Improved Multimodal Biometric Watermarking in Authentication Systems Based on DCT and Phase Congruency Model

[1] Bairagi Nath Behera ,[2] V.K. Govindan

[1, 2] Department of Computer Science and Engineering
National Institute of Technology, Calicut, Kerala

Abstract

This paper presents multi-modal biometric watermarking techniques for personal identification system based on DCT and Phase Congruency model. The proposal made here is an improved algorithm for embedding biometrics data (such as fingerprint image with demographic information of person) in the face image of the same individual for authentication and recognition which can be employed in E-passport and E-identification cards. Phase congruency model is used to compute embedding locations having the low frequency on DCT coefficients of face image and Normalization correlation based on both human perceptivity and robust property is used for embedding watermark in these locations. This enhances Quality, Recognition accuracy and Robustness of both cover and watermark image with minimum computational complexity. Experimental results demonstrate that the proposed watermark technique is better robust or resilient against different type of image processing attacks.

Keywords: *Authentication, Discrete Cosine Transform, Multimodal Biometrics, Phase Congruency Model.*

1. Introduction

A biometrics is a branch of pattern-recognition that makes use of features derived from physiological or behavioral characteristic of the persons to recognize/identify them[1]. Biometrics-based personal identification techniques are better utilized than traditional knowledge based technology .The weakness of traditional knowledge based techniques such as password which can lost or stolen and authentication certificates which can be lost or misplace. Moreover, biometric data are not replaceable, unique and need not be kept secret[2].Again fingerprint recognition system have better matching performance, which helps to solve the problem based on legitimate proofs of evidence in court by the forensic science[2]. Watermarking is better security than encryption. Because encryption does not provide security once the data is decrypted. However in watermarking techniques, watermark data are integrated with cover image, even after extracting the watermark [3]. Watermarking works as a facilitator for multi-modal biometric verification along with template protection. The main objective of multi modal biometric watermarking techniques are provide security to biometric data without compromising the quality and recognition accuracy or verification accuracy of both biometric cover image and biometric watermark data. Imperceptibility, robustness, capacity, security and low computational complexity are the basic properties needed to achieve an effective watermarking algorithm [4].

The rest of this paper is organized as follows: Section 2 provides a compact review of related work on different types of watermarking algorithms and application scenarios on biometrics. In section 3, we describe an existing algorithm briefly, discuss the issues that are yet to be addressed and then present the proposed work. The Section 4 shows experimental result, and finally, the paper conclusion and future work in Section 5.

2. Related Work

There are various algorithms based on biometric watermarking used in authentication system. Most of them use biometric quantities *viz.* iris, frequency of speech, face images, fingerprints or a combination of these and robustness to survive from different type of common image processing attacks. Some of these approaches are briefly reviewed in the following:

Vatsa et al. [5] presents a novel biometric watermarking technique for embedding face image of user in to his/her fingerprint image by using DWT and Support Vector Machine based learning algorithm. The authors claim that the work enhances quality, improves recognition accuracy and provides security to both face and fingerprint image and also robust to geometric and frequency attacks.

Moon et al. [6] describes performance analysis on watermark technique for secure multimodal biometric system employing both fingerprint and face. A dual watermarking technique using fingerprint as cover image ensures that first one embeds robust watermark and next fragile watermarks without interference between embedded information. The authors reported better results

for user verification accuracy and watermark detection accuracy.

Li et al. [7] proposed a salient region-based authentication watermarking technique for protecting and verifying the integrity of biometric templates. In this technique, three level hierarchical structural authentication schemas are used for tamper detection and localization accuracy. PCA features of biometric images are used for recognition system. The system reconstructs the face to use it as a second source of authenticity. Experimental results show that this technique can detect the tampered region, and recover the biometric features without degrading recognizing quality.

Yeung and Pankanti [8] proposed an invisible fragile watermarking technique for image verification on fingerprint-based personal recognition and authentication system. To improve the security, the original watermark image is first transformed into other mixed image which does not have the meaningful appearance and this mixed image is used for new watermark image. So this algorithm is more secure.

Both Vatsa et al. [9] and Park et al. [10] proposed a technique for embedding iris feature template in to face image for authentication through two level verification. In the first level, verification is based on face image and in the second level the verification is based on extracted iris features from face image. Giannoula and Hatzinakos [11] proposed a newmultimodal biometric system by embedding both voice pattern and iris image into DWT coefficient of fingerprint image based on an energy-classification criterion for automatic recognition system. Advantages of this technique are reduced system data rate, resilient against JPEG2000 compression and guaranteed to accurate data reconstruction for recognition systems.

Bairaginath Behera and V. K. Govindan [12] proposed a biometric watermark algorithm that embeds Mel frequency cepstral coefficient (MFCC) matrix of voice data, fingerprint image and demographic information of person into face image of the same individual by using DCT and RDWT. This algorithm improved the quality, recognition accuracy, embedding capacity and noise free perceptual transparency with low computational complexity.

Picard et al [13] proposed new biometric watermark technique combined with 2-D bar codes and Copy Detection Pattern to verify fraud-proof ID document and prevent a genuine document to be used by an illegitimate user .The main goal of this technique is hide sensitive data of user along with provide self-authentication. For protection against unauthorized use of ID documents, a secrete key and copy-detection pattern are used to detect against duplication and multiple copies of ID document respectively.

M.Paunwala and S.Patnaik [14] proposed a biometric watermarking algorithm for embedding iris and fingerprint templates in low frequency AC coefficients of selected 8×8 DCT blocks of standard test image. Selection of blocks is based on human visual system and neighborhood estimation technique to achieve better perceptual transparency and robustness against various signal processing and channel attacks.

M. Qi et al. [15] proposed a novel biometric data hiding technique based on correlation analysis to protect the integrity of transmitted biometric data for network-based identification. In this method, the biometric data are embedded based on correlation between biometric data with cover image analyzed by partial least squares and particle swarm optimization (PSO) techniques. Experimental results show that this work provides good imperceptibility along with resistance to common image processing attacks and efficient for network-based multimodal biometrics identification.

Y.Cao et al. [16] presents a biometric watermark technique for embedding face image into fingerprint image based on contourlet transform and quantization. Texture complexity based on human visual system selects the best blocks to embed watermarks. This technique provides better robustness to JPEG, Gaussian noise and filtering attacks. Experimental results showed that this technique provides effective security, integrity and recognition rates to both the face and fingerprint images.

Bin Ma et al [17] proposed a new robust watermarking technique for multimodal biometric authentication system by embedding fingerprint minutiae into the block pyramid level of face regions based on first-order statics Quantization index modulation (QIM) technique. In this paper it is described about trade-offs between robustness, capacity and fidelity properties on this watermarking algorithm. Experimental result evaluates the robustness of fingerprint towards JPEG compression with respect to different bit priority block pyramid level.

Noore et al. [18] presents a new digital watermarking technique for embedding face and demographic text image in to fingerprint image. The technique first applies 2-level Discrete Wavelet Transform on fingerprint image to find textual feature region on wavelet sub bands for embedding watermark. Extract the watermark from fingerprint image by using extracted key, which store information about embedded location. This technique enhanced visual imperceptibility and provided integrity to Automatic Fingerprint Identification System by extracting high quality face and text image from fingerprint image. Experimental results show that fingerprint and extracted images are resilient to cropping, compression, filtering, and noise attack.

M.R.M Isa and S. Aljareh et al. [19] presents DCT based watermark technique combine with PCA face recognition algorithm for provide security to biometric image without degrade performance of recognition rate. In this technique, DCT based cox algorithm [4] apply on face image to hide password of that individual for self-authentication. This technique is robust to noise, median cut and JPEG compression attack.

Hoang et al. [20] proposed a remote multimodal biometric framework system based on fragile watermarking by embedding fingerprint minutiae in facial image, over networks to server for self-authentication. In this technique, fingerprint image is embedded on face image based on amplitude modulation and priority level of bits sequence to reduce error rates and bandwidths.

Zebbiche et al. [21] proposed robust fingerprint watermark schema, embedding watermark data into the region of interest of fingerprint image by using segmentation technique. DCT and DWT transform coefficients are modeled by a generalized Gaussian model. This technique ensures resiliency towards filtering, noise, and compression, cropping attacks.

It is evident from the literature that the existing techniques have serious demerits. Some of them suffer from higher complexity, poor quality, poor recognition accuracy of the images and low robustness properties to survive from different type of image processing attacks.

3. Proposed Work

Our present work proposes an improved algorithm for achieving lower complexity, increased quality, verification accuracy and robustness. In this Section, first, we provide a brief description of an important existing algorithm and pin point the deficiency of the algorithm.

Bedi et al. [22] proposed a multimodal biometric watermarking for personal identification systems by using DCT and particle swarm optimization (PSO) technique. This algorithm aims to embed fingerprint and demographic information of user into his/her face image for self- authentication. In the embedding step, first, apply the Discrete Cosine Transform (DCT) on each 8x8 blocks of face image. The four most significant bits of each pixels of fingerprint and some demographic information bits are combined to form watermark (W). Apply Particle Swarm Optimization (PSO) algorithm on each 8x8 blocks of DCT coefficients to finding best embed location for embedding the watermark. The objective function for PSO algorithm is based on the combination of both human perception model and robustness property. The extracted key store the information about embedded location which is help for extracting hidden fingerprint image and demographic information from face image at extracted technique. The performance of the approach is studied using Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) [23] and Normalized Correlation (NC) with respect to different type of image processing attack.

Issues of the Algorithm

The above algorithm has the following limitations:

- High Computational Complexity :-
  Applying PSO algorithm on each block of DCT coefficients to finding best location for embedding watermark has high computational complexity[12][24].
- Reduced Quality and Recognition accuracy :-
  Different type of image processing attacks reduces quality and recognition accuracy of both cover and watermark image.

A. The Proposed Algorithm

The proposed algorithm aims to embed fingerprint image and demographic information of person into face image of that individual. The proposed technique has the following features:

- It is very important that perceptibility of the fingerprint images as well as that of the cover face should not be affected negatively. Hence, fingerprint images are embedded in suitable manner to avoid the aforementioned.
- This technique provides more robustness against common image processing attack without degrade quality and recognition accuracy of both face and fingerprint image.
- Both extracted fingerprint and watermarked face image will provide better quality and recognition accuracy for self-authentication at receiver ‘end.

Proposed Watermark Embedding Technique:-

1. Read the gray scale face image (F).
2. Apply Discrete Cosine Transform on gray scale face image.
3. Apply Phase congruency model on DCT coefficients for finding low frequency coefficients [14, 25, 26].
   X=DCT coefficients.
   ROI_L=region of interest of low frequency coefficients on X.
4. Read the gray scale fingerprint image (I) and extract four MSB’s of each pixel in I and append with demographic information bits to form watermark sequence (W) which is to be embedded in this DCT coefficients of face image .
5. Embed the watermark using on algorithm 1:
   Key: = embed_binary (X, ROI_L, W);

Where Key stores the embedded location which is needed at the time of extracting watermark.

6. Change DCT coefficients by using binary_one, binary_zero methods [22, 27] and Key.
7. Apply Inverse Discrete cosine transform (IDCT) to get watermarked image (WI).

Algorithm:1 The basic algorithm to find embedding location based on sorted Normalization Correlation value is as following:-

Procedure Key: = embed_binary (X, ROI, W)
Input:-
X= DCT Coefficients matrix.
ROI= Low frequency region of Interest.
W=watermark in binary format.
Output:-
Key = embed location of watermark.

1. X=X (:) and ROI=ROI (:); // convert into one dimension.
2. i=1, count=1,j=1,k=1;
3. While (i<=length(X))
4. If (ROI (i) ==low frequency) //check for low frequency coefficient
5. OZ(i)= NC_function (X (i),0);
   //find Normalization correlation for bit 0.
6. OO(i)= NC_function (X (i),1);
7. //find Normalization correlation for bit 1.
8. End If
9. End While
10. L_zero:=calculate number of zero bits in W.
11. L_one:=calculate number of one bits in W.
12. Sort the location ofboth OZ and OO matrix based on ascending order of Normalization Correlation values .
13. Zero_location:=find the first L_zero number of embedded location from OZ matrix.
14. One_location:=find the first L_one number of embedded location from OO matrix.
15. While(count<=length(W))
16. If (W(count)==0)//check for embedding zero bit
17. Key(count)=Zero_location (j);
18. j= j+1;
19. Else
20. Key(count)=One_Location(k);
21. k=k+1;
22. End If
23. count=count+1;
24. End while
25. End Procedure

Algorithm: 2 The NC_function is based on Normalization Correlation as following:
Procedure T: = NC_function (P, bit)
Input: -
P=DCT coefficient
bit = bit value either 0 or 1.
Output: -
T=NC_function value

1. If (bit==0)
2. X= binary_zero (P); //change of coefficient by embedding zero bit
3. Else
4. X= binary_one (P); //change of coefficient by embedding one bit
5. End If
6. Nc =Normalization correlation between P and X.
7. NCF=1-Nc;
8. If (0<=NCF<=0.5)
9. T=NCF;
10. Else
11. T=Infinite;
12. End If
13. End Procedure

Both binary_zero and binary_one methods [22, 27] are used for change in coefficient by embedding bit zero and embedding bit one respectively.

Proposed watermark extracting algorithm:

1. Read the watermarked image (WI).
2. Apply DCT on watermarked image.
   S=DCT coefficients
3. By using Key, extract the fingerprint image using algorithm 3 of paper [12] as following
   W=binary_extract (S, Key);
4. Extract demographic information bit from W.
5. Convert binary value of W into decimal value and resize to original size to get fingerprint image.

4. Experimental Results

We are embedding the fingerprint image {Fig. 1 (e) to (h)} of size 90x90 into gray color face image of512x512 {Fig. 1 (a) to (d)}. We have implemented the proposed watermarking technique in Matlab (R2012a) and compared with an existing multimodal biometric algorithm [22]. The experiments were performed with test fingerprint images from the database FVC 2004 DB1 (Fingerprint Verification Competition, 2004) [28], and test face images from The Indian Face Database [29].The quality and recognition accuracy of the watermarked image are measured by using Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) [23] respectively. The robustness of the watermarked image is represented by Normalized Correlation (NC) [12].

Discussion and Analysis:

In Existing algorithm [22], PSO algorithm is applied on each 8x8 blocks of DCT coefficients for computing best eight locations to be embedding for eight bits of watermark data .But PSO algorithm choose the embedded coefficient randomly and after 100 iteration it gives optimized values according to the optimization function based on both SSIM and NC. The Computational

complexity [24] to find the best DCT coefficient for embedding by using PSO algorithm is 0(m.I.N).

Where m= total number of swarm in PSO algorithm.
I = number of Iteration.
N=total number blocks=(X/u)*(Y/v).
X= length of cover image.
Y= width of cover image.
u= length of block size.
v= width of block size.

Embedding on low frequency region of DCT coefficients are more robust or resilient against different type of common image processing attack [14, 26]. In proposed technique, we are first identifying the low frequency region on DCT coefficient by using Phase congruency model [25]. Normalization correlation value for embedding bit zero and bit one are calculated on these low frequency coefficient regions. The best embedding locations for bit zero and one are computed according to sorted Normalization correlation values for bit zero and one respectively. The proposed algorithm does not divide the face image into 8x8 blocks. The computational complexity for finding best embeds location for embedding watermarking is is0(X.Y).

The proposed watermarking technique ensures better robustness as compared to existing work [22]. Because, in the existing algorithm, as the PSO algorithm is used for computing embed location randomly, the locations computed need not be accurate for low frequency DCT coefficients.

Again the proposed work improved the quality and recognition accuracy when compared to the existing work [22]. This is because in existing technique, each eight bits of watermark areembedded in eight locations of each 8x8 block of DCT coefficients. It does not attempt to find the best eight locations on each 8x8 block. Also, some block may contain best locations and some other block may contain less good locations, depending on the block's characteristics.

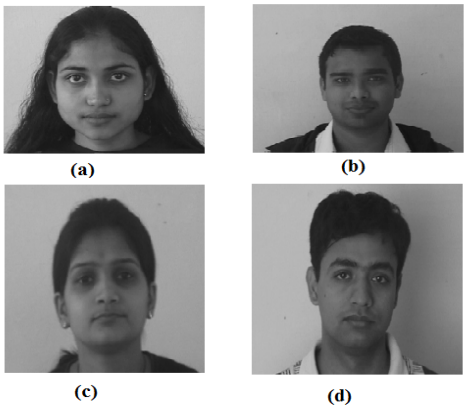

Fig. 1: Host face images (a) F1, (b) F2, (c) F3, (d) F4

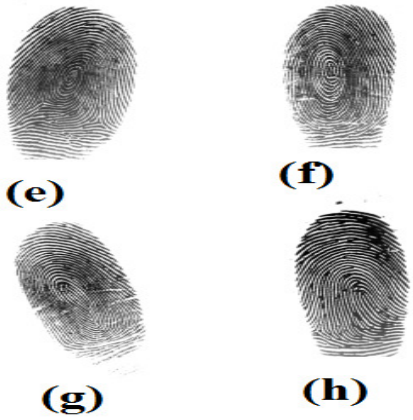

Fig. 2: Watermark fingerprints (e) I1, (f) I2, (g) I3, (h) I4

Table1. Comparison of the values of the quality measures PSNR, SSIM and NC values between cover image and watermarked image obtained in both existing [22] and proposed algorithms, after embedding the fingerprint images I1, I2, I3 and I4 together with demographic data in the corresponding host face images F1, F2, F3 and F4.

Host Image	Quality Metric	Existing Technique (4096 bytes)	Proposed Technique (4096 bytes)
F1	PSNR	43.0537	45.6350
	SSIM	0.9705	0.9813
	NC	0.9991	0.9994
F2	PSNR	43.3997	44.8069
	SSIM	0.9718	0.9755
	NC	0.9993	0.9993
F3	PSNR	44.5288	45.4953
	SSIM	0.9713	0.9822
	NC	0.9990	0.9991
F4	PSNR	43.1293	44.5080
	SSIM	0.9901	0.9754
	NC	0.9989	0.9993

From Table 1it shows that Quality and Recognition accuracy between Original and Watermarked Cover image by using proposed technique is better than existing work [22].

From Table 2 and Table 3 it shows that PSNR, SSIM and NC values between cover and watermarked image and between original and extracted watermark respectively, are better than the existing work [22] with respect to different type of image processing attacks.

Table2. Comparison of the values of PSNR, SSIM and NC between original and watermarked cover image, obtained after embedding the fingerprint (I1) in to the face image F1 by using both existing [22] and proposed watermarking algorithm with respect to different type of image processing attacks.

ATTACK	Watermarked cover face Image (FI)		
	Quality Metric	Existing Technique	Proposed Technique
No Attack	PSNR	43.0537	45.6350
	SSIM	0.9705	0.9813
	NC	0.9991	0.9994
JPEG Comp 90 %	PSNR	42.9932	45.5423
	SSIM	0.9239	0.9742
	NC	0.9933	0.9968
JPEG Comp 80%	PSNR	37.6056	40.8821
	SSIM	0.9011	0.9667
	NC	0.9798	0.9859
JPEG Comp 70%	PSNR	37.0352	40.4315
	SSIM	0.8865	0.9662
	NC	0.9695	0.9728
Sharpen	PSNR	33.9288	43.3571
	SSIM	0.8494	0.9707
	NC	0.9755	0.9987
Sharpen edges	PSNR	40.3916	40.4091
	SSIM	0.9531	0.9626
	NC	0.9858	0.9969
Diffuse glow	PSNR	34.7390	42.9553
	SSIM	0.8672	0.9851
	NC	0.8550	0.9978
Median filter	PSNR	35.5697	44.8426
	SSIM	0.8532	0.9822
	NC	0.9906	0.9998
Blurring Attack	PSNR	39.5122	42.4134
	SSIM	0.9380	0.9841
	NC	0.9495	0.9968
5% salt and Pepper attack	PSNR	28.1324	28.2176
	SSIM	0.8177	0.8366
	NC	0.8192	0.8286
Gamma correction	PSNR	34.6724	40.4091
	SSIM	0.9122	0.9526
	NC	0.7951	0.9969
Scaling attack	PSNR	43.2341	43.9553
	SSIM	0.9586	0.9851
	NC	0.9989	0.9989
Gaussian Attack	PSNR	33.9628	38.8426
	SSIM	0.8181	0.8822
	NC	0.7533	0.9698

5. Conclusion and Future Work

A study on different techniques of watermarking concludes that digital watermarking is not as secure as data encryption, because watermark can be destroyed by various attacks like removal attacks, geometrical attacks, cryptographic attacks and protocol attacks[30]. Different watermarking algorithms are employed for different approaches and prescribes the different trade-offs between various properties such as robustness, tamper resistance, fidelity, and false positive rates[12]. In general robust watermark are made by embedding watermark ontransform domain coefficients of cover image. Some watermarking technique uses extracted key for extract or detect watermark from cover image, such techniques are needed to keep privacyon the keys.

Table3. Comparison of the values of PSNR, SSIM and NC between original and extracted watermark image, obtained after extracting the fingerprint (I1) from the watermarked face image F1 by using both existing [22] and proposed watermarking algorithm with respect to different type of image processing attacks.

ATTACK	Watermark Fingerprint Image (I1)		
	Quality Metric	Existing Technique	Proposed Technique
No Attack	PSNR	Infinite	Infinite
	SSIM	1	1
	NC	1	1
JPEG Comp 90 %	PSNR	29.9982	30.5131
	SSIM	0.8122	0.8783
	NC	0.9912	0.9965
JPEG Comp 80%	PSNR	28.4311	29.1382
	SSIM	0.5081	0.5921
	NC	0.9621	0.9836
JPEG Comp 70%	PSNR	23.7723	24.2541
	SSIM	0.3998	0.4365
	NC	0.9597	0.9630
Sharpen	PSNR	29.8648	30.7645
	SSIM	0.7186	0.7926
	NC	0.9831	0.9954
Sharpen edges	PSNR	25.9852	26.8658
	SSIM	0.4312	0.5290
	NC	0.9811	0.9883
Diffuse glow	PSNR	21.0853	22.2128
	SSIM	0.2302	0.3521
	NC	0.7721	0.9170
Median filter	PSNR	20.8831	22.2448
	SSIM	0.2009	0.2611
	NC	0.7921	0.8952
Blurring Attack	PSNR	18.9976	19.5457
	SSIM	0.1994	0.2043
	NC	0.8381	0.8598
5% salt and Pepper attack	PSNR	15.0721	15.4654
	SSIM	0.0941	0.1234
	NC	0.7196	0.7429
Gamma correction	PSNR	17.9864	18.8265
	SSIM	0.3491	0.4374
	NC	0.8734	0.9120
Scaling attack	PSNR	15.0987	15.3407
	SSIM	0.2967	0.3183
	NC	0.9281	0.9382
Gaussian Attack	PSNR	18.0964	18.9795
	SSIM	0.2991	0.3265
	NC	0.8759	0.9230

A new technique to embed demographic data and fingerprint information with the image of his face is proposed. This is achieved without affecting the perceptibility of the original face and fingerprint image. The proposed technique has shown significant improvement on quality, complexity, accuracy of recognition. It also provided better robustness properties that helps survive from various image processing attacks.As a future work, we are planning to improve the security of the proposed watermarking algorithm by enhancing blinding nature with cryptography concepts.

References

[1] Mingxing, S. Horng, P. Fan, R. Run, R.Chen, J. Lai, M.K. Khan, and K.O. Sentosa. "Performance evaluation of score level fusion in multimodal biometric systems." Pattern Recognition 43, no. 5 (2010): 1789-1800.

[2] W.Kim and H.Lee. "Multimodal biometric image watermarking using two stage integrity verification". Signal Process., 89(12):2385–2399, December 2009.

[3] A.K. Jain, U.Uludag, and R.L Hsu. "Hiding a face in a fingerprint image". In Pattern Recognition, 2002. Proceedings. 16th International Conference on, vol. 3, pp. 756-759. IEEE, 2002.

[4] Cox, Ingemar J.; Kilian, Joe; Leighton, F.T.; Shamoon, T., "Secure spread spectrum watermarking for multimedia," Image Processing, IEEE Transactions on, vol.6, no.12, pp.1673,1687, Dec 1997 doi: 10.1109/83.650120 .

[5] Vatsa, Mayank, Richa Singh, and Afzel Noore. "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking." IEICE Electron. Express 2, no. 12 (2005): 362-367.

[6] Moon, Daesung, Taehae Kim, SeungHwan Jung, Yongwha Chung, Kiyoung Moon, Dosung Ahn, and Sang-Kyoon Kim. "Performance evaluation of watermarking techniques for secure multimodal biometric systems." In Computational Intelligence and Security, pp. 635-642. Springer Berlin Heidelberg, 2005.

[7] Li, ChunLei, Bin Ma, Yunhong Wang, and Zhaoxiang Zhang. "Protecting biometric templates using authentication watermarking." In Advances in Multimedia Information Processing-PCM 2010, pp. 709-718. Springer Berlin Heidelberg, 2010.

[8] Pankanti, Sharath and Minerva M. Yeung. "Verification watermarks on fingerprint recognition and retrieval." In Electronic Imaging'99, pp. 66-78. International Society for Optics and Photonics, 1999.

[9] M.Vatsa, R.Singh,P.Mitra, and A.Noore."Digital watermarking based secure multimodal biometric system". In Systems, Man and Cybernetics, 2004 IEEE International Conference on, vol. 3, pp. 2983-2987. IEEE, 2004.

[10] K.R Park, D.S.Jeong, B. J.Kang, and E.C.Lee "A study on iris feature watermarking on face data." In Adaptive and Natural Computing Algorithms, pp. 415-423. Springer Berlin Heidelberg, 2007.

[11] A.Giannoula, and D. Hatzinakos. "Data hiding for multimodal biometric recognition." In Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on, vol. 2, pp. II-165. IEEE, 2004.

[12] Bairaginath Behera and V.K.Govindan "Image Watermarking in biometric data recognition systems based on dct and rdwt", International Conference on Electrical Engineering and Computer Science, April-2013, Coimbatore, ISBN: 978-93-83060-02-3, page no-54-60.

[13] J.Picard, C.Vielhauer, and N.Thorwirth. "Towards fraud-proof ID documents using multiple data hiding technologies and biometrics." In Proceedings of SPIE, vol. 5306, pp. 416-427. 2004.

[14] M.Paunwala and S.Patnaik. "DCT Watermarking Approach for Security Enhancement of Multimodal System." ISRN Signal Processing 2012 (2012).

[15] Qi, Miao, Yinghua Lu, Ning Du, Yinan Zhang, Chengxi Wang, and Jun Kong. "A novel image hiding approach based on correlation analysis for secure multimodal biometrics." Journal of Network and Computer Applications 33, no. 3 (2010): 247-257.

[16] Cao, Yuqiang, Weiguo Gong, Mingwu Cao, and Sen Bai. "Robust biometric watermarking based on Contourlet transform for fingerprint and face protection." In Intelligent Signal Processing and Communication Systems (ISPACS), 2010 International Symposium on, pp. 1-4. IEEE, 2010.

[17] Ma, Bin, Chunlei Li, Yunhong Wang, Zhaoxiang Zhang, and Yiding Wang. "Block pyramid based adaptive quantization watermarking for multimodal biometric authentication." In Pattern Recognition (ICPR), 2010 20th International Conference on, pp. 1277-1280. IEEE, 2010.

[18] Noore, Afzel, Richa Singh, Mayank Vatsa, and Max M. Houck. "Enhancing security of fingerprints through contextual biometric watermarking." Forensic Science International 169, no. 2 (2007): 188-194.

[19] Isa, Mohd Rizal Mohd, and Salem Aljareh. "Biometric image protection based on discrete cosine transform watermarking technique." In Engineering and Technology (ICET), 2012 International Conference on, pp. 1-5. IEEE, 2012.

[20] Hoang, Tuan, Dat Tran, and Dharmendra Sharma. "Remote multimodal biometric authentication using bit priority-based fragile watermarking." In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, pp. 1-4. IEEE, 2008.

[21] Zebbiche, K., F. Khelifi, and A. Bouridane. "An efficient watermarking technique for the protection of fingerprint images." EURASIP journal on information security 2008 (2008): 4.

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

[23] P.Bedi , R.Bansal, and P.Sehgal. "Using PSO in image hiding scheme based on LSB substitution". In Advances in Computing and Communications, pages. 259-268. Springer Berlin Heidelberg, 2011.

[24] H.J.Escalante, M.Montes, and L.E.Sucar. "Particle swarm model selection." The Journal of Machine Learning Research 10 (2009): 405-440.

[25] P.Kovesi, "Image features from phase congruency", Videre: A Journal of Computer Vision Research, MIT Press, Vol. 1, No. 3, page. 1-26, 1999.

[26] M.Vatsa, R.Singh, and A.Noore. "Feature based rdwt watermarking for multimodal biometric system". Image Vision Comput.,27(3):293–304, February 2009.

[27] Lin, Shinfeng D., Shih-Chieh Shie, and J. Y. Guo. "Improving the robustness of DCT-based image watermarking against JPEG compression." Computer Standards & Interfaces 32.1 (2010): 54-60.

[28] Fingerprint Verification Competition 2004 .http://biometrics.cse.msu.edu/fvc04db/.

[29] V.Jain, A.Mukherjee. The Indian FaceDatabase. http://viswww.cs.umass.edu/~vidit/IndianFaceDatabase/.

[30] Sirvan, Khalighi, Tirdad Parisa, and Rabiee Hamid R. "A contourlet-based image watermarking scheme with high resistance to removal and geometrical attacks." EURASIP Journal on Advances in Signal Processing 2010 (2010).