ISSN: 0974-5572
IJCTA
International Journal of
CONTROL THEORY
AND APPLICATIONS
UGC APPROVED JOURNAL
ज्ञान-विज्ञान विमुक्तये
INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 31 • 2017

Secure Multimodal Biometric Authentication System - A Case Study and Analysis

R. Parimala[a] and C. Jayakumar[b]

[a]Research Scholar, Dept. of Computer Science, Bharathiar University, Coimbatore, India
E-mail: parimalasuresh80@gmail.com
[b]Professor, Dept. of CSE, Sri Venkateswara College of Engineering, sriperumbudur, India
E-mail: cjayakumar2007@gmail.com

Abstract : In an era of information technology, mobile phones are more and more widely usedworldwide, not only for basic communications, but also as a tool to deal with personalaffairs and process information acquired anywhere at any time. And it is time for moneyless transaction which leads to the increase in the enormous number of users. Hence security should also build in such a way to overcome the speed of users. Hence this multimodal system is adopted for banking purposes. It may be used in customer care section, telebanking, authentication for OTP generation and many. The security of the entire system is strengthened using the multimodal biometric systems which are assumed to be unique for every individual. The biometric traits involved are Fingerprint, Ear and Voice biometric.

Keywords: *Ear, Voice, Fingerprint, Cashless Banking, Authentication, multimodal biometric.*

1. INTRODUCTION

Technology brings a new dimension to biometrics in this information society era, and in turn biometrics brings a new dimension to individual identity authentication and verification. Biometrics and cryptography are two potentially complementary security technologies. Using biometrics for security purposes becomes popular, but using biometrics by means of cryptography is still a hot research topic. Many traditional cryptographic algorithms are available for securing information, but all of them are dependent on the secrecy of the private key. To overcome this dependency biometric may be used. There have been a number of attempts to bridge the gap between the fuzziness of biometrics and the exactitude of cryptography, by deriving biometric keys from biometric entities. This contribution tackles the interaction between cryptography based on Ear, Speech and Traditional finger print biometrics.

The primary aim of this paper is to perform scientific research in the imaging and security fields to enhance quality of biometric authentication methods. The objectives of this research can be summarized as follows:

1. To develop a new key generation method to enhance security, in order to overcome the drawbacks of traditional authentication techniques that use PIN or passwords.

2. To facilitate the development of methods for utilizing unique features of finger print in cryptographic key development infrastructure.
3. To incorporate the key generated from the authenticated fingerprint features along with Ear and Voice Recognition system, for enhanced security using encryption technique.
4. To analyse the efficiency and security of developed system involving the biometric cryptosystem.
5. To exploit the claimed merging of biometric and cryptography for integrated usage, and contribution addition in the field of Bio-crypt and Biosecurity.

2. RELATED WORKS

Chen et.al.,[1] in their research utilized a fingerprint sensor for acquisition of fingerprint images and implements an algorithm on internal hardware to perform verification of users. Experiment results show that this implementation has a relatively good performance.

The speech features encompass high-level and low level parts. While the high-level features are related to dialect, speaker style and emotion state that are not always adopted due to difficulty of extraction, the low-level features are related to spectrum, which are easy to be extracted and are always applied to ASR[2]. In a research concentrating on optimizing vector quantization (VQ) based speaker identification, the number of test vectors are reduced by pre-quantizing the test sequence prior to matching, and the number of speakers are reduced by pruning out unlikely speakers during the identification process [6].The best variants are then generalized to Gaussian Mixture Model (GMM) based modeling. The results of this method show a speed-up factor of 16:1 in the case of VQ-based modelling with minor degradation in the identification accuracy, and 34:1 in the case of GMM-based modeling. Jain et.al., [11] has proposed a multimodal biometric system which integrates face, fingerprint and speaker verification. The earlier work in Soutar [8] suggested a cryptographic key being extracted directly from a biometric template where a randomly chosen key can be connected with the biometric. A combined framework for DWT and LSB based biometric watermarking algorithm is proposed. In a series of work by Uludag et al. [3][9]introduced several methods for combining data hiding with Biometrics. In [3], Jain et al. introduced two applications of an amplitude modulation based watermarking method which hides a user’s biometric data in a variety of images. Hao et al. proposed a fuzzy commitment scheme in [2] . A biometric template is supposed to be in the form of an ordered bit string, which is XOR-ed with a same length code word of an error correcting code. This code word then generates a cryptographic key. The flaw in this system, is the chance for key prediction. Vatsa et al. [10] presented a novel biometric watermarking algorithm for improving the recognition accuracy and protecting the face and fingerprint images from tampering. Multi-resolution DWT (Discrete Wavelet Transform) is used for embedding the face image in a fingerprint image. Zebbiche et al. [4]and Jain et al.[3] proposed methods using watermarking to protect fingerprint data. They introduced an application of wavelet-based watermarking method to hide the fingerprint minutiae data in fingerprint images. Vatsa et al. [10] suggested to generate a biometric signature directly from a biometric template using some standard cryptographic algorithms. However, the biometric template must have all the bits exactly correct, which is unrealistic for all the biometric except DNA pattern.

3. DESIGN OF THE PROPOSED SCHEME

Before proceeding with the discussions on the proposed scheme, the main aspects involved in the proposed algorithm are discussed.

1. Introducing three biometric traits is of much advantage in which two of the entities are chosen to be embedded and the left over entity is used in the key generation process used to embed the two former traits. The key generated has been used in embedding the data.

2. As a concept of image processing three main attitudes are involved. Discrete Wavelet Transformation, Discrete Cosine Transformation and Image Scrambling. DWT produces multi-scale image decomposition. It produces the result in the form of the decomposed image, very effectively revealing data redundancy in several scales. In DCT the image is divided into segments. Each segment is then a subject of the transform, creating a series of frequency components that correspond with detail levels of the image. The proposed method considers 5-level DWT. Any compression level may compress data to some extent but the motive of the work is to minimize the space occupied by the image in the server space such optimal compression is needed. The overall design of the proposed scheme may be divided into four modules which in turn fall into the two phases of the biometric authentication system as follows:

    a) Enrolment Phase

    - Image acquisition and processing
    - Data embedding

    b) Verification Phase

    - Data extraction
    - Check module

3.1. Enrolment Phase

Enrolment phase of any biometric system is a step to store data or its template into the corresponding database.

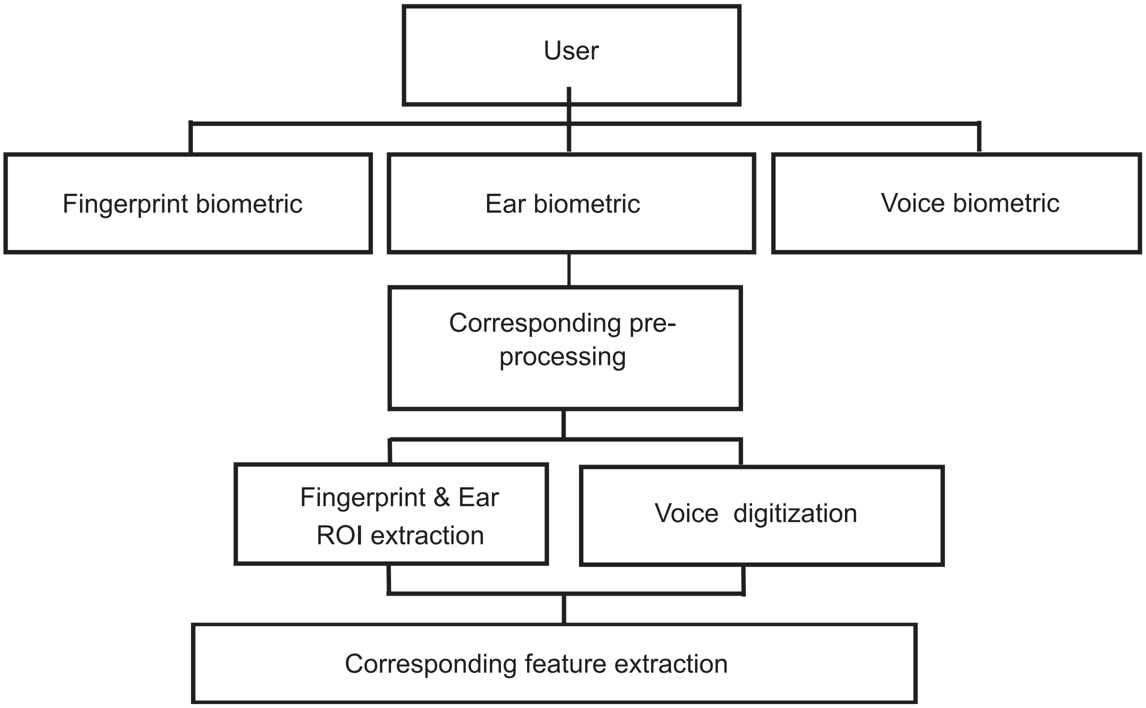
User
Fingerprint biometric
Ear biometric
Voice biometric
Corresponding pre-processing
Fingerprint & Ear ROI extraction
Voice digitization
Corresponding feature extraction

Figure 1: (*a*) Enrollment Phase

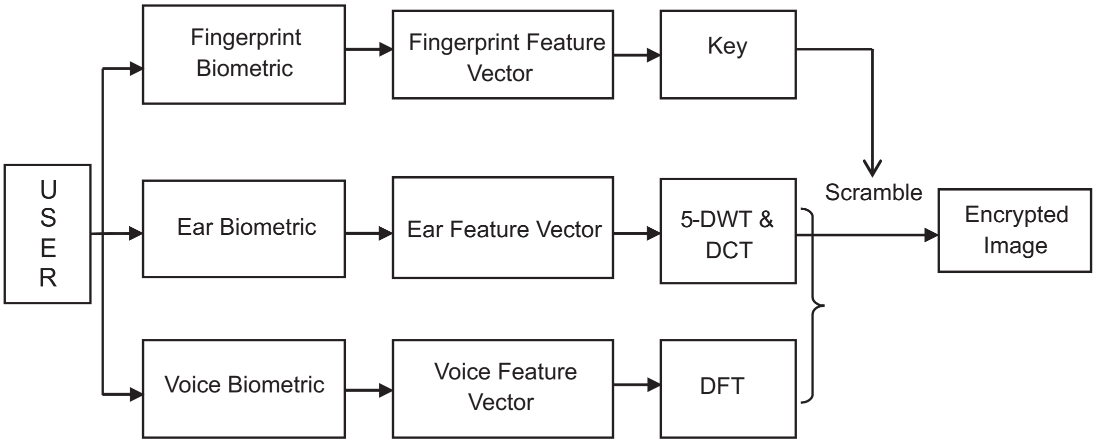

Figure 1: (*b*) Enrolment Phase- Detailed structure

3.1.1. Image Acquisition and Processing

Image acquisition and processing module invokes capturing of raw biometric images of fingerprint, Ear and Speech, which are then processed to extract the Region of Interest and are consecutively passed into the Enhanced Raymond Thai's [7] fingerprint feature extraction algorithm and the extracted features are saved as template in the fingerprint database in .dat format. Similarly the raw ear image is processed and passed into the proposed feature extraction algorithm to extract its features and save its template. The stored fingerprint template is given as input to the proposed fingerprint key generation algorithm to generate a binary key. Feature extraction in ear image involves GLCM.

3.1.2. Data Embedding

The watermark embedding procedure involves with it an encrypted fingerprint, the key generated from it and an embedding procedure that also performs image compression using frequency domain transforms like DWT and DCT. The fingerprint is encrypted using Arnold scrambling process which is executed key number of times.

3.2. Verification Module

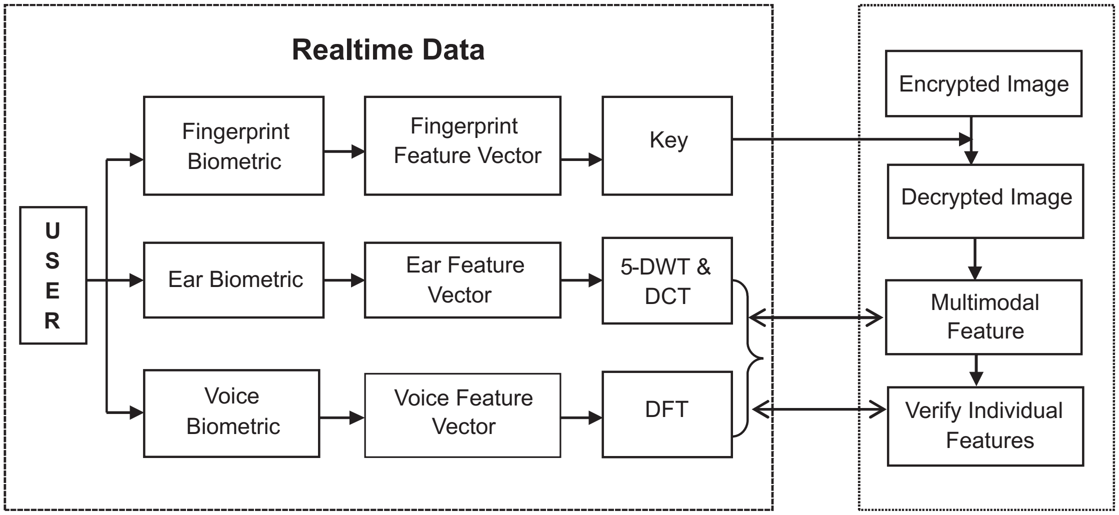

Figure 2: Verification Phase

Verification is a 1:1 process. The data to be verified is checked against its corresponding data entered in the database during enrollment. Identification is a 1: N process. A single data to be verified or authenticated is checked for a match among the n available data stored in the database. The verification phase is carried as in figure 2.

3.2.1. Data extraction

The extraction procedure proposed involves the retrieval of Ear features and Speech features based on the key generated from the fingerprint image. The transformed face image obtained undergoes inverse transform of the 1- level DCT and 5 –level DWT to obtain the original Ear image which will be utilized in the checking process. On the other hand, the fingerprint obtained undergoes the unscrambling process to generate the decrypted fingerprint template.

3.2.2. Check module

Checking process involves checks at three stages. If the system identifies failure at even one stage the entire authentication scheme assumes the person to be fraudulent or unauthorized. The checks performed are:

1. Comparison of the key generated from the live scan image of the fingerprint and the one stored in the database at the time of enrollment.

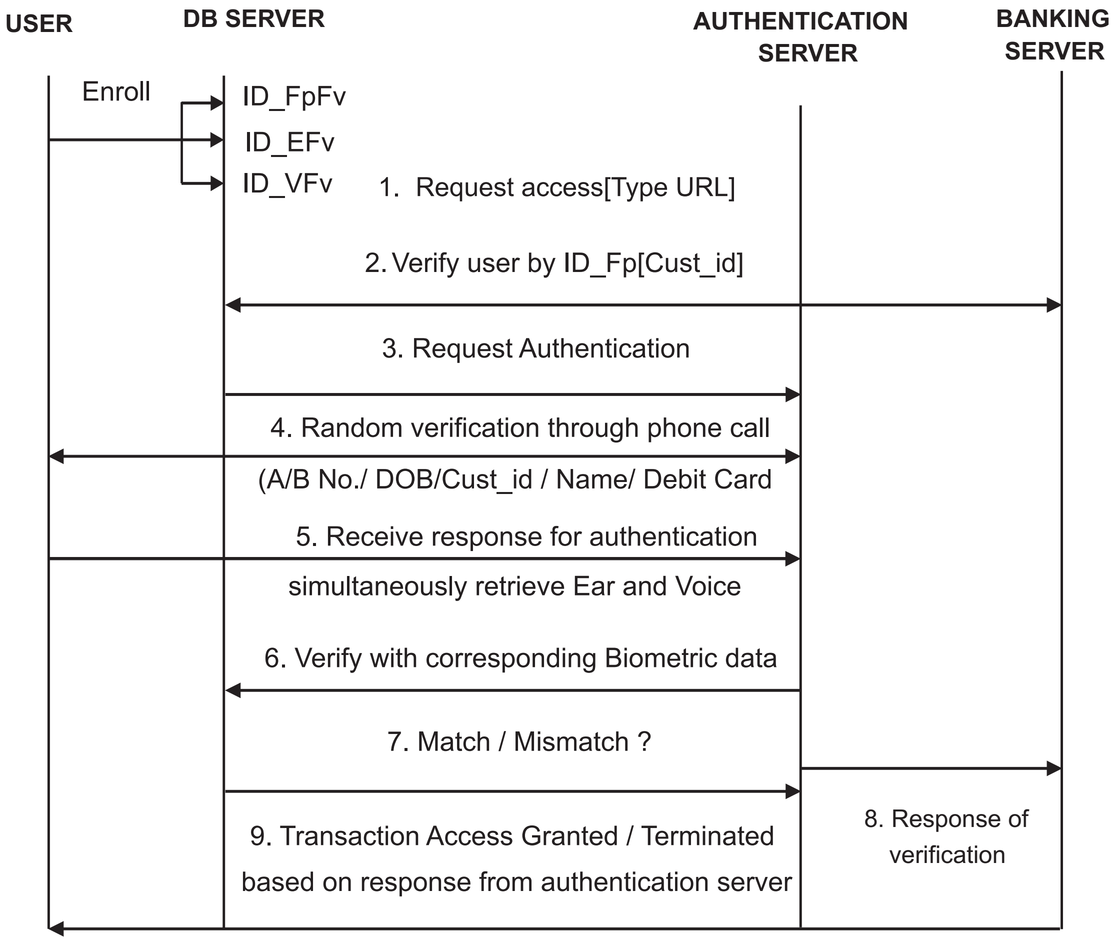
USER
DB SERVER
AUTHENTICATION SERVER
BANKING SERVER
Enroll
ID_FpFv
ID_EFv
ID_VFv
1. Request access[Type URL]
2. Verify user by ID_Fp[Cust_id]
3. Request Authentication
4. Random verification through phone call
(A/B No./ DOB/Cust_id / Name/ Debit Card
5. Receive response for authentication
simultaneously retrieve Ear and Voice
6. Verify with corresponding Biometric data
7. Match / Mismatch ?
8. Response of verification
9. Transaction Access Granted / Terminated
based on response from authentication server

Figure 3: Banking System- Case study

2. Verification of Ear image extracted against the Ear template stored in the database during enrollment.
3. After performing the unscrambling process the fingerprint template obtained is compared with the one stored in the database. So that the data retrieval process proceeds to verify the speech data taken in live to be compared with that of the stored template. If all traits of the person matches, he/she is authenticated else rejected.

A case study as with the Bank sector transactions are also discussed. The overall architecture for the case study is provided in figure 3.

4. CONTRIBUTIONS

Original contributions resulting from the proposed and published research work could be grouped as following proposed algorithms: Fingerprint Feature Extraction Algorithm [12] follows the general methodology as other existing feature extraction algorithm with some steps advanced to that of Raymond Thai[7],but has proven to show high accuracy with faster performance. Ear Feature Extraction Algorithm is found to perform better with high results when compared to that of existing feature extraction algorithm that exists with other biometric traits. The proposed algorithm was tested on the database available online. Fingerprint Key Generation Algorithm has been proposed for the key generation from the extracted Fingerprint features. This generation is based on thresholding. Combined Frequency Domain Transformation involves the compression of the captured Ear image enabling storage in space specified token. Hence transformation is applied to the enrolled Ear image. This transformation involves Discrete Cosine Transform (1-DCT) and Discrete Wavelet Transform (5-DWT). The variation in the levels has been shown to enable compression with better Peak Signal to Noise Ratio (PSNR) and Mean Average Error (MAE) values. Also Data embedding and extraction procedure are followed. Embedding procedure and the extraction procedure are carried out as shown in figure 1 and figure 2 of the design phase.

5. PERFORMANCE EVALUATION

The performance of the automated combined ear, speech and fingerprint biometric system is evaluated at various levels. The Experimental results obtained on self-created Ear biometric to take all possible factors into consideration like scaling, illumination, different camera view point for ear biometrics. Some samples of self- created database is also stored. Fingerprint biometric data taken from FVC 2002 and speech biometric data tested on the self-created database in which 10 samples for a user is trained and about 150 user data is stored. Self- acquired database is acquired in an indoor environment such that less noise factors are available during image acquisition and speech recording. Ear Database is collected over 150 right and left ear images of ±10◦angle variation and speech data were taken from 150 subjects (10 samples per person) at approximately.

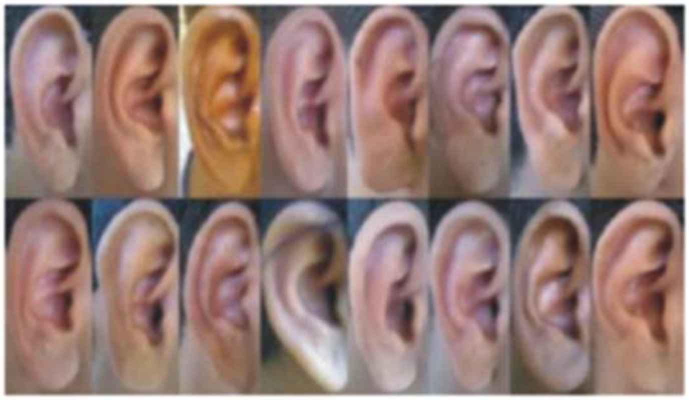

Figure 4: Sample Ear images from created database

Ear samples from the created databases are shown in Figure 4. Ear images and speech data were taken from students using smartphone Nokia XL having 5MP camera. 'Euclidian distance' and 'Bhattacharya distance' were applied to calculate efficiency in a faster manner. Table 2 and 3 gives the recognition rates (in %). In these experiments, in every trial, the template set consists of three random images from each subject and the remaining images serve as the testing set. One individual testing set was compared with one template set from 30 persons with 3 template images each. Then, one test image is compared against all 85 template images using a classifier. The result per trial is the closest matching image in template. Using Euclidean distance 81.31% and using Bhattacharya distance, 80.61% accuracy was obtained as mentioned in Table 1.

Table 1
Matching Score using Euclidean distance & Bhattacharya distance

Trial	*Measure*	*Ear Biometric*	*Speech Biometric*	*Fingerprint Biometric*	*Multimodal Biometric*
T1	ED	77.89	83.07	88.92	82.47
	BD	73.89	78.97	91.73	80.71
T2	ED	82.63	67.12	98.58	81.96
	BD	73.83	89.48	94.31	85.05
T3	ED	70.25	94.16	88.75	83.57
	BD	88.93	73.59	76.38	78.81
T4	ED	82.58	87.49	77.26	81.62
	BD	72.57	73.92	89.98	78.00
T5	ED	74.26	82.58	89.88	81.42
	BD	82.29	68.13	73.48	73.81
T6	ED	88.97	78.88	81.59	82.33
	BD	75.05	88.91	85.17	82.22
T7	ED	88.78	82.57	79.58	82.82
	BD	78.39	79.87	87.59	81.13
T8	ED	78.99	79.58	82.56	79.56
	BD	72.95	78.25	88.25	79.00
T9	ED	81.72	85.68	68.97	77.97
	BD	78.95	77.58	89.55	81.21
T10	ED	71.58	80.98	87.99	79.36
	BD	87.28	78.25	95.28	86.12

ED- EUCLIDEAN DISTANCE

BD-BHATTACHARYA DISTANCE

In order to test our proposed schemes for monomodal and multimodal biometric recognition systems and proceed with their evaluation and comparison the following case scenarios are considered as in figure 5.

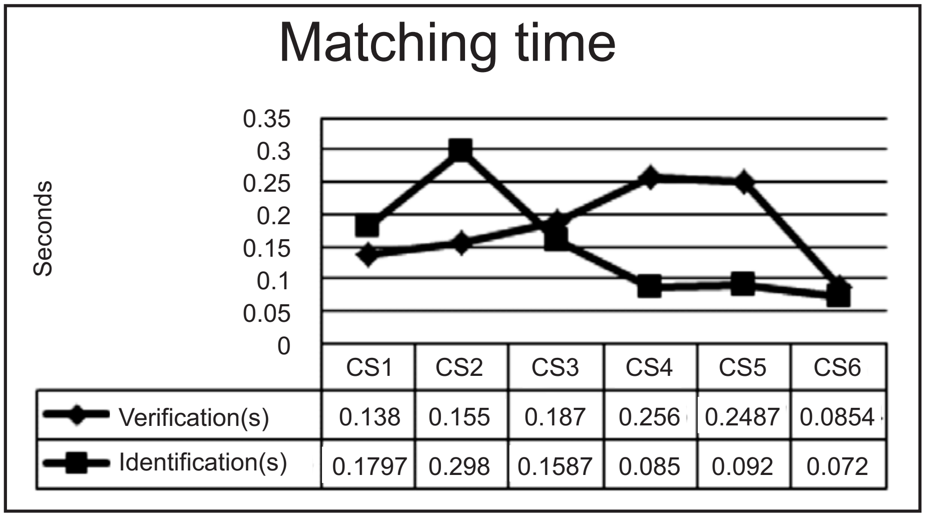

Figure 5: Matching time for case scenarios in seconds

Case Scenario 1: Both verification and identification processes are implemented with a monomodal Ear Biometric recognition system.

Case Scenario 2: Both verification and identification processes are implemented with a monomodal Fingerprint recognition system.

Case Scenario 3: Both verification and identification processes are implemented within a monomodal Speech recognition system.

Case Scenario 4: Both verification and identification processes is implemented within a multimodal biometric recognition system of combined Ear, Fingerprint and Speech recognition Biometric using the sum rule based matching.

Case Scenario 5: Both verification and identification processes is implemented within a multimodal biometric recognition system of combined Ear, Fingerprint and Speech recognition Biometric using the weighted sum rule based matching.

Case Scenario 6: Both verification and identification processes is implemented within a multimodal biometric recognition system of combined Ear, Fingerprint and Speech recognition Biometric using our proposed matching system.

Table 2
Best FAR, FRR of Ear and speech Biometrics

Threshold	*Ear*		*Speech*	
	FAR	*FRR*	*FAR*	*FRR*
0.2	0	99.054	0	99.94
0.25	0	83.745	0	95.82
0.3	0	37.882	0	57.78
0.35	0	5.181	0	20.49
0.4	0.005	0.238	0.01	9.82
0.45	7.599	0	0.098	4.07
0.5	99.499	0	99.499	0

Table 3
Best FAR, FRR of fingerprint Biometrics

Threshold	*Fingerprint*	
	FAR	*FRR*
10	0.000	99.000
20	0.005	95.800
30	0.100	70.290
40	0.600	56.780
50	10.000	30.890
60	13.430	28.780
70	13.950	26.770
80	14.010	15.980
90	67.870	50.760
100	90.890	12.670

6. CONCLUSION

Among the *n* number of biometric entities, fingerprint and Ear were chosen, since they could be of common use in identification or Authentication. Also, in order to enhance this security, another biometric entity, the Speech biometric is chosen. The key generated from fingerprint is used to embed Speech biometric with that of Ear image. The watermarking scheme with high resistance to attacks has been developed and implemented.

REFERENCES

[1] Chen, X.; Tian, J.; Su, Q.; Yang, X. & Wang, F. (2005). A Secured Mobile Phone Based on Embedded Fingerprint Recognition Systems. In: Intelligence and Security Informatics, Kantor, P. et al., (Eds.), pp. 549-553, Springer Berlin / Heidelberg, Retrieved from http://dx.doi.org/10.1007/11427995_57

[2] Hao,F.,Anderson,R. and Daugman,J., "Combining crypto with biometrics effectively", IEEE Transactions on Computers,Vol. 55,No.9, 2005.

[3] Jain,A.K., Uludag.,U. and Hsu,.R.K., " Hiding a face in a fingerprint image", Proceedings of International Conference on Pattern Recognition, Vol.3, pp.756–759, 2002.

[4] Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi and Ahmed Bouridane, " Protecting fingerprint data using watermarking", First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06), pages 451–456, 2006.

[5] Chen, W. & Huang, J. (2009). Speaker Recognition using Spectral Dimension Features. Proceedings of 2009 4th International Multi-Conference on Computing in the Global Information Technology, pp. 132-137, ISBN 978-0-7695-3751-1, Cannes, La Bocca, France, August 23-29, 2009

[6] Kinnunen, T.; Karpov, E. & Fränti, P. (2006). Real-Time Speaker Identification and Verification. IEEE Transactions on Audio, Speech, and Language Processing, Vol. 14, No. 1, (January 2006), pp. 277-288, ISSN 1558-7916

[7] Raymond Thai, "Fingerprint Image Enhancement and Minutiae Extraction", Thesis submitted to School of Computer Science and Software Engineering, University of Western Australia, 2003.

[8] Soutar,C. and Roberge,D., "Biometric encryption" , ICSA Guide to Cryptography, McGraw- Hill, 1999.

[9] Uludag,U. and Pankanti,S., "Biometric Cryptosystems: Issues And Challenges" , Proceedings of the IEEE, Vol.92, No.6, pp.948-960, 2004.

[10] Vatsa,M.,Richa Singh,Noore,Houck,M. and Keith, " Robust biometric image watermarking for fingerprint and face template protection" , IEICE Electronics Express, Vol.3,No.2, pp.22-26,2006.

[11] Jain, A.; Pankanti, S.; Prabhakar, S.; Hong, L. & Ross, A. (2004). Biometrics: A Grand Challenge. Proceedings of 2004 17th International Conference on Pattern Recognition, pp. 935-942, ISBN 0-7695-2128-2, East Lansing, Michigan, USA, August 23-26, 2004

[12] Prasanalakshmi,B., Gomathi,B. And Deepa,K., "Biometric Cryptosystem Involving Two Traits and Palm Vein as Key" Procedia Engineering,Vol.30,pp.303-310,ISSN 1877-7058, 10.1016/j.proeng.2012.01.865, March 2012.