion

A novel multilevel fingerprint watermarking technique using CS theory has been proposed in wavelet domain. The proposed watermarking technique has used for modification detection and protection of biometric template at system database and matcher module of biometric authentication system. The proposed technique provides security to biometric template and prevents alternation in large scale biometric system and provide following advantages:

1. It is explore sparsity properties of Discrete Wavelet transform to generate encrypted and compressed watermark information.
2. It maintains the high quality of fingerprint image after embedding two biometric modalities.
3. The key point of the proposed technique is the compressive sensing theory. For each watermark biometric image a different sparse measurement information will be generated. This will increase security of biometric system. If imposter applies incorrect measurement information, then the watermark reconstructed procedure can't be perform and output will be random noise.
4. It is provide security against spoofing attack on biometric template because it is difficult to generate three biometric modalities by imposter because of two biometric modalities is encrypted by CS theory framework and embed into third modalities of same individual.
5. If the fingerprint image is modified biometric iris and face image can be used for identification and authentication of the individual.

Acknowledgment

We would like to thank National Laboratory of Pattern Recognition (NLPR), Institute of Automation, Chinese Academy of Sciences (CASIA), China to provide iris and fingerprint image database. Also thank to Vidit Jain and his research team to provide 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*, November 2012.

[3] A. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, June 2006, pp. 125-143.

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

[5] N. Ratha, J. Connell and R. Bolle, "An Analysis of Minutiae Matching Strength", *in Proceedings International Conference Audio and Video-based Biometric Person Authentication, Halmstad*, Sweden, June 2001, pp. 223-228.

[6] A. Jain, A. Ross and S. Pankanti, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, January 2004, pp. 4-20.

[7] V. Inamdar, P. Rege and M. Arya, "Offline Handwritten Signature based Blind Biometric Watermarking and Authentication Technique using Biorthogonal Wavelet Transform", *International Journal of Computer Applications*, volume 11, no. 1, December 2010, pp. 19-27.

[8] V. Jundale and S. Patil, "Biometric Speech Watermarking Technique in Images Using Wavelet Transform", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, February 2010, pp. 33-39.

[9] D. Mathivadhani and C. Meena, "A Comparative Study of Fingerprint Protection using Watermarking Techniques", *Global Journal of Computer Science and Technology*, volume 9, issue 5, January 2010.

[10] M. Vatsa, R. Singh and A. Noore, "Feature Based RDWT Watermarking for Multimodal Biometric System", *Elsevier Science*, June 2007.

[11] 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*, vol. 3, no. 2, January 2006, pp. 23-28.

[12] M. Vasta, R. Singh and A. Noore, "Improving Biometric Recognition Accuracy and Robustness Using DWT and SVM Watermarking", *IEICE Electronics Express*, vol. 1, no. 12, June 2005, pp. 362-367.

[13] A. Giannoula and D. Hatzinakos, "Data Hiding for Multimodal Biometric Recognition", *In Proceedings of the 2004 IEEE International Symposium on Circuits and Systems*, volume 2, 2004, pp. 160-165.

[14] 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*, volume 2, Issue 2, May 2013.

[15] A. Sreedhanya and K. Soman, "Ensuring Security to the Compressed Sensing Data Using a Steganographic Approach", *Bonfring International Journal of Advances in Image Processing*, vol. 3, no. 1, March 2013, pp. 1-7.

[16] M. Fakhr, "Robust Watermarking Using Compressed Sensing Framework with Application to MP3 Audio", *The International Journal of Multimedia & Its Applications (IJMA)*, volume 4, no. 6, December 2012.

[17] M. Raval, M. Joshi, P. Rege and S. Parulkar, "Image Tampering Detection Using Compressive Sensing Based Watermarking Scheme", *In Proceedings of MVIP 2011*, December 2011.

[18] M. Sheikh and R. Baraniuk, "Blind Error Free Detection of Transform Domain Watermarks", *in Proceedings of IEEE International Conference on Image Processing*, San Antonio, Texas, United States, September 2007.

Copyright © 2015 MECS

[19] D. Donoho, "Compressed Sensing", *IEEE Transaction on Information Theory*, vol. 52, no. 4, April 2006, pp. 1289-1306.
[20] E. Candès, "Compressive Sampling", in Proceedings of the International Congress of Mathematicians, Madrid, Spain 2006.
[21] R. Baraniuk, Lecture notes "Compressive Sensing", *IEEE Signal Processing Magazine*, Vol. 24, July 2007, pp. 118-124.
[22] E. Candès and J. Romberg, "L1-Magic: Recovery of Sparse Signals via Convex Programming", October 2005.
[23] J. Tropp and A. Gilbert, "Signal Recovery from Random Measurements via Orthogonal Matching Pursuit", *IEEE Transactions on Information Theory*, vol. 53, no. 12, December 2007, pp. 4655-4666.
[24] W. Dai and O. Milenkovic, "Subspace Pursuit for Compressive Sensing Signal Reconstruction", 2009.
[25] Vidit Jain, Amitabha Mukherjee, "The Indian Face Database", 2002. http://vis-www.cs.umass.edu/~vidit/IndiaFaceDatabase.
[26] For Fingerprint Database: http://bias.csr.unibo.it/fvc2004/databases.asp.
[27] For iris Database: http://www.sinobiometrics.com/caisairis.html.
[28] H. Tsai and C. Liu, "Wavelet Based Image Watermarking with Visibility Range Estimation Based on HVS and Neural Networks", *Pattern Recognition*, 44(2011), pp. 751-763.
[29] Z. Wang and A. Bovik, "A Universal Image Quality Index", J. *IEEE Signal Processing Letters*, 9(3), 2004, pp. 84-88.
[30] 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, pp. 123-129, June 2013.
[31] E. Candès, "The Restricted Isometry Property and Its Implications for Compressed Sensing", *Comptes rendus de l'Acad'emie des Sciences Serie I*, vol. 346, no. 9 -10, pp. 589 – 592, May 2008.
[32] J. Laska, M. Davenport and R. Baraniuk, "Exact Signal Recovery from Sparsely Corrupted Measurements through the Pursuit of Justice", *Signals, Systems and Computers, 2009 Conference Record of the Forty-Third Asilomar Conference on , IEEE*, 2009, pp. 1556-1560.

Authors' Profiles

Rohit M. Thanki has received B.E. degree in Electronics and Communication from Atmiya Institute of Technology & Science, Saurashtra University, Rajkot, Gujarat, India in 2008 and M.E. degree in Communication Engineering from G H Patel College of Engineering and Technology, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India in 2010. He is currently pursuing his PhD in Electronics and Communication Engineering from C U Shah University, Wadhwan City, India. He has published and presented more than 20 research papers in various high impact factor international journals and various international as well as national conferences. He has published two books based on his research work with Lambert Publishing House, Germany. He is life member of ISTE and Student member of IEEE. His areas of interests are Digital Watermarking, Compressive Sensing, Biometric Security, Pattern Recognition, Image & Signal Processing,

Dr. Komal R. Borisagar received B.E. degree in Electronics and Communication from C. U. Shah Engineering College, Saurashtra University, Rajkot, Gujarat, India in 2002 and M.E. degree in Communication System Engineering from Changa Institute of Technology, Gujarat University, Ahmedabad, Gujarat, India in 2008. In 2012, she received her doctoral degree from the Department of Electronics and Communication Engineering, JJT University, Rajasthan, India. She has 10 year of teaching experience. She is working as Assistant Professor at Electronics & Communication Department, Atmiya Institute of Technology and Science, Rajkot. Her areas of interest are wireless communication, speech processing and signal & image processing.

How to cite this paper: Rohit M. Thanki, Komal R. Borisagar,"Compressive Sensing Based Multiple Watermarking Technique for Biometric Template Protection", IJIGSP, vol.7, no.1, pp.53-60, 2015.DOI: 10.5815/ijigsp.2015.01.07

Copyright © 2015 MECS