ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(1), 42–48, January 2015* DOI : 10.17485/ijst/2015/v8i1/52707

Experimental Study of Sparse Watermarking Techniques for Multibiometric System

Rohit M. Thanki[1*] and Komal R. Borisagar[2]

[1]Faculty of Technology & Engineering, C U Shah University, Wadhwan City, Gujarat, India; rohitthanki9@gmail.com
[2]EC Department, Atmiya Institute of Technology & Science, Rajkot, Gujarat, India

Abstract

This paper focus on study and analysis of effect of watermarking technique in spatial domain combined with cs theory on verification and authentication performance of multibiometric system. In presented techniques, watermark fingerprint is compressed using CS theory before embedding into host biometric. These compressed fingerprint features embed into face image such that watermarked face image is used for verification and authentication of individual. Compressed fingerprint features are used for cross verification and authentication of individual. The modified LSB substitution based technique and modified correlation based technique using WGN combined with CS theory used to secure biometric data at system database and communication channel between two checkpoints of multibiometric system, respectively. The verification accuracy of multibiometric system using these watermarking techniques is around 96 % with more computational security and high perceptual quality of biometric data. The results show that these watermarking techniques do not have effect on authentication performance of multibiometric system. The novelty of paper is combined compressive sensing theory with watermarking technique for security of multibiometric data.

Keywords: Biometric Data, CS Theory, Multibiometric System, Watermarking

1. Introduction

In recent years, multibiometric system is used for recognition and identification of individual because multibiometric authentication system is overcome disadvantages of unimodal biometric system[1,2]. Multibiometric system is improving accuracy and security compare to unimodal biometric system[2]. Multibiometric system is utilized two or more than two biometric characteristics of individual for verification and authentication[2, 3]. Multibiometric system can be operated into three different mode like serial, parallel and hierarchical[3]. Multibiometric system has more advantages compared to biometric system but there are two big issues like template protection and fusion model associated with designing of multibiometric system. For solution of issues like template protection, digital watermarking technique is a one of solutions for template protection[4].

In this paper, we have study and analyzed two watermarking techniques combined with CS theory framework for multibiometric template protection. These two techniques provided two levels of security to biometric template at system database and communication channel between two modules of biometric system. One biometric template compressed and encoded fingerprint features used as a watermark is watermarked in face such that watermarked face image is used verification and authentication of individual. Here compressed and encoded fingerprint feature is used for cross verification and authentication of individual. For generation of compressed watermark fingerprint feature, Compressive Sensing (CS) theory[5,6] is used. These sparse measurements of fingerprint features get after application of Compressive Sensing theory is encoded in the binary from using uniform quantizer and is unique for every individual. These encoded sparse measurements of fingerprint features

*Author for correspondence

embedded into the face image of same owner to protect face template as well as perform the multibiometric operation. For watermarking, two spatial domain watermarking technique namely modified correlation based technique using WGN and modified LSB substitution based technique combined with Compressive Sensing (CS) theory framework are presented. The sparse watermarking based multibiometric system is shown in Figure 1. Here we used word **"sparse watermarking"** because in proposed techniques, we explore sparseness of Discrete Cosine Transform (DCT) for generation of sparse measurements of watermark biometric image.

2. Sparse Watermarking Techniques in Spatial Domain

Digital watermarking is process of embedding digital content as a watermark into host medium. Digital watermark is used for ownership and authentication of owner. The standard watermarking technique having some properties have been given in papers[7,8]. These properties are:

1. The watermark must be difficult to extract from watermarked content without introducing degradation to original content.
2. The watermark must be survived all image processing operations like compression, filtering and adding noise to watermarked content.

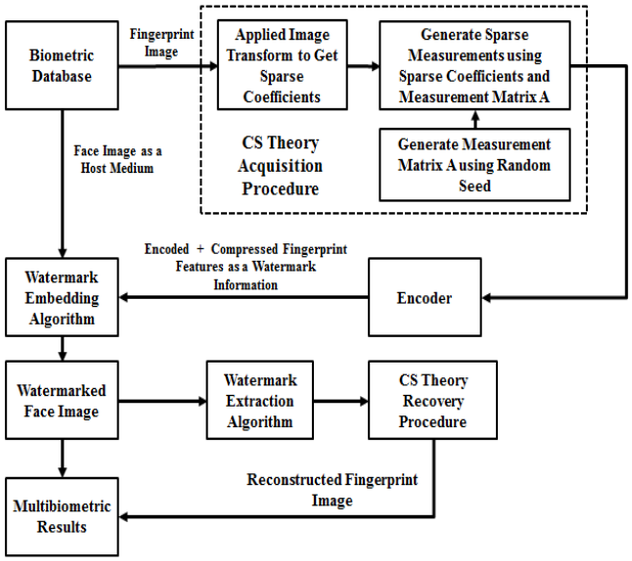


Figure 1. Block Diagram of Sparse Watermarking based Secure Multibiometric System.

3. An embedded watermark must be imperceptible to human visual system.
4. For watermarking application to biometric, watermark must not be detectable by the imposter authorities.

Figure 2 shows proposed watermark embedding and extraction for multibiometric template protection. Based on these properties and application to security of large scale multibiometric system, we have design and analyzed two watermarking algorithm in spatial domain with combination of CS theory for multibiometric template protection namely:

1. Modified Correlation Based Technique using WGN Signal[9]
2. Modified LSB Substitution Based Technique[10]

2.1 Modified Correlation Based Technique using WGN Signal[9]

For watermark embedding, correlation properties of White Gaussian Noise (WGN) signal as applied to a biometric image are used[9]. Encoded sparse measurements of fingerprint features $W_{Sparse}(x, y)$ is embed into original biometric image $B(x, y)$ according to equation 1:

$$B_W(x, y) = B(x, y) + N * W_{Sparse}(x, y) \quad (1)$$

Where $N$is noise power of WGN between 1 to 5 dB and $B_W(x, y)$ is the watermarked biometric image.

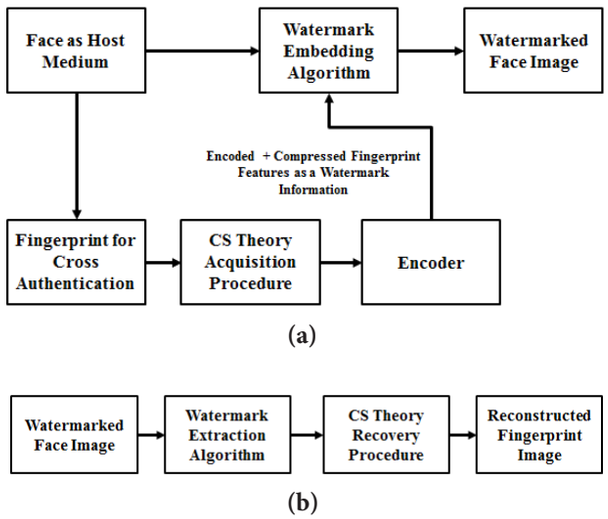
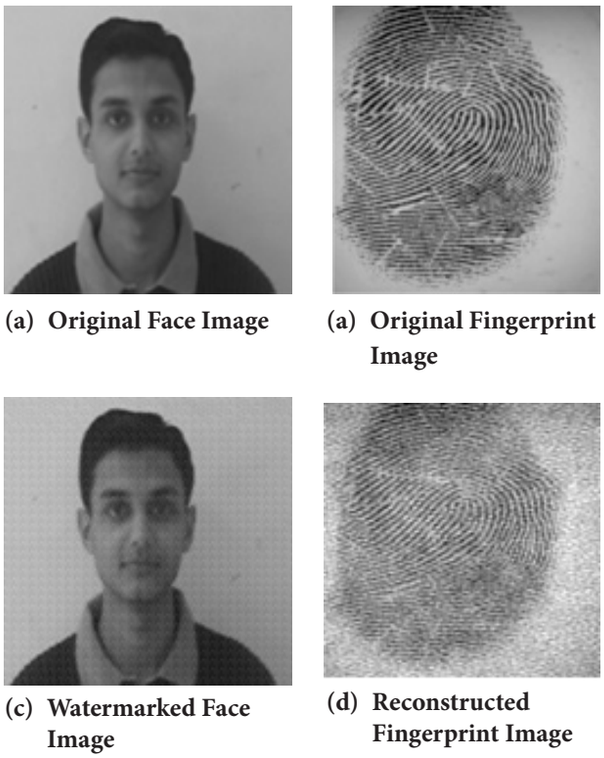


Figure 2. (a) Watermark Embedding (b) Watermark Extraction.

For detection of watermark, the encoded sparse measurements of fingerprint features with same power of noise and the correlation between WGN signal and watermarked biometric image is computed. If the correlation result exceeds threshold value, then encoded sparse measurements detect and set bit 1 value. After getting extracted sparse measurements of fingerprint features in binary form and then applied uniform quantizer to get actual sparse measurements of fingerprint features. Then applied cs recovery algorithm namely OMP[11] on actual sparse measurements to get reconstructed watermark fingerprint image at detector side. This technique used for template protection against modification attack at communication channel between two modules of multibiometric system.

Figure 3 shows the original face image[17], watermark fingerprint image[18], watermarked face image and reconstructed fingerprint image using OMP CS recovery algorithm after extraction and decoding with PSNR value 40.18 dB and SSIM value 98.89 %.



(a) Original Face Image

(a) Original Fingerprint Image

(c) Watermarked Face Image

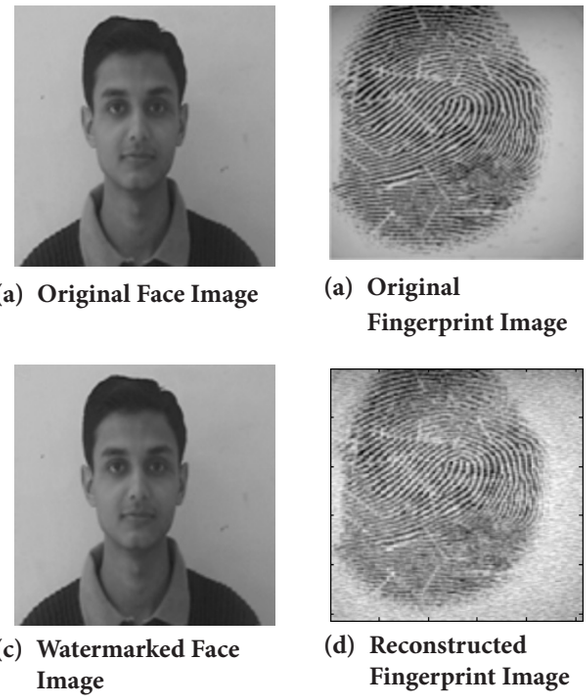
(d) Reconstructed Fingerprint Image

Figure 3. Results of Modified Correlation Based Technique using WGN.

2.2 Modified LSB Substitution Based Technique[10]

For watermark embedding, two Least Significant Bits (LSB) of particular block of host face image is modified by encoded sparse measurements of fingerprint features and generated watermarked face image. For detection of watermark, two Least Significant Bits (LSB) of watermarked face image take and reshape into extracted sparse measurements of fingerprint features from this LSB. Then compute BER between encoded sparse measurements and extracted sparse measurements. If BER value is equal to zero than applied uniform quantizer on extracted sparse measurements to get actual sparse measurements of fingerprint features. Then applied cs recovery algorithm namely OMP[11] on actual sparse measurements to get reconstructed watermark fingerprint image at detector side. If BER value is greater than zero then watermark fingerprint image cannot reconstructed from its extracted sparse measurements. This technique used for template protection against spoof attack at system database of multibiometric system.

Figure 4 shows the original face image[17], watermark fingerprint image[18], watermarked face image and reconstructed fingerprint image using OMP CS recovery algorithm after extraction and decoding with PSNR value 68.63 dB and SSIM value 99.70 %.



(a) Original Face Image

(a) Original Fingerprint Image

(c) Watermarked Face Image

(d) Reconstructed Fingerprint Image

Figure 4. Results of Modified LSB Substitution Based Technique.

3. Effect of Sparse Watermarking Techniques on Multibiometric System

In any multibiometric authentication system, two procedures are very important like verification and authentication of individual. The performance of multibiometric system is measured based on these two procedures. So design any template protection technique such that it is should not degraded performance of these two procedures. We have check performance of multibiometric authentication system is change or nor due to these proposed watermarking techniques. In order to showcase the effect of these proposed watermarking techniques on multibiometric system, we use face matching algorithm developed in[12, 13] and fingerprint matching algorithm developed in[14, 15]. We selected these algorithms because output of these algorithms give Euclidean distant between test biometric image and its closest match in the system database.

3.1 Effect of Modified Correlation Based Technique using WGN on Multibiometric System

In this section, we have given analysis of effect of modified correlation based technique using WGN on authentication and verification accuracy for face and fingerprint system of multibiometric system. For authentication and verification performance of face system, we stored 160 watermarked versions of authentic face images in a database and used 160 authentic face and 160 fake face images as query images to the database. For authentication and verification performance of fingerprint system, we stored 160 reconstructed watermark versions of authentic fingerprint images in a database and used 160 authentic fingerprint and 160 fake fingerprint images as query images to the database.

From the result obtained using matching algorithm[12, 13] based on various thresholds, we have calculated four probabilities with named like FRR-F, FRR-WF, FAR-F and FAR-WF and based on these values, plot Receiver Operating Characteristics (ROC) curve for face system of modified correlation based technique using WGN as shown in Figure 5.

Based on chart in Figure 5, we have selected threshold value is 1500. Distance between fake face images computed with watermarked face image in system database. The average distance is 6659.27 which are greater than selected threshold value. Also compute distance between authentic face images with watermarked face images and average distance between them is 492.56. Since the distance between watermarked face image and authentic face image is less than threshold show that face system unaffected by modified correlation based technique using WGN. These results are summarized in Table 1.

From the result obtained using matching algorithm[14, 15] based on various thresholds, we have calculated four probabilities with named like FRR-FP, FRR-WFP, FAR-FP and FAR-WFP and based on these values, plot Receiver Operating Characteristics (ROC) curve for fingerprint system of modified correlation based technique using WGN as shown in Figure 6.

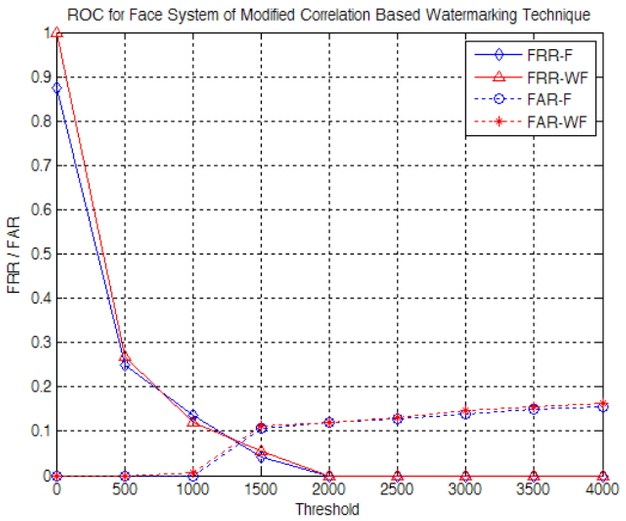


Figure 5. Roc Curve of Face System for Modified Correlation Based Technique Using WGN.

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

Table 1. Average Distance between Watermarked, Authentic and Fake Face Images (for 160 Images)

Average Distance between Watermarked and Authentic Face Image	Average Distance between Watermarked and Fake Face Image	Threshold
492.56	6659.27	1500

Based on chart in Figure 6, we have selected threshold value is 1000. Distance between fake fingerprint images computed with reconstructed fingerprint image in system database. The average distance is 1203.42 which are greater than selected threshold value. Also compute distance between authentic fingerprint images with reconstructed fingerprint and average distance between them is 732.25. Since the distance between reconstructed fingerprint image and authentic fingerprint image is less than threshold show that fingerprint system unaffected by modified correlation based technique using WGN. These results are summarized in Table 2.

Equal Error Rate (EER) difference for face system using ROC Curve shown in figure 5 is 1 % using watermarking and without watermarking. Equal Error Rate (EER) difference for fingerprint system using ROC Curve shown in figure 6 is 0.4 % using watermarking and without watermarking. Based on results shows in figure 5 and 6 that ROC curve of FAR and FRR values of face and fingerprint systems with watermarking is same as ROC curve of FAR and FRR values of face and fingerprint systems without watermarking which is indicated that modified correlation based watermarking technique using WGN fulfilled the criteria of template protection technique.

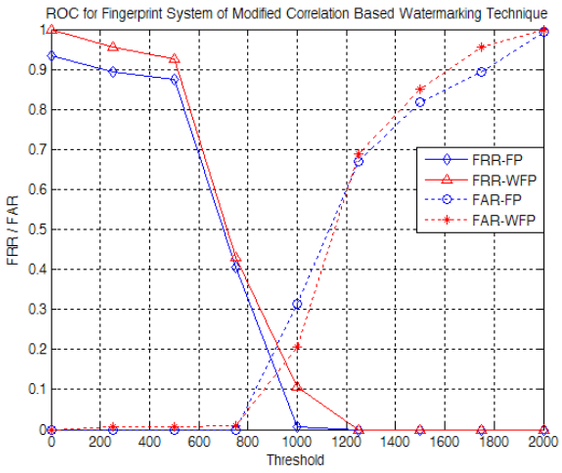


Figure 6. Roc curve of fingerprint system for modified correlation based technique using WGN.

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

Table 2. Average distance between watermarked, authentic and fake fingerprint images (for 160 Images)

Average Distance between Reconstructed Watermark and Authentic Fingerprint Image	Average Distance between Reconstructed Watermark and Fake Fingerprint Image	Threshold
732.35	1203.42	1000

For verification performance of multibiometric system, we have calculated verification accuracy of original host face image, verification accuracy of original fingerprint image, verification accuracy of watermarked face image and verification accuracy of reconstructed fingerprint image using equation described in[16]. The verification accuracy of face recognition[12, 13] is 96.25 % on original test faces and verification accuracy of fingerprint recognition[4,15] is 99.38 % on original test fingerprints. In modified correlation based technique using WGN, the verification accuracy of face recognition and fingerprint recognition is 94.38 % (after watermarking) and 88.13 % (after reconstruction) respectively. An overall verification accuracy of 96.69 % was achieved for modified correlation based watermarking technique using WGN based multibiometric system with compression of template and enhanced in template security.

3.2 Effect of Modified LSB Substitution based Technique on Multibiometric System

In this section, we have given analysis of effect of modified LSB substitution based technique using WGN on authentication and verification accuracy for face system of multibiometric system. Here we have not performed authentication and verification accuracy for fingerprint system because fingerprint is reconstructed when no attack applied on watermarked face image. Without attack, authentication and verification accuracy for fingerprint system using this watermarking technique is almost 100 %.

For authentication and verification performance of face system, we stored 160 watermarked versions of authentic face images in a database and used 160 authentic face and 160 fake face images as query images to the database. From the result obtained using matching algorithm[12,13] based on various thresholds, we have calculated four probabilities with named like FRR-F, FRR-WF,

FAR-F and FAR-WF and based on these values, plot Receiver Operating Characteristics (ROC) curve for face system of modified LSB substitution based technique as shown in Figure 7.

Based on chart in Figure 7, we have selected threshold value is 750. Distance between fake face images computed with watermarked face image in system database. The average distance is 2275.61 which are greater than selected threshold value. Also compute distance between authentic face images with watermarked face images and average distance between them is 90.75. Since the distance between watermarked face image and authentic face image is less than threshold show that face system unaffected by modified LSB substitution based technique. These results are summarized in Table 3.

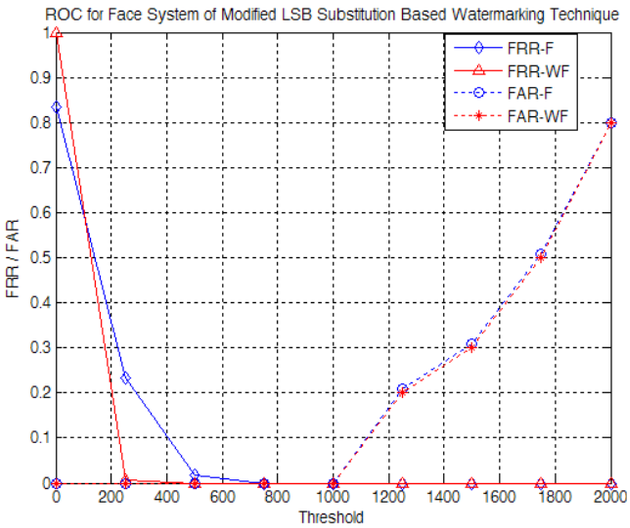


Figure 7. Roc curve of face system for modified LSB substitution based technique.

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

Table 3. Average distance between watermarked, authentic and fake face images (for 160 Images)

Average Distance between Watermarked and Authentic Face Image	Average Distance between Watermarked and Fake Face Image	Threshold
90.75	2275.61	750

Equal Error Rate (EER) difference for face system using ROC Curve shown in Figure 7 is 0 % using watermarking and without watermarking. Based on results shows in Figure 7 that ROC curve of FAR and FRR values of face systems with watermarking is same as ROC curve of FAR and FRR values of face systems without watermarking which is indicated that modified LSB substitution based watermarking technique fulfilled the criteria of template protection technique.

For verification performance of multibiometric system, we have verification accuracy of original host face image and verification accuracy of watermarked face image using equation described in[16]. The verification accuracy of face recognition[12,13] is 96.25 % on original test faces. In modified LSB substitution based technique, the verification accuracy of face recognition is 96.25 % (after watermarking). An overall verification accuracy of 96.25 % was achieved for modified LSB substitution based technique based multibiometric system with compression of template and enhanced in template security.

4. Conclusion

The study proposed two new biometric watermarking techniques for improving security of multibiometric authentication system. This paper presented two watermarking technique in spatial domain combined with CS theory for protection and authentication of multibiometric template. The proposed watermarking techniques provide security to biometric template at system database and over communication channel of biometric system against spoofing and stolen attacks. The verification accuracy of multibiometric system with modified correlation based technique using WGN is found to be 96.69 % and with modified LSB substitution based technique it is found to be 96.25 %. The payload capacity of proposed watermarking techniques obtained due to cs theory better than existed watermarking techniques in literature.

5. Acknowledgements

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

6. References

1. Jain A, Kumar A. Biometric Recognition: An Overview, Second Generation Biometrics: The Ethical, Legal and Social Context. In: Mordini E. Tzovaras D, editor. Springer; 2012, p. 49–79.
2. Jain A, Ross A, Pankanti S. Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security. 2006 June; 1(2):125–43.
3. Jain A, Ross A, Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology. Special Issue on Image and Video Based Biometrics. 2004 Jan; 14(1):4–20.
4. Jain A, Uludag U. Hiding Fingerprint Minutiae in Images; Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID); 2002. p. 97–102.
5. Candes E. Compressive Sampling. Proceedings of the International Congress of Mathematicians; 2006; Madrid, Spain.
6. Baraniuk R. Lecture notes Compressive Sensing. IEEE Signal Process Mag. 2007 July; 24:118–24.
7. Bolle RM, Connell JH, Pankanti S, Ratha NK, Senior AW. Guide to Biometrics. Springer Verlag; 2004.
8. Langelaar G, Setyawan I, Lagendijk RL, Watermarking Digital Image and Video Data. IEEE Signal Process Mag. 2000; 17:20–43.
9. Thanki R, Borisagar K. A Novel Robust Digital Watermarking Technique using Compressive Sensing for Biometric Data Protection. IJECCE. 2013 July; 4(4):1133–9, ISSN
10. Thanki R, Borisagar K. Biometric Template Spoofing Detection Using Sparse Watermarking Scheme. IJRITCC. 2014 July; 2(7):1768 –72.
11. Tropp J, Gilbert A. Signal Recovery from Random Measurements via Orthogonal Matching Pursuit. IEEE Trans Inform Theor. 2007 Dec; 53(12):4655–66.
12. Turk M, Pentland A. Face Recognition Using Eigenfaces. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition; 1991 Jun; Maui, USA. p. 586–91.
13. Moon H, Phillips P. Computational and Performance aspectsofPCA-basedFaceRecognitionAlgorithms.Perception. 2001; 30:303–21.
14. Jain A, Prabhakar S, Pankanti S. A Filterbank based Representation for Classification and Matching of Fingerprint. International Joint Conference on Neural Networks (IJCNN); 1999; Washington DC. p. 3284–5.
15. Prabhakar S. Fingerprint Classification and Matching Using a Filterbank [Ph.D. Thesis]. Michigan State University; 2001.
16. Vasta M, Singh R, Noore A. Improving Biometric Recognition Accuracy and Robustness Using DWT and SVM Watermarking, ELEX, 2005 Jun; 1(12):362–7.
17. Jain V, Mukherjee A. The Indian Face Database. 2002. Available from http://vis-www.cs.umass.edu/~vidit/IndiaFaceDatabase
18. Fingerprint Database. Available from http://bias.csr.unibo.it/fvc2004/databases.asp