International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 7 1768 – 1772

Biometric Template Spoofing Detection Using Sparse Watermarking Scheme

Rohit Thanki
Research Scholar, Faculty of Technology & Engineering
C U Shah University
Wadhwan City, Gujarat, India
rohitthanki9@gmail.com

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

***Abstract*—** In this paper, a semi fragile watermarking scheme based on compressive sensing theory proposed for detection of spoofing or modification of biometric template. This proposed scheme is explored sparseness, incoherent and computation security provided by compressive sensing for biometric template protection. The Discrete Cosine Transform (DCT) coefficients of biometric template are used to compute sparse measurement vector which is used as secure watermark information. This sparse measurement vector of biometric template as a watermark is embedding into two LSB of selected block of host biometric template of same individual. Extracted sparse measurement vector is required for CS theory recovery algorithm to reconstruct the original watermark biometric image at detector side. The biometric spoofing can be detected by comparing extracted sparse measurement vector and original sparse measurement vector of watermark biometric.

Keywords *- Biometric Spoofing; Compressive Sensing; Sparse Watermarking; Spatial Domain*

*****

I. INTRODUCTION

Watermarking schemes are used for copyright protection and content authentication of multimedia content like images, videos and text over internet [1, 2 and 3]. In most of watermarking schemes, embed random sequences into host medium according to secure watermark logo or image bit [1, 2 and 3]. In 2001, Ratha and its researcher team introduced issued like biometric template spoofing or modification at system database and biometric template stone at communication system in biometric system [4]. For solving these issues, watermarking is one solution is proposed by Jain and its researcher team in 2003 [5].

In this paper, a semi-fragile watermarking scheme using compressive sensing theory framework proposed for spoof detection of biometric template. N×N dimensional biometric watermark is converting into its transform domain using DCT and then multiple N×1dimensional of DCT coefficients with M×N dimensional of random seed with to generate M×1 dimensional sparse measurement vector. This sparse measurement vector used as watermark information for embed and extraction. This sparse measurement vector is used for spoof or modification detection for biometric template. The watermarking idea is taken from [7, 14] with significant modification and improvements in computation security in implementation. The work also goes a step further wherein it sparse measurement vector of biometric watermark is generated using compressive sensing theory which used as watermark and extracts this sparse measurement vector at detector side for comparing with original sparse measurement vector for detection of spoofing or modification of biometric template.

The Compressive Sensing theory is provides computational security and compression to biometric data. The bit error rate (BER) measure is used for detection of biometric spoofing or modification. Section 2 describes the related work and literature review followed by section 3 describes the proposed watermarking scheme followed by section 4 describes implementation and analysis of experimental results. Finally gives the conclusion of the paper.

II. RELATED WORK

Many researchers are introduced and proposed various watermarking schemes for biometric template and content authentication in last decade are reviewed below. Authors in [6] described fragile watermarking scheme which provides more securing protection and verification using watermarked version of fingerprint images for copyright protection application. Authors in [7] described simple data hiding scheme based on LSB substitution for standard images for copyright protection application. Authors in [8] introduced multimodal biometric image watermarking scheme based on blind and spread spectrum scheme for face and fingerprint data using two stage integrity verification. The authors in [8] also described that proposed method is able to find tamper region in watermarked data using feature vectors of face image is embed as watermark pattern into fingerprint image.

Authors in [9] described fragile watermarking for remote multimodal biometric authentication for embedding biometric feature values into facial image using combination of amplitude modulation and determining bit priority level of feature values over network base authentication system. This proposed method is improving security of biometric data and reduce bandwidth. Authors in [10] described using PSO algorithm is used for find best location in spatial domain of host medium where embeds secure watermark pixel. Authors in [11] introduced image watermarking scheme using CS theory for detection of image tampering using wavelet transform for reducing dimension and improved security of data.

Authors in [12] proposed watermarking scheme with flexile self recovery quality based on compressive sensing and discrete cosine transform. Then extracted watermark data for checking sparseness in DCT domain without any modification. This scheme is used for image tampering identification. Authors in [13] proposed robust watermarking method to enhance security of multimodal biometric authentication system. The authors in [13] are described that fist convert face feature into raw data as watermark and embed into fingerprint with a blind SS – QIM scheme. The authors in [14] are described simple LSB

 ISSN: 2321-8169
1768 – 1772

substitution method for standard video where embed logo into video frame.

III. PROPOSED WATERMARKING SCHEME

This section described proposed watermarking scheme where applied image transform like DCT on watermark biometric image and convert into its sparse measurement vector using compressive sensing framework which is described in [15, 16 and 17]. Then encode this sparse measurement vector into logic 0 and 1 using uniform quantization procedure. After encoding, embed sparse measurement vector as a watermark into two LSB of selected block of host biometric image in spatial domain. This proposed scheme is divided into four phases like watermark preparation using Cs theory framework, embedding procedure, extraction procedure and spoofing detection procedure. The block diagram of proposed scheme is shown in figure 1.

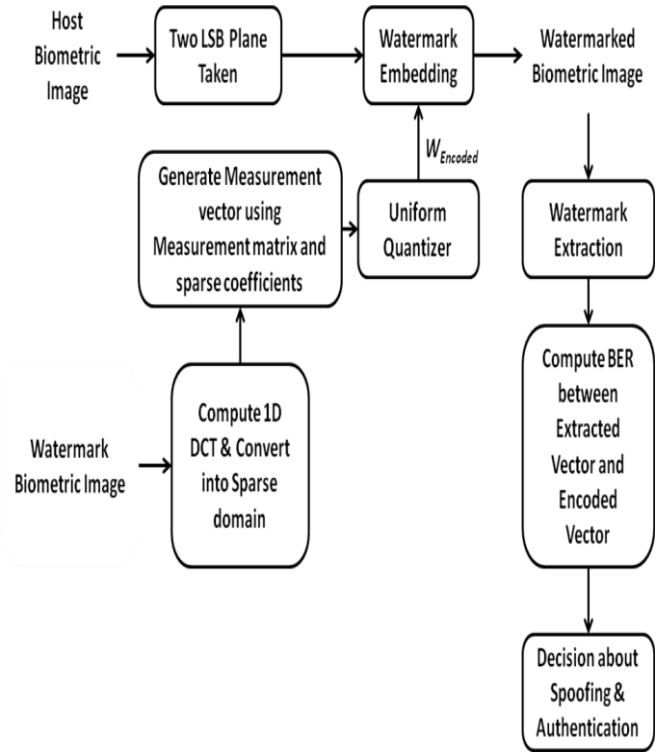


Figure 1. Proposed Watermarking Scheme

A. Watermark Preparation Using CS Theory Framework

- Take watermark biometric image of an owner and compute size of watermark biometric image.
- Apply image transform like Discrete Cosine Transform (DCT) on watermark biometric image and convert into its sparse coefficients vector using below equation [16, 17]:

$$x = \psi \times f \quad (1)$$

Where x is representing sparse coefficient of watermark biometric image; Ψ is representing appropriate basis function (DCT); f is representing original watermark biometric image.

- Generate measurement matrix using length of sparse coefficients and random seed which is same for embedder and detector side.
- Then generate sparse measurement vector of watermark biometric image using below equation for size of row data of watermark biometric image [16, 17].

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

Where y is representing sparse measurement vector with size of M×1; ϕ is representing measurement matrix which is multiplication of appropriate basis coefficients and random seed with size of M×N; x is representing sparse coefficient vector of watermark biometric image with size of N×1.

- Then sparse measurement vector is quantized using a uniform quantizer and encode into logic 0 and 1 and reshape this encoded sparse measurement vector into matrix form which is denoted as $\boldsymbol{W_{Encoded}}$. This encoded sparse measurement vector use as a watermark information.

B. Embedding Procedure

- Take host biometric image of an owner and compute size of M × N. Then divide host biometric image into equal blocksize and chose one block for embedding watermark.
- For entire size of sparse measurement vector repeat below step for generation of watermarked biometric image where two LSB of each pixel of host biometric is modified according to encoded sparse measurement vector.

```
For i = 1: Nm
    For j = 1: Mm
        I_W_block (i, j) = bitset (I (i, j), W_Encoded, 2);
    End
End
```

- Reshape all pixels and generate watermarked biometric image.

C. Extraction Procedure

- Take watermarked biometric image and compute size of M × N. Then divide watermarked biometric image into equal blocksize and take block which is used for generation of watermarked image.
- For entire size of sparse measurement vector repeat below step for extraction of sparse measurement vector of watermark biometric image.

```
For i = 1: Nm
    For j = 1: Mm
        W_Extracted (i, j) = bitget (I_W_block (i, j), 2);
    End
End
```

- Reshape extracted matrix and which is denoted as $\boldsymbol{W_{Extracted}}$.

D. Spoofing Detection Procedure

- For spoofing detection, Compare the BER value between the encoded sparse measurement vector $\boldsymbol{W_{Encoded}}$ and extracted sparse measurement vector $\boldsymbol{W_{Extracted}}$ is equivalent to comparing MSE value between the two images which is described in [19] and MSE value between the two hash values which is described in [12].
- Here two condition based on some fixed threshold value $\boldsymbol{\tau_{BER}}$ are formulated for spoof detection of biometric template.

- Condition 1: Biometric Template is authentic and not spoof or modified by imposter if $BER\ (W_{Encoded}, W_{Extracted}) < \tau_{BER}$;
- Condition 2: Biometric Template is unauthentic and spoof or modified by imposter $BER\ (W_{Encoded}, W_{Extracted}) > \tau_{BER}$;
- If condition 1 is fulfill then decode actual sparse measurement vector from extracted sparse measurement vector and applied CS recovery algorithm described in [18] to reconstruction watermark biometric image at detector side.

IV. EXPERIMENTAL RESULTS

Performance of the scheme is evaluated using Face samples from Indian Face database [22] and Fingerprint samples from FVC 2004 [23] which is shown in figure 2. For experiments 8 bits gray scale fingerprint images taken as watermark information and face images taken as a host medium. The size of watermark and host biometric image is M × N = 256 × 256 pixels selected.

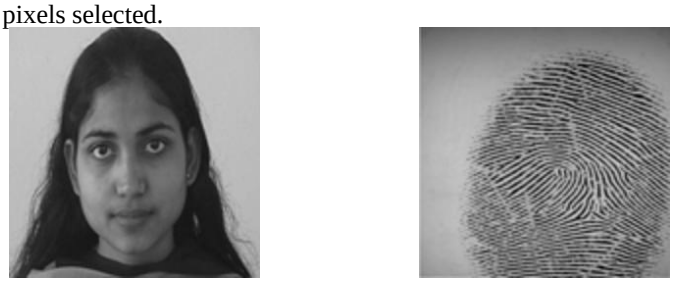


Figure 2. Standard Test Biometric Template Images

For generation of sparse measurement vector of fingerprint, DCT coefficients of fingerprint image is get using 1D Discrete Cosine Transform (DCT) and generated sparse measurement vector using equation 2 are as follows $y_{256\times1} = \phi_{256\times256} \times x_{256\times1}$. Measurement matrix ϕ is generated with help of rand function in MATLAB where input of rand function is length of row data of watermark biometric image and length of sparse coefficients. Then sparse measurement vector values y are quantized using 256 uniform level quantizer to obtain the encoded sparse measurement vector with 1 bits / level. The size of encoded sparse measurement vector is 256 × 1. This encoded sparse measurement vector is converted in to a matrix of size 16 × 16 which is used as a watermark information. The encoded sparse measurement vector is shown in figure 3.

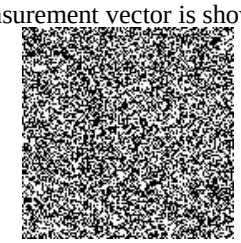


Figure 3. Encoded Sparse Measurment Vector of watermark biometric

This watermark information is embedding into two LSB of 16 × 16 block size of host biometric image which is depending on programmer. Because of this approach is provide computational security to algorithm because of only programmer is known which 16 × 16 blocksize of pixels of host medium is modified according to encoded sparse measurement vector of watermark biometric. The same quantizer is used at detector side for decoding of sparse measurement vector if not spoofing is detected. The result of experimentation is summarized in Table 1 and figure 4 with PSNR and NCC of watermarked image as 69.24 dB and 1.00 respectively. Figure 4 shows that watermarked biometric image having high perceptual quality and figure 5 shows that reconstruct watermark biometric image having high similarity with original watermark image. Structural Similarity Measure Index (SSIM) [24] used for finding similarity between original watermark image and reconstruct watermark image at detector side when biometric is not modified by imposter.

Figure 4. (a) Original Host Biometric Face Image; (b) Watermarked Biometric Face Image with PSNR = 69.24 dB and NCC = 1.0

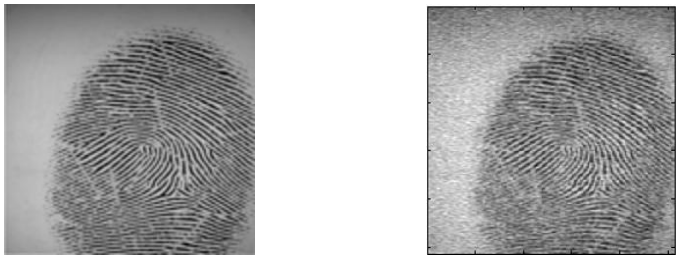


Figure 5. (a) Original Watermark Biometric Fingerprint Image; (b) Reconstruct Watermark Fingerprint Image with SSIM = 99.62

Peak Signal to Noise ratio (PSNR), NCC and BER are used as a quantitative measure for performance evaluation in term of perceptual invisibility and fragility property of proposed watermarking algorithm. The threshold value τBER is chose 0.1 for compare of sparse measurement vector for spoof detection. Comparing the BER between the extracted and encoded measurement vector is similar to comparing MSE between the two images [12, 19].

For checking fragility of proposed scheme, different attacks like JPEG compression (Quality factor Q = 90), Gaussian noise (mean = 0, variance = 0.001), Salt & Pepper noise (density = 0.005), Speckle noise (variance = 0.004), Median Filter (size = 3 × 3), histogram equalization and cropping applied on watermarked image. Results shows in table 1 is indicate that the proposed scheme is shows robustness against cropping and salt & Pepper noise attack and not robust against JPEG compression, Gaussian noise, Speckle noise, Median filter and Histogram equalization attack which indicated that this proposed scheme having property of semi-fragility.

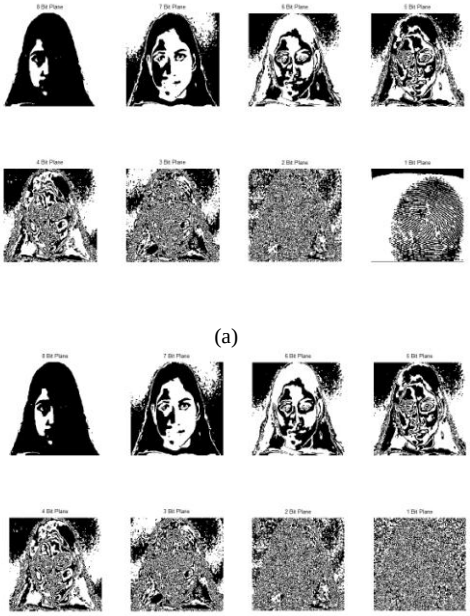
TABLE I. QUANTITATIVE MEASURES OF PROPOSED SCHEME

Attacks	PSNR (dB)	NCC	BER	Decision
No Attack	69.24	1.00	00	Authentic
JPEG Compression	49.04	1.00	118	Unauthentic
Gaussian Noise	30.00	0.99	133	Unauthentic
Salt & Pepper Noise	28.27	0.99	00	Authentic
Speckle Noise	29.77	0.99	136	Unauthentic
Median Filter	52.09	1.00	58	Unauthentic
Histogram Equalization	21.39	0.98	167	Unauthentic
Cropping	27.26	0.99	00	Authentic

BER values in table 1 is indicates that watermark biometric image is declared not spoof and authentic only if BER value is less than 0.1 for comparison of extracted sparse measurement vector and encoded sparse measurement vector considering all attacks on watermarked image otherwise biometric image is spoof or modified by imposter.

In order to show the effect of proposed watermarking scheme on biometric system, face matching algorithm described in [20, 21] used for face recognition and fingerprint matching algorithm described in [25, 26] used for fingerprint recognition which gives Euclidean distance between query biometric image and its closest match in database. Here stored 150 watermarked versions of face images and 150 reconstruct versions of fingerprint images is generated using proposed scheme in a database. The threshold distance selected 1500 for face recognition and 1000 for fingerprint recognition. The accuracy of face and fingerprint recognition is 100 % before applying proposed scheme and after applying proposed scheme is 100 % which shows that proposed scheme does not effect on performance of biometric system.

The computational security of proposed scheme is excellent compare to existed scheme in [7, 14] after applying bit plane slicing attack on watermarked image because when bit plane slicing attack is applied on watermarked biometric image generated using scheme described in [7, 14] then secure watermark information is easy retrieved by imposter which is shown in figure 6(a). When bit plane slicing attack is applied on watermarked biometric image using proposed scheme then secure watermark information is not retrieved by imposter which is shown in figure 6 (b) because of two reasons. First reason is that instead of watermark pixels, embed sparse measurement vector of watermark and second reason is that sparse measurement vector of watermark information embed into particular block of host biometric medium instead of all pixels of host biometric medium.



(a)

(b)

Figure 6. (a) Bit Plane Representation of Watermarked Image generated using Scheme described in [7, 14]; (b) Bit Plane Representation of Watermarked Image generated using Proposed Scheme

V. CONCLUSION

This paper shows a semi-fragile watermarking scheme using compressive sensing theory for spoof detection of biometric template. The encoded sparse measurement vector of secure watermark fingerprint image used as a reference data. This reference data may be destroyed by imposter than secure watermark biometric data recovery is not possible at detector side which is indicated spoofing or modification of template is done by imposter. Proposed scheme is partially robust against salt & pepper noise and cropping attack. The computational security of proposed scheme is excellent compare to existed scheme in [7, 14] after applying bit plane slicing attack on watermarked image. The proposed scheme is compared with existed scheme which is described in [7, 10, 11 and 14] shows that proposed scheme provide more quality perceptual to biometric template in term of PSNR values and computational security because of compressive sensing framework. The comparison of proposed scheme with existed scheme in consideration of various features is given in table 2.

TABLE II. COMPARISON OF PROPOSED SCHEME WITH EXISTED SCHEME IN [7], [10], [11] AND [14]

Features	Scheme in [7] & [14]	Bedi Scheme et al. [10]	Zhang Scheme et al. [11]	Proposed Scheme
Type	Robust	Robust	Fragile	Semi-fragile
PSNR (dB)	46.37	40	37.90	69.24
No. of LSB	One	One	Three bit of 8 × 8 DCT block of image	Two
Host Medium	Standard image or video	Standard image	Standard image	Any biometric image
Watermark Information	Random numbers or logo	Logo or standard image	Random hash	Encoded measurement vector of biometric image
Computational Security Achieved	No such scope	PSO Algorithm	CS Theory Framework	CS Theory Framework
Authentication through Template Matching	No such scope	No such scope	No such scope	Possible

ACKNOWLEDGMENT

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.

REFERENCES

[1] R. Wolfgang, C. Podilchuk and E. Dalp, "Perceptual Watermarks for Digital Images and Video", Proceedings of IEEE, vo. 87, no. 7, pp. 1108 – 1126, 1999.

[2] 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

[3] 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

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

[6] S. Pankanti and M. Yeung, "Verification Watermarks on Fingerprint Recognition and Retrieval", In Electronic Imaging'99, pp. 66-78, International Society for Optics and Photonics, 1999.

[7] C. Chan and L. Cheng, "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition 37, pp. 469-474, 2004.

[8] W. Kim and H. Lee, "Multimodal Biometric Image Watermarking Using Two Stage Integrity Verification", Signal Process, 89(12), pp. 2385-2399, December 2009.

[9] T. Hoang, T. Dat and D. Sharma, "Remote Multimodal Biometric Authentication Using Bit priority-based Fragile Watermarking", In Proceedings of 19th IEEE International Conference on Pattern Recognition (ICPR 2008), pp. 1-4, 2008.

[10] P. Bedi, R. Bansal and P. Sehgal, "Using PSO in Image Hiding Scheme based on LSB Substitution", In Advances in Computing and Communications, pp. 259-268, Springer Berlin Heidelberg, 2011.

[11] X. Zhang, Z. Qian, Y. Ren and G. Feng, "Watermarking with Flexible Self-recovery Quality based on Compressive Sensing and Compositive Reconstruction", IEEE Transactions on Information Forensics and Security, vol. 6, no. 4, pp. 1123-1232, 2011.

[12] 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.

[13] C. Li, B. Ma, Y. Wang and Z. Zhang, "Sparse Reconstruction Based Watermarking for Secure Biometric Authentication", Biometric Recognition, volume 7908, pp. 244-251, December 2011.

[14] A. Kothari and V. Dwivedi, "Performance Analysis of Spatial and Frequency Domain based Digital Image Watermarking – A Road towards Video Watermarking", Proceeding of International Conference of Innovative Science and Technology, pp. 515-519, Rajkot, April 2011.

[15] D. Donoho, "Compressed Sensing", IEEE Transaction on Information Theory, vol. 52, no. 4, pp. 1289– 1306, April 2006.

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

[17] R. Baraniuk, Lecture notes "Compressive Sensing", IEEE Signal Processing Magazine, Vol. 24, pp. 118-124, July 2007.

[18] E. Candès and J. Romberg, "L1-Magic: Recovery of Sparse Signals via Convex Programming", October 2005.

[19] L. W. Kang, C.S. Lu, and C.Y. Hsu, "Compressive sensing- based image hashing", Proc. ICIP 2009, pp.1285- 1289, 2009.

[20] M. Turk and A. Pentland, "Face Recognition Using Eigen faces", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 586 – 591, Maui, Hawaii, USA, June 1991.

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

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

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

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

[25] 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.

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