Security of Biometric Data Using Compressed Watermarking Technique

Rohit Thanki*, Komal Borisagar**
*Faculty of Technology & Engineering, C U Shah University, Wadhwan, India
**Department of Electronics and Communication Engineering, Atmiya Institute of Technology & Science, Rajkot, India

Article Info

Article history:

Received Jul 22, 2014
Revised Sep 9, 2014
Accepted Sep 20, 2014

Keyword:

Biometric Data
Compressive Sensing Theory
Singular Value Decomposition
Discrete Wavelet Transform
Watermarking

ABSTRACT

This paper has focus on biometric data security over open communication channel of biometric system. Here biometric data is encoded using cs theory and wavelet based embedding technique. The biometric data is convert into encoded sparse measurements which is generating using SVD, random seed and uniform quantization process. Then these encoded sparse measurements are embedding into the host color biometric data using wavelet based watermarking technique. This proposed technique has explored dimension reduction and computational security provided by compressive sensing. This proposed technique has also helps to compressed and to send secret data over noisy communication channel of biometric system against various attacks. The proposed technique provides more security compare to existed technique in literature due to CS theory. The novelty of proposed technique is that, watermark information is compressed and encoded iris image using CS theory and uniform quantization.

Corresponding Author:

Rohit Thanki,
Research Scholar, Department of Electronics and Communication Engineering,
Faculty of Technology and Engineering, C U Shah University,
Surendranagar – Ahmedabad Highway, Wadhwan City, Gujarat, India.
Email: rohitthanki9@gmail.com

1. INTRODUCTION

Biometric template based authentication system is used for human identification and authentication in organization in present world because of every individual having unique biometric characteristics [1, 2]. In 2001, Ratha and its research team are identified several vulnerable points in biometric authentication system [3]. There are most important vulnerable point in biometric system is template modification at communication channel between two modules. AK Jain and its research team are proposed that digital watermarking is one of solution for this issue [4]. They are also point out some disadvantages in biometric system like sensor noise, different variation in database, security and privacy of biometric template. For over come of these disadvantages, A. Ross and its research team are give new biometric system which is called as multimodal biometric system where two or more biometric template is used for identification and authentication of individual [5, 6]. But when multimodal biometric system is design for large scale biometric data, then biometric template can be easily reconstructed form stored feature at system database by imposter and this situation is introduced security of biometric template protection issue in multimodal biometric system.

In few last years, many researchers are proposed and described watermarking technique for biometric data protection. Here some of techniques are reviewed which is related to proposed work. Author in [7] described image watermarking technique where wavelet coefficients are modified according to bit of watermark information. Author in [8] described blind biometric watermarking scheme for signature using wavelet transform where second level details wavelet coefficients of host image is modified accord to signature bit. Author in [9] proposed a DWT and DCT based watermarking technique for multimodal biometric data protection. In this technique, SVD is applied on biometric watermark data and this data is embedding into higher frequency wavelet coefficients. Author in [10] described robust watermarking technique to enhance security of multimodal biometric system. In this proposed technique, first face feature taken as watermark data which is embedding into fingerprint image using blind SS – QIM scheme.

Author in [11] described a new authentication scheme based on multimodal biometric verification and ridgelet transform watermarking technique for face and iris data for Digital Rights Management (DRM). Author in [12] proposed multimodal biometric watermarking technique based on correlation analysis for security of biometric data over communication channel of network. In this proposed technique, authors are first find correlation between watermark and host image using PLS and PSO and based on this result. Biometric data are embedding into host image. Author in [13] proposed LSB and wavelet based watermarking technique for secure face feature embed into fingerprint image. Author in [14] proposed various watermarking technique performance for security of user verification based on fingerprint and facial image. The authors claim that this approach improves accuracy of user verification and watermark detection. Author in [15] proposed watermarking technique based on cs theory which includes compressed sensing process and compressed sensing recovery process. This technique is more robust and secure against different watermarking attacks.

The work present in paper arises from developing watermarking technique for multimodal biometric system where iris data embeds as a biometric data. Now a day, iris is an accepted trait for worldwide as individual authentication. In this paper, a technique is proposed which embeds encoded sparse measurements of iris data as a watermark in first level horizontal and vertical wavelet coefficients of red channel of host color face image. The host color face image is decomposed using single level discrete wavelet transform. The encoded sparse measurements of iris data is generated using Singular Value Decomposition (SVD) and Compressive Sensing Theory framework. We have explored sparseness provided by SVD to generate linear measurement vector. We have borrowed the idea from [7 and 25] with significant modification in technique. The proposed work also goes a step further where biometric data is compressed and encoded by CS theory framework and uniform quantization respectively before embedding into host medium. The reset of paper organized such that section 2 described basic concept of CS theory, section 3 described proposed watermarking technique and section 4 described experiment results and last section 5 described conclusion.

2. BASIC CONCEPT OF COMPRESSIVE SENSING THEORY

Any signal or image can be reconstructed from its Fourier coefficients successfully proved by D. Donoho and E. Candès in 2006 [19, 20]. Based on this concept, E. Candès introduced new signal processing theory is called Compressive or Compressed Sensing Theory. Compressive sensing is a new technology where signal or image is acquired in a compressed format. Any image can be acquired in a compressed format using below equation 1 and 2:

$$x = \Psi \times f \tag{1}$$

$$y = A \times x \tag{2}$$

Where y is a sparse measurements of image with size of M × 1 (M ≤ N), A is a measurement matrix which is same for embedder and detector side (M × N), Ψ is basis transformation which is applied on image, x is a spa rse coefficient with size of N × 1, f is an original image. Here M is deciding factor for dimensional reduction and image compression rate.

The cs recovery process is inversion of cs acquisition. Where compressed data are fed to some non-linear optimization algorithm to reproduced the complete signal or image. When measurement matrix A is satisfies RIP property and incoherence property [21] then sparse coefficients *x* can be get form measurements using below equation 3:

$$\min \|S\|_1 \, s.t. y = A \times x \tag{3}$$

Where S is indicated CS recovery algorithm like L_1 minimization, Basis pursuit, OMP.

3. PROPOSED WATERMARKING TECHNIQUE

This section describes the proposed watermarking technique based on compressive sensing theory and correlation properties of Pseudo Random Noise (PN) sequence in wavelet domain. In this proposed technique, color face image is taken as host medium and applied single level discrete wavelet transform (DWT) on red component of host face image and get HL and LH wavelet coefficients for watermark embedding. The iris image is taken as watermark medium and which is converted into sparse measurements using cs theory. The uniform quantization is used for encoding sparse measurements of iris image into bit 0 and 1. These encoded sparse measurements of iris image taken as watermark information which is embed into color face image. The proposed technique is divided into three parts like watermark preparation, watermark embedding procedure and watermark extraction & reconstruction procedure. The proposed watermark embedding procedure and extraction & reconstruction procedure is shown in figure 1 and 2 respectively. In figures dotted box have shown cs acquisition procedure at embedder side and cs reconstruction procedure at detector side.

3.1. Watermark Preparation

The watermark preparation steps are described below:

- Take watermark biometric image and computer size of image which is N × N.
- Applied singular value decomposition (SVD) on watermark biometric image and convert into U, S and V matrix. The S matrix value with size of $N^2 \times 1$ which is taken as sparse coefficients and denoted as *x*.
- Generate measurement matrix *A* with size of $M \times N^2$ ($M \leq N$) using random seed which is same at embedder and decoder. Where M is deciding factor for compression.
- Generate sparse measurements *y* of biometric image using measurement matrix *A* and sparse coefficients *x* using equation 1 and 2.
- Then applied uniform quantization with 2 bit / level on sparse measurements and encoded into W (0, 1).
- Now these encoded sparse measurements are used as secure watermark information.

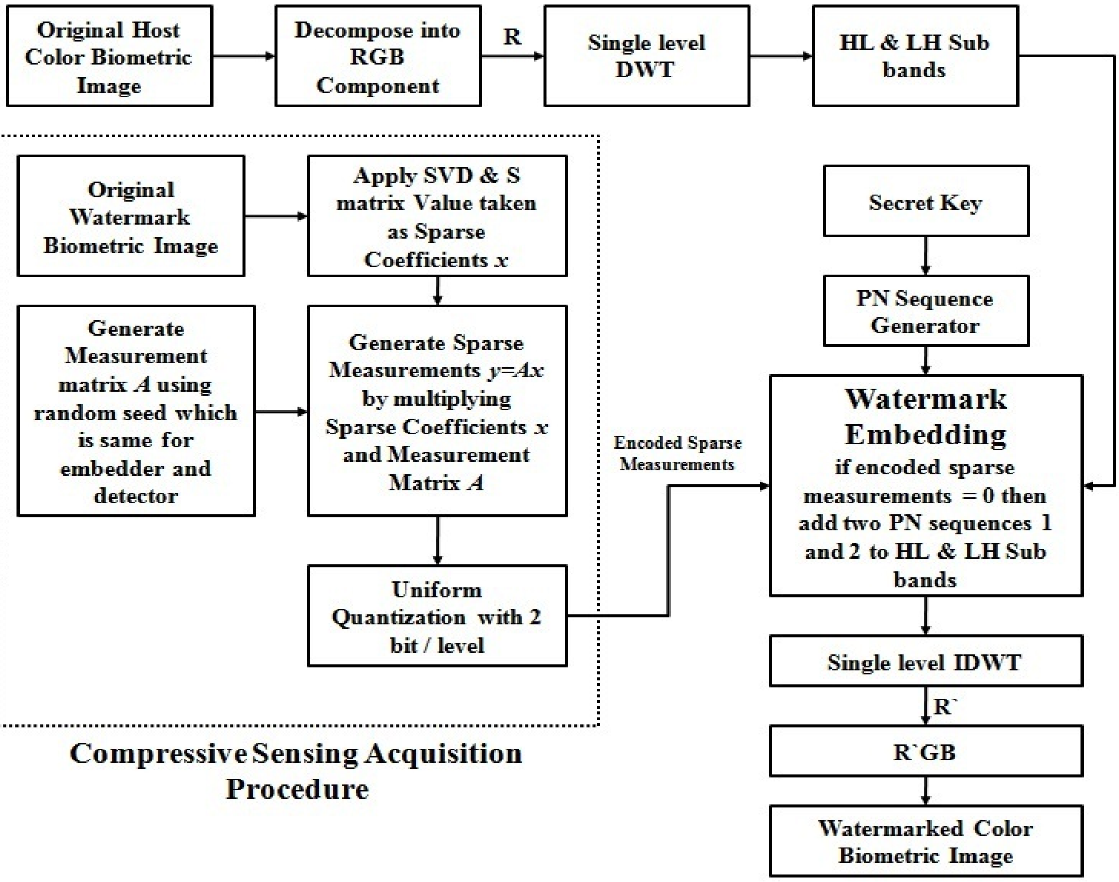
Original Host Color Biometric Image
Decompose into RGB Component
R
Single level DWT
HL & LH Sub bands
Original Watermark Biometric Image
Apply SVD & S matrix Value taken as Sparse Coefficients x
Generate Measurement matrix A using random seed which is same for embedder and detector
Generate Sparse Measurements y=Ax by multiplying Sparse Coefficients x and Measurement Matrix A
Uniform Quantization with 2 bit / level
Compressive Sensing Acquisition Procedure
Encoded Sparse Measurements
Secret Key
PN Sequence Generator
Watermark Embedding if encoded sparse measurements = 0 then add two PN sequences 1 and 2 to HL & LH Sub bands
Single level IDWT
R`
R`GB
Watermarked Color Biometric Image

Figure 1. Watermark Embedding Procedure

3.2. Watermark Embedding Procedure

The watermark embedding steps are described below (adopted from 7, 16, 17 and 18):

- Take host color biometric image and compute size of M × N. Take red component of host biometric image where watermark information is embedded.
- Applied single level discrete wavelet transform on red component of host biometric image and get different wavelet coefficients like LL, HL, LH and HH.
- Generate two pn sequences is generated using fixed noise power where one pn sequence is for bit 0 and another pn sequence is for bit 1.
- Generate watermarked biometric image using Cox algorithm [22] equation and which is given below.
- If encoded sparse measurements is bit 0 then

$$HL_{1R}(RW) = HL_{1R} + N * PN\_Sequence\_1 \quad (4)$$

$$LH_{1R}(RW) = LH_{1R} + N * PN\_Sequence\_2 \quad (5)$$

Where HL_{1R} *(RW)* and LH_{1R} *(RW)* is modified HL and LH Subband of red component of host biometric image, HL_{1R} and LH_{1R} is original *HL* and *LH* Subband of red component of host biometric image, *N* is gain factor, *PN_Sequence_1* is pn sequence 1 for bit 0 of encoded sparse measurements, *PN_Sequence_2* is pn sequence 2 for bit 1 of encoded sparse measurements.

- Applied inverse single level discrete wavelet transform to get watermarked biometric image.

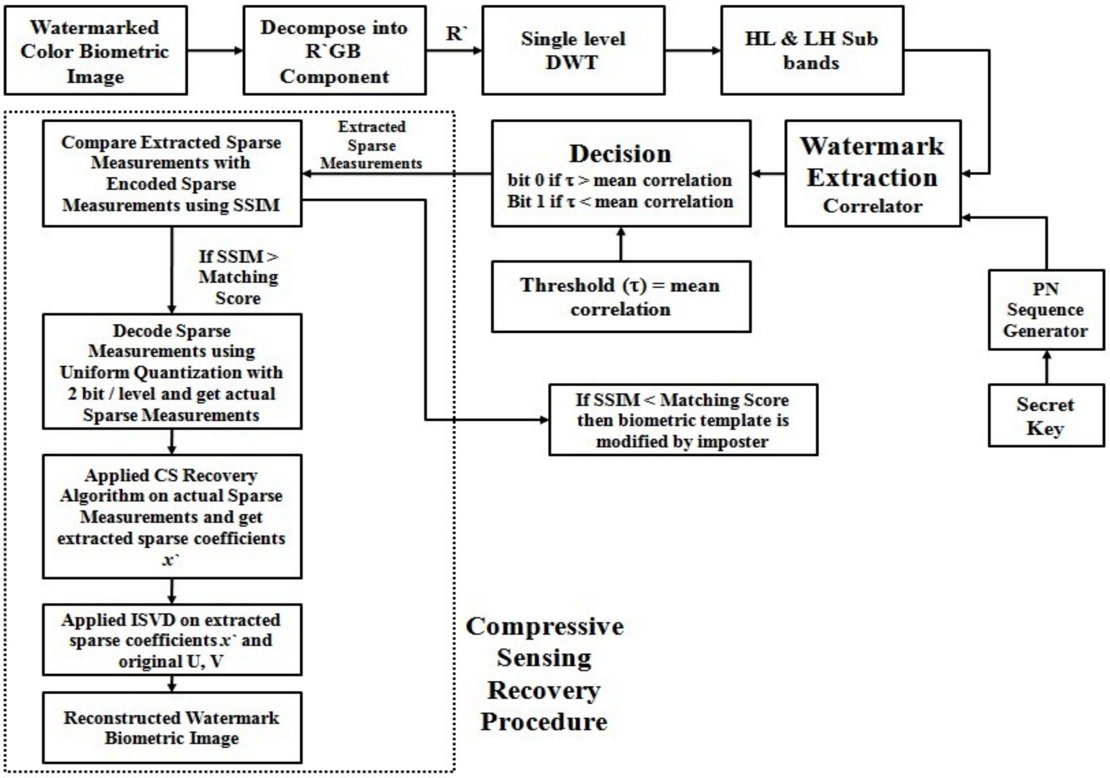
Watermarked Color Biometric Image
Decompose into R`GB Component
R`
Single level DWT
HL & LH Sub bands
Watermark Extraction Correlator
PN Sequence Generator
Secret Key
Decision
bit 0 if τ > mean correlation
Bit 1 if τ < mean correlation
Threshold (τ) = mean correlation
Extracted Sparse Measurements
Compare Extracted Sparse Measurements with Encoded Sparse Measurements using SSIM
If SSIM > Matching Score
If SSIM < Matching Score then biometric template is modified by imposter
Decode Sparse Measurements using Uniform Quantization with 2 bit / level and get actual Sparse Measurements
Applied CS Recovery Algorithm on actual Sparse Measurements and get extracted sparse coefficients x`
Applied ISVD on extracted sparse coefficients x` and original U, V
Reconstructed Watermark Biometric Image
Compressive Sensing Recovery Procedure

Figure 2. Watermark Extraction & Reconstruction Procedure

3.3. Watermark Extraction & Reconstruction Procedure

The watermark extraction & reconstruction steps are described below (adopted from 7, 16, 17 and 18):

- Take watermarked biometric image and compute size of M × N. Take red component of watermarked biometric image for extraction of encoded sparse measurements.

- Applied single level discrete wavelet transform on watermarked biometric image and get different wavelet coefficients like LL, HL, LH and HH.
- Initialize decoded sparse measurements to all ones.
  Decoded_sparse_measurement = ones (1, M × 1), where M = size of encoded sparse measurements
- Find correlation in HL and LH components of watermarked biometric image.
  1. $Correlation\_Horizontal() = corr2(HL_{1R}, PN\_Sequence\_1);$
  2. $Correlation\_Vertical() = corr2(LH_{1R}, PN\_Sequence\_2);$
  3. $Correlation(Watermarked) = (Corrlation\_Horizontal() + Correlation\_Vertical()) / 2;$
- Compare the correlation with mean correlation for setting value of decoded sparse measurements.
  1. If(correlation(bit) > mean (correlation))
     Decoded_sparse_measurement (bit) = 0;
- After getting decoded value of sparse measurements and compare this decoded sparse measurements with encoded sparse measurements using SSIM [7] for decision about reconstruction of watermark biometric image.
- It comparison result is greater than matching score value and then get actual value of sparse measurements from decoded values using uniform quantization which is used at embedder side.
- After getting decoding value of sparse measurements, then applied cs recovery algorithm on this sparse measurements using correct measurement matrix *A* which is generated at embedder side.
- After application of cs recovery algorithm, extracted sparse coefficients *x'* of watermark biometric image is get at detector side.
- Applied inverse singular value decomposition (SVD) on extracted sparse coefficients, original U and V matrix value to get reconstructed watermark biometric image.

4. EXPERIMENTAL RESULTS

This is described results of proposed watermarking technique. For performance of proposed watermarking technique evaluated using color face image taken from Indian face database [23] and gray scale iris image from CASIA iris database [24] which is shown in figure 3. The size of watermark image is 128 × 128 pixels and host color image is 256 × 256 pixels.

(a) (b)

Figure 3. (a) Original Host Face Image (b) Original Watermark Iris Image

For generation of sparse measurements of iris image, singular value decomposition (SVD) is applied on iris image and get singular (S) matrix value as sparse coefficients *x* with size of 16384 × 1. Measurement matrix *A* with size of 512 × 16384 is generated using random seed. Then generate sparse measurements of iris image using equation 1 with size of 512 × 1 using $y_{512\times1} = A_{512\times16384} \times x_{16384\times1}$. These sparse measurements of iris image are encoded using uniform quantization with 2 bit / level. The bits of encoded sparse measurements of iris image are 1024 (512 × 2) which is used as watermark information is shown in figure 4.

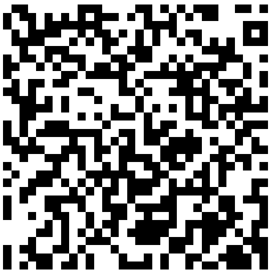

Figure 4. Encoded Sparse Measurements of Iris Image

This encoded sparse measurements as watermark information is embedding into HL and HL wavelet coefficients of red component of host face image to get watermarked color face image. Daubechies wavelet is used to decompose HL and LH coefficients of red component of host face image. The gain factor value is set to 2. The watermarked color image is shown in figure 5 (a) and extracted sparse measurements of iris image are shown in figure 5 (b).

(a) (b)

Figure 5. (a) Watermarked Face Image (b) Extracted Sparse Measurements of Iris Image

SSIM [26] is used for find similarity between extracted sparse measurements and encoded sparse measurements of iris image for decision about modification of data and reconstruction of iris image from sparse measurements based on matching score. The value of matching score is set 0.9. If the similarity score is greater than matching score then biometric data is authenticate and iris image reconstructed from its sparse measurements. For decoding sparse measurements of iris image from extracted sparse measurements used uniform quantization which is used at embedder side and get actual value of sparse measurements of iris image. This actual sparse measurements value is used for reconstruction of watermark iris image. If the similarity score is less than matching score then biometric data is modified by imposter and unauthenticated.

The cs recovery algorithm like orthogonal matching pursuit (OMP) algorithm [27] used for reconstruction of watermark iris image from sparse measurements. The input data for OMP algorithm is measurement matrix A with size of 512 × 16384, sparse measurements with size of 512 × 1 and sparsity level 128 and output of OMP algorithm is extracted sparse coefficients with size of 16384 × 1. Applied inverse SVD on original U, V matrix and extracted sparse coefficients to get reconstructed watermark iris image which is shown in figure 6.

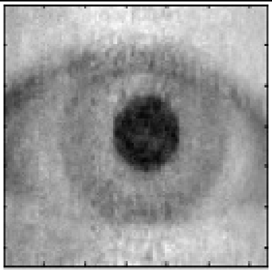

Figure 6. Reconstructed Watermark Iris Image using CS recovery process

PSNR, NCC and BCR are used for performance measurement of proposed technique. The PSNR is used perceptual quality measure between original color image and watermarked color image. The NCC is used to find correlation between original color image and watermarked color image. The NCC value is near to 1 is indicated that watermarking technique is more robust. BCR is used to find bit correct rate between original watermark and extracted watermark. In this paper, PSNR, NCC is calculated between original face image and watermarked image and BCR is calculated between encoded sparse measurements and extracted sparse measurements value.

This proposed watermarking technique is also tested for common watermarking attacks like compression, addition of different noise, and geometric attacks like cropping. The Table 1 summarized the PSNR, NCC value between original color host face image and watermarked color host face image and SSIM, BCR value between encoded sparse measurements and extracted sparse measurements. In watermark embedding procedure, the two PN sequences are multiplied with a gain factor and embedded in wavelet coefficients of color biometric image. Table 2 shows that value of the gain factor does not affect on watermarked image and extracted watermark information.

Table 1. Quality Measures of Proposed Watermarking Technique

Results	**No Attack**	**JPEG Attack**	**Gaussian Noise Attack**	**Salt & Pepper Noise Attack**	**Speckle Attack**	**Cropping Attack**
		Q = 90	**μ=0, σ=0.001**	**Density = 0.005**	**Variance = 0.004**	
NCC	0.96	0.98	0.95	0.95	0.95	0.95
PSNR (dB)	38.17	38.82	37.39	37.17	37.41	37.74
SSIM	0.99	0.99	0.99	0.99	0.99	0.99
BCR	1.00	1.00	1.00	1.00	1.00	1.00

Table 2. Effect of Gain Factor on Proposed Watermarking Technique

Gain Factor	**PSNR (dB)**	**NCC**	**SSIM**	**BCR**
1	39.24	0.98	0.99	1.00
2	38.17	0.96	0.99	1.00
3	37.40	0.94	0.99	1.00
4	36.68	0.91	0.99	1.00
5	36.19	0.89	0.99	1.00
6	35.78	0.86	0.99	1.00
7	35.41	0.84	0.99	1.00
8	35.14	0.82	0.99	1.00
9	34.93	0.81	0.99	1.00
10	34.73	0.79	0.99	1.00

The watermarking technique idea is borrowed from [7 and 25], there are significant modification is taken place in proposed technique compared with Inamdar [7] and Hajjara [25]. The comparison of proposed technique with technique in [7, 25] with different parameters are summarized in table 3. In the proposed work discussed here, single level horizontal and vertical details of red component are used for embedding; while in [7] second level decomposition is obtained from approximation band, while in [25] it is obtained from horizontal details for embedding. In the proposed technique two PN sequence are embedded at a time in single level wavelet coefficients according to encoded sparse measurements of watermark which is generated using CS theory and uniform quantization. In the proposed technique, watermark biometric data is compressed before embedding into host medium. In technique [7], larger size of watermark image is degraded watermarked image quality which is limitation of this technique. Where in the proposed technique, larger size of watermark image is compressed using cs theory framework and embeds into host medium without degrading watermarked image quality.

Table 3. Comparison of Proposed technique with Inamdar technique [7] and Hajjara technique [25]

Parameters	Proposed Technique	Inamdar Technique [7]	Hajjara Technique [25]
Wavelet Decomposition	First level Horizontal & Vertical Details of Red component	Second level of Approximation Details	Second level of Horizontal Details
PSNR Range	34 to 40 dB	30 to 38 dB	3 to 5 dB
No. of PN Sequence	Two PN Sequences are embedded at a time in Horizontal and Vertical Details bands	Three PN Sequences are embedded at a time in all details bands	Only One PN Sequence is embedded in either in bands
Watermark	Encoded Sparse Measurements of Iris Image	Signature Image	Logo
Computational Security Achieved	Due to Compressive Sensing Theory plus Secret Key	Secret Key	Secret Key
Compression of Watermark Data	Due to Compressive Sensing Theory	No such scope	No such scope
Authentication through Template Matching	Feature of Reconstructed iris image extracted and matched	Feature of Recovered Signatures are extracted and matched	No such scope

5. CONCLUSION

This paper proposed a new biometric watermarking technique using wavelets and CS theory. The proposed technique combines the field of biometric watermarking and compressive sensing. The proposed technique is robust against Gaussian, Speckle and Salt & pepper noise, Cropping and JPEG compression. This technique is not robust against histogram equalization and filter attacks. This technique is used to biometric data protection over communication channel between two modules of biometric system.

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: 49 – 79.

[2] A Jain, K Nandakumar and A Nagar. “Biometric Template Security”. *EURASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics*. 2008: 1 – 17.

[3] N Ratha, J Connell and R Bolle. “Enhancing Security and Privacy in Biometric Based Authentication Systems”. *IBM Systems Journal*. 2001; 40(3): 614 – 634.

[4] A Jain and U Uludag. “Hiding Biometric Data”. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2009; 25(11): 1494 – 1498.

[5] 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*. 2004; 14(1): 4 – 20.

[6] A Jain, A Ross and S Pankanti. “Biometrics: A Tool for Information Security”. *IEEE Transactions on Information Forensics and Security*. 2006; 1(2): 125 – 143.

[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*. 2010; 11(1): 19 – 27.

[8] G Langelaar, I Setyawan and R Lagnedijk. “Watermarking of Digital Image and Video Data – A State of Art Review”. *IEEE Signal Processing Magazine*. 2000: 20 – 46.

[9] N Chaudhary, D Singh and D Hussain. “Enhancing Security of Multimodal Biometric Authentication System by Implementing Watermarking Utilizing DWT and DCT”. *IOSR Journal of Computer Engineering*. 2013; 15(1): 6 – 11.

[10] C Li, B Ma, Y Wang and Z Zhang. “Sparse Reconstruction Based Watermarking for Secure Biometric Authentication”. *Biometric Recognition*. 2011; 7908: 244 – 251.

[11] S Edward, S Sumanthi and R Ranihemamalini. “*Person Authentication Using Multimodal Biometrics with Watermarking*”. Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN). 2011: 100 – 104.

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

[13] 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*. 2006; 3(2): 23 – 28.

[14] D Moon, K Tachae, S Jung, Y Chung, K Moon, D Ahn and S Kim. “Performance Evaluation of Watermarking Techniques for Secure Multimodal Biometric Systems”. *In Computational Intelligence and Security*, Springer Berlin Heidelberg. 2005: 635 – 642.

[15] 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*. 2013; 2(2): 56 – 61.

[16] P Reddy, V Prasad and D Rao. “Robust Digital Watermarking of Color Images under Noise Attacks”. *International Journal of Recent Trends in Engineering*. 2009; 1(1): 334 – 338.

[17] Chris Shoemaker. “Hidden Bits: A Survey of Techniques for Digital Watermarking”. *Independent Study EER-290*, Prof Rudko, Spring. 2002.

[18] G Langelaar, I Setyawan and R Lagnedijk. “Watermarking of Digital Image and Video Data – A State of Art Review”. *IEEE Signal Processing Magazine*. 2000: 20-46.

[19] D Donoho. “Compressed Sensing”. *IEEE Trans. Inform. Theory*. 2006; 52(4): 1289-1306.

[20] E Candès. “Compressive Sampling”. Proceedings of the International Congress of Mathematicians, Madrid, Spain. 2006.

[21] E Candès and J Romberg. “L1-Magic: Recovery of Sparse Signals via Convex Programming”. 2005.

[22] I Cox, J Kilian, T Shamoon and F Leighton. “Secure Spread Spectrum Watermarking for Multimedia”. *IEEE Transactions on Image Processing*. 1997; 6(12): 1673 – 1687.

[23] V Jain, A Mukherjee. “The Indian Face Database”. http://vis-www.cs.umass.edu/~vidit/IndiaFaceDatabase. 2002.

[24] For Iris Database: http://www.sinobiometrics.com/caisairis.html

[25] S Hajjara, M Abdallah and A Hudaib. “Digital Image Watermarking Using Localized Biorthogonal Wavelets”. *European Journal of Scientific Research*. 2009; 26(4): 594 – 608.

[26] Z Wang, A Bovik, H Sheikh and E Simoncelli. “Image Quality Assessment from Error Visibility to Structural Similarity”, *IEEE Transaction on Image Processing*, vol. 13, no. 4, April 2004.

[27] J Tropp and A Gilbert, “Signal Recovery from Random Measurements via Orthogonal Matching Pursuit”. *IEEE Transactions on Information Theory*. 2007; 53(12): 4655 – 4666.

BIOGRAPHIES OF AUTHORS

Mr. Rohit M Thanki has received B.E. degree in Electronics and Communication Engineering from Saurashtra University, Rajkot and M.E. in Communication Engineering from Sardar Patel University, Vallabh Vidyanagar. He is currently pursuing his Ph.D. in Electronics and Communication Engineering from C U Shah University, Wadhwan City, Gujarat, India. His area of research is to Design Watermarking Algorithm for Biometric Data Protection. He has guided more than 15 UG students in their project work. He has published 11 research papers in various high impact factor international journals. He has presented 7 research papers in various national and international conferences. He has published books titled Comparative analysis of digital watermarking techniques and Design of Operational Transconductance Amplifier with Lambert Publishing House, Germany. His area of interest is Digital Watermarking, Image & Signal Processing, Compressive Sensing, Pattern Recognition, and Digital VLSI Design.

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, and Ahmedabad in 2008. In 2012, she received her doctoral degree from the Department of Electronics and Communication Engineering, JJT University, Rajasthan. She has teaching experience of over 10 years. 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.