Grenze International Journal of Engineering and Technology, Jan Issue

An Efficient Multi Biometric Crypto-Key Generation

Bhagya B.P[1], Sangam Kumar G.H[2] and Lalitha Y.S[3]
[1,3]Don Bosco Institute of Technology/ ECE Department, Bangalore, India
Email: bhagya2k@gmail.com, pati.lalitha12@gmail.com
[2]PESU, ECE Department, Bangalore, India
Email: hgsangam@pes.edu

***Abstract*— Biometrics refers to the technology for personal recognition or authentication based on our physiological and/or behavioural characteristics. Distinctiveness, Permanence, Collectability, Performance, Acceptability, and Circumvention are the properties of biometric Using only one biometric trait in Authentication systems may not provide all the properties mentioned above. We use more than one biometric trait (similar / different) simultaneously which is called as multi biometric, provides more robust. There are a number of other sources that can be combined to enhance security in the case of combining different biometric modalities. In this paper shows the basic biocrypto system technique used in most of the research. This shows the cryptosystem which stores a key and will be released once the verification is done. Cryptography methods is combined with multibiometric which enhances the security of privacy data.**

***Index Terms*— Key Generation,Cryptography , Biometric, Feature Extract**

I. INTRODUCTION

Biometrics refers to the technology for personal recognition or authentication based on our physiological and/or behavioral characteristics. Physiological Characteristics: face, Fingerprint, Hand geometry, Iris, Retina, Palm print, Facial Thermogram, Ear, Hand vein. Behavioral Characteristics: Voice, Signature, Gait, Keystroke. Biochemical Characteristics: DNA, Odour. Universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention are the properties of biometric. Using only one biometric trait in Authentication systems may not provide all the properties mentioned above. We use more than one biometric traits (similar / different) simultaneously which is called as multi biometric, provides more robust. There are a number of other information sources that can be combined to enhance security in the case of combining different biometric modalities. The following figure 1 shows the basic biocrypto system technique .

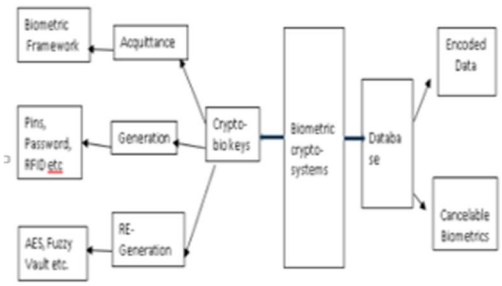


Figure 1: Basic Bio-crypto system technique

Grenze ID: 01.GIJET.10.1.304

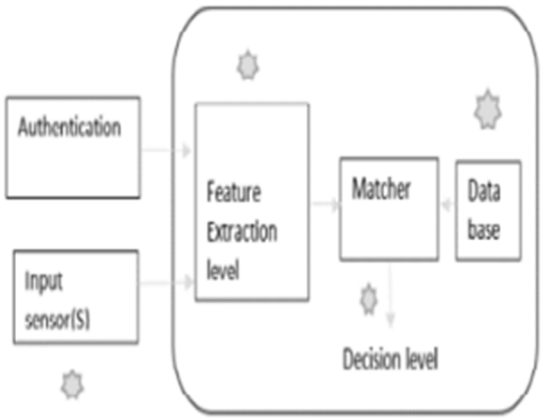


Figure 2: Different stages of attacks on a basic biometric system

II. Related Work

In a few years, multi-modal biometric fusion has gained considerable popularity as its efficiency is improved. Multimodal biometric cryptography increases device security. The literature has studied such cryptography techniques using multimodal biometrics. By fusion of finger print, retina, and finger vein with encryption techniques, Jagadiswary and Saraswady [7] have developed the multi-modal device. The system suggested has GAR of 94%, FAR of 1.46% and FRR of 1.07%, and a multimodal system with iris and palm vein, which was proposed by Bala and Joanna [8]. Features of the two modalities have been extracted via the extraction process, followed by an algorithm to protect the feature set with the Blow fish cryptography. The device proposed is very poor in FAR and FRR. S. More et al. [9] suggested a multimodal device with the modes of input of fingerprint, ears, iris and palm. The functional extraction method extracts input features and uses the cryptographic Algorithm Data Encryption Standard (DES) to secure features. With the aid of MATLAB, experimental results are shown. Gawande et al. [10] have proposed a multimodal framework that combines fingerprint and iris at extractive level and then employs a cryptographic method to secure input templates. For presentation of the results the publicly accessible CASIA database is used. With cryptographic encryption, the results of this proposed system are enhanced. Raghu and Deepthi [11] suggested a cryptographing-based multimodal authentication method. The secret key identified by the user is used to combine fingerprint and iris features. Experimental evidence suggests that the device proposed is better than a cryptographic unimodal one. A framework that will help users upgrade their biometric password and address several issues in existing biometric systems was proposed by Ashok et al [12]. Biometric password development is using the hacking feature. Biometric cryptography enhances system protection and provides better performance than many current systems. Mathew [13] has suggested an encrypted biometric device that uses the biometric modality to produce the secret key. To encrypt the Iris, you use the 32-bit fingerprint Id. The technique of Blow fish encryption is used to encrypt the template at registration time. During the decryption authentication process, the user is authentic or imposter. A device to enhance safety with the help of a bio-metric key was proposed by Arunachalam and Subramanian. FKP and fingerprint for the biometric key generation using K-mean algorithm are used in this framework. To encrypt a prototype, AES encryption technique is used. Also used for checking errors and deleting bad tempering is Cyclic redundancy check. E.S. Shameem S, Germany. [15] a multibiometric framework that combines FKP with face has been suggested. The Scale Invariant Feature Extraction (SIFT) procedure is known as the Multi-Modal Biometric Automation System (MMBAS) which reduces the system complexity and eliminates errors caused by failed samples. Experimental findings suggest that the system proposed is much better than the current system. S. Chaudhary and R. Nath [16] proposed a system which incorporated face, Iris and voice in combination with the Sum Rule Fusion technique. The device suggested is much better than the unimodal one. To verify device output, publicly accessible databases are used. With the aid of the MUBI tool the experimental results are shown. The multimodal system of FKP, face and palm print was proposed by Jacob Vetha Raj [17] and Anne Wincy. The feature set is extracted by the SIFT and Speed Up Robust Features (SURF) method and the Support Vector Machine (SVM) classifier used. The proposed system's FAR and FRR is less than unimodal. Experimental findings illustrate the performance and reliability of the proposed method.

III. Methodology

Key generation with Receiver's Enrolment In session-based communication, the session keys are exchanged before the sender and the receiver begin a secure session. The session key will originally be created randomly in this form of communication and passed to another user using public key encryption. In symmetric cryptography, the mutual key is used for message transmission from sender to receiver. The authentication of communicating parties is a big problem in this protocol. The sender and receiver authentication is checked through a trustworthy certification by third parties. Authenticity also relies on a third-party's reliability. Authenticity verification is also required before sharing their biometric data with each other in biometric symmetric encryption, where biometric data from both users produce and exchange an encryption key. There are two problems in this case. A finger-print data can be intercepted by an attacker and an attacker can generate the key through the algorithm that is transmitted via (unsecure). A theoretical approach is used when biometric receiver data are inscribed in the sender to overcome this problem. The biometric data that are stored can be used to authenticate the owner (i.e. the receiver) and since it is saved at sender side it is not necessary to send the key generation to other users (sender). In this way, biometric data is transmitted to another user through an unsecured channel. However, the cancellable stored template is used to safely forward the cancellable sender template. This method eliminates the need for authentication by third parties. At the time of registration, we recommend storing cancellable biometrics to preserve the privacy of the owner's biometric identity.

IV. System Description

In this method, it follows the same methodology used in approaches for cancellable fingerprint transformation models. The method involves three stages of registration, session key generation and template update. Enrolment. A database for biometric data of the recipient is stored at the sender site. This technique is called the sender's recipient registration. This is the following approach to registering recipients. First, it is presumed that minutiae (ride termination and bifurcation) points are extracted from the sender and receiver fingerprint image and biometrical data vectors are extracted at their own position. In addition, both sender and receiver build an annullable template (CTS), using the unique user key (Sks, Sks). In this way, the function vector can be used. Thirdly, the cancellable receiver template (CTR) has been XORed and the cancellable sender template (CTS,CTR) to lock CTR is stored in the sender's database and CTRlock is stored in CTR

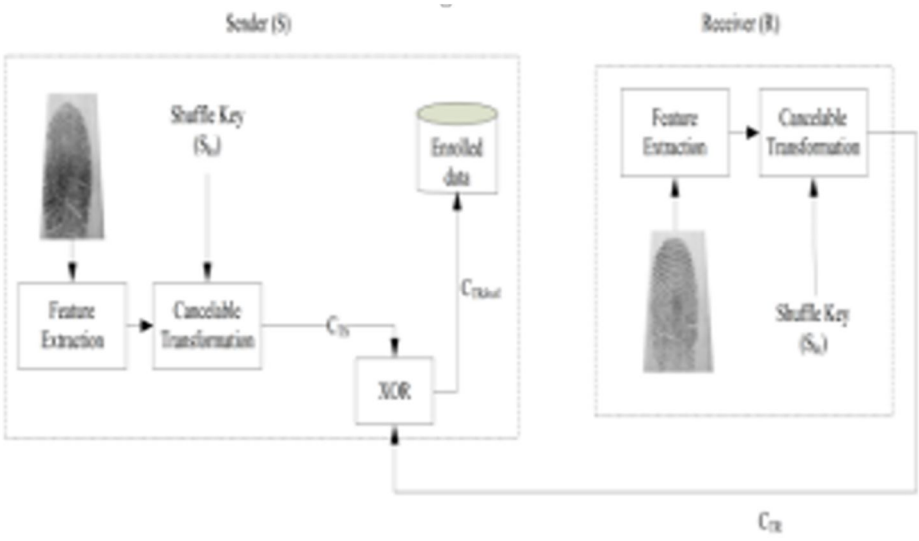


Figure 3 Enrollment process

V. Generation And Sharing Of Key Sessions

Following is the registration process, a session key is created in the sender and recipient cancellable templates. As key generation and authentication happens, the sender's fingerprint is captured and precise points are extracted. The cancellable Test template (C'TS) is created by means of the same keys (SKs). The locked template (CTRlock)

is opened by the test template XORing (CTR = CTRlock ⊕C'T'S). Sender and recipient initially each have their own shuffle keys, and locked cancellable receiver models are stored in the sender's database. Fig. 5.28 demonstrates the main generation and sharing process. When the recipient wishes to safely connect with the sender, the following steps are taken.

1. The receiver will submit a request for authentication.
2. The sender acknowledges the request from the recipient.
3. The receiver produces a test cancellable template (C'_{TR}) using its own SKr shuffle key from an early fingerprint and sends hash value ($h(C'_{TR})$) to sender.
4. Sender also generates a cancellable test sample (C'_{TS}) with his shuffle key (SKs) from his fingerprint.
5. Send the locked cancellable template (C_{TRlock}) stored in the database to be opened and the hash value $h(C_{TR})$ generated.
6. Sender compare the hash value received ($h(C'_{TR})$) to the hash value ($h(C_{TR})$ generated). If both are similar, the recipient is authentic and cryptographical key is created by the sender and recipient's cancellable templates. In the previous chapter, GenKey Cryptographic key = GenKey(C_{TR} ,C_{TS}).
7. Sender will lock the C_{TS} with the stored Cancellable Receiver Prototype (C_{TR}). C_{TSlock} = C_{TS} = C_{TR}, respectively.
8. Sender sends the C_{TSlock} to the receiver.
9. Receiver unlocks C_{TSlock} and generates the cryptographic key by XORing its own C'_{TR}. Key Ksr = GenKey(C'_{TR}, C_{TS}) cryptographic key. GenKey is the key generation algorithm discussed in the last chapter from cancelable templates. Now both sender and recipient have the same key (Ksr).
10. The created key (Ksr) can be considered as the session key and can be started securely with this key communication.

In the above steps, the hash value of the cancellable template is computed using the following method using an XOR dependent hash function. The cancellable prototype (CTR) is shown as a bit stream and the dimensions of the CTR are separated by the expected hash value(|h(CTR)|). If the division is recalled, the necessary sum of zero with the remainder is applied. Then, first block is XORed, and the result is XORed, the third block, and so forth. All blocks are XORed, with the previous results, and hash value is determined, except for the initial two blocks. In this process, sender and recipient authentication is tested in the following manner. The cancellable receiver template is stored in the sender's database and is locked with the cancellable sender template. Therefore the cancellable receiver prototype can be unlocked with its own fingerprint data by only genuine senders. Secondly, the hash of an enrolled cancellable receiver prototype corresponds to the hash value submitted by an applicant and is only matched when an original recipient requests his or her own fingerprint information. Thus, before safe contact begins, both users will be authenticated with their cancellable templates.

VI. Face Based Cryptographic Key Generation

The proposed methods for facial cryptographic key generation are discussed in this section. Figure 4 displays the diagrammatic description of the solution proposed. A variety of features of biometrics are derived from the face images of the customer. The extracted characteristics are quantized, then mapped for corresponding feature points to the binary representation. The binary properties formed and the randomly generated key is bound with the fuzzy vault. During authentication, when the authentication face features provided have major overlaps with those inscribed, the cryptographic key is correctly recovered. This section provides descriptions of the methods suggested.

A. Feature Extraction

As the extractor function, the Principal Component Analysis (PCA) is used. PCA is an unsupervised learning technique that offers optimal representation of the input in the lower dimensional space in the least value of the square error sense. In the method of Eigenface [127], given a Z = {Zi} C i=1 training set, the PCA is used to find the covarian matrix N-vectors, which contains C classes for each class {Zi} Ci j=1 , consisting of a number of face pictures zij, a total of $N' = \sum$ Ci C i=1 images, a training set Z is used to find the N, the covariance matrix eigenvectors of the PCA,

$$Scov = 1/N' \sum\sum(z_{ij}\, C_i\, j{=}1\; C\; i{=}1 - \bar{z})\,(zij - \bar{z})\; T \qquad (5.24)$$

Where $\bar{z} = 1/N' \sum \sum (z_{ij} - \bar{z})(z_{ij} - \bar{z})$ Ci T j=1 C i=1 is the ensembles average. The characteristics Eigen faces are the first N($\leq N'$) eigenvectors, which are referred to as a. The original image is transformed by a linear mapping into the Ndimensional face space:

$$yij = \psi\, T\, (zij - \bar{z}) \qquad (5.25)$$

Where the orthonormal vectors of base ψ are. In the transformed face space, the following classification of facial patterns is possible.

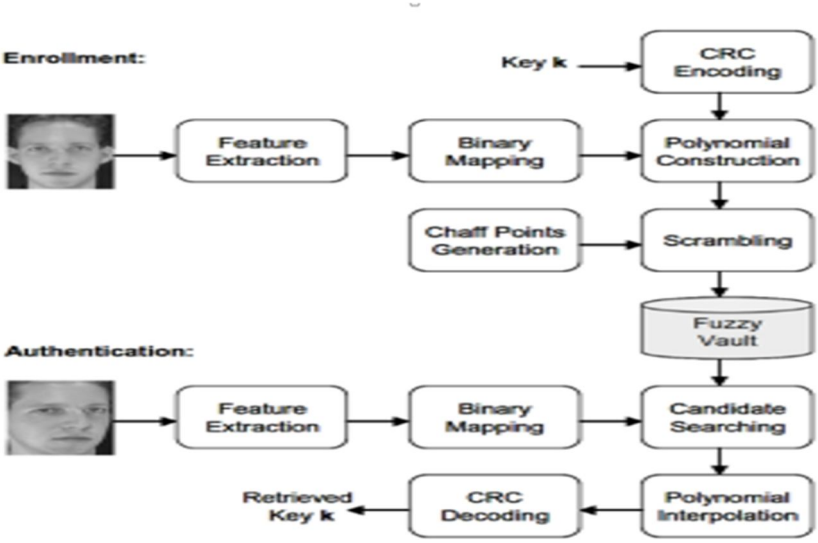


Figure 4 General Structure of the approach proposed

B. Binary Mapping

Unlike fingerprints, which use the specifics of points for functional matching, the PCA functions extracted are a series of real numbers, and it is normally difficult to accurately match them. One approach is to fit functional points based on proximity. But how to describe proximity is not easy. We propose a method for generating a two-dimensional quantification of facial features between the extracted features and the pairs of random vectors. The binary function process is as follows: Unlike fingerprints, where the coordinates of the minutiae points can be used for feature matching, the extracted PCA features are a set of real numbers, and generally exact matching is impossible. One method is to perform the matching of feature points based on closeness. However, it is not clear how to define the closeness. In this section, we propose a method to produce binary representation of face features based on 2-dimensional quantization of the distance vectors between the extracted features and pairs of random vectors. The procedure of producing binary features is as follows:

1. Extraction of the biometric data vector $y \in R\ N$
2. Create two random size NxM matrices, D+1≤M≤N, where D is a polynomial order for fluid vault building. To convert them into orthomorphic matrices Q1 and Q2 apply the Gram-Schmidt method.
3. The r_1 and r_2 elements are distributed uniformly to [0 τ], where τ is the pre-set value and two random Vector r_1 and r_2, length M.
4. Compute $R_{1i} = Q_{li*r1i}$ and $R_{2i} = Q_{2i*r2i}$, i=1..... M where I indicate the subscript in the column of i^{th} (Q1, Q2) and i^{th} (r_1, r_2).
5. In the case of R_1 and R_2, $d_{1i}=\|y-R1i\|^2$ and $d_{2i}=\|y-R_{2i}\|^2$ compute a Euclidean distance between y and each column vector.
6. In 256 steps, quantize d_{1i} and d_{2i} and map them to binary b_{1i} and b_{2i} strings.
7. In addition to the binary features, the corresponding bits in both b_{1i} and b_{2i}, i.e. bi=[b_{1i}| b_{2i}], i=1 .... M, are combined.

The N-dimensional face characteristics are mapped to the binary features of M 16-bit using the proposed procedure. The use of two distance vectors enables binary functions to be projected onto a 2-D image plane square where the b1i and b2i match the x and y axis coordination. This increases the exactness of the corresponding feature points as the binary feature bi matches both b1i and b2i. The projection of a y function on both axes is independent because of the randomness of R1 and R2. The orthogonization in step 2 creates binary chains in each direction which are uncorrelated. Step 3 and 4 generate different standard orthogonal vectors. The quantification and binary characteristically distributed over the entire plane would thus make it easier to conduct a brute force attack.

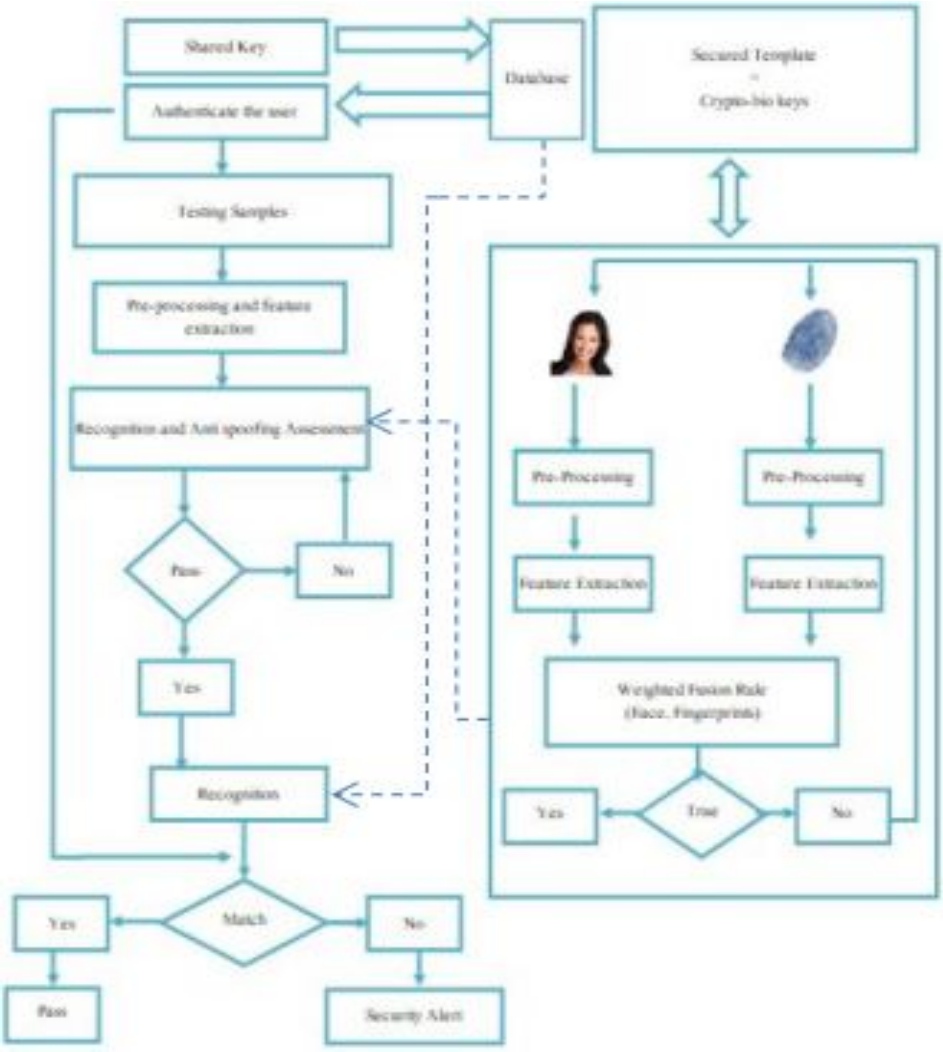
VII. Proposed Work

Figure 5 shows the architecture of the proposed biometric cryptographic multimodal device that combines the face and fingerprint. In the enrollment step two modes, namely fingerprint, should be captured and face-by-sensor, then extra noise from the pictures should be extracted using median filtering and the region of interest (ROI).

VIII. Fusion Level

We use an average fusion scheme, while the fused score is determined as a weighted combination of the results obtained by the M matching streams for each type of class (e.g. customer or impostor).where f is the fused score, xm is the normalized match score from the mth matcher and wm is the corresponding weight (obtained on some development data) in the interval of 0 to 1, with the condition

$$f = \sum_{m=1}^{M} w_m x_m \qquad \sum_{m=1}^{M} w_m = 1$$



IX. Results

The proposed system will definitely provide a better solution for anti-spoofing crypto-biometric system. Considering unimodal crypto-system and also considering multimodal crypto system. We have achieved better result using multimodal cryptosystem as shown in Table 1

TABLE I RESULT COMPARISON

Degree of Polynomial		n=8		n=10		n=12	
Biometric Modality	Cryptographic Algorithm	GAR(%)	FAR(%)	GAR(%)	FAR(%)	GAR(%)	FAR(%)
ME(DB1) + DPCA_2DPCA	FVA	98.47	1.25	92.54	0.53	88.35	0.22
ME(DB2) + DPCA_2DPCA		97.65	0.81	89.68	0.36	83.72	0.17
ME(DB3) + DPCA_2DPCA		96.52	0.72	87.70	0.27	85.69	0.11
GF(DB1) + DPCA_2DPCA	FVA	93.78	0.67	90.53	0.43	85.76	0.27
GF(DB2) + DPCA_2DPCA		90.85	0.52	87.85	0.21	83.99	0.17
GF(DB3) + DPCA_2DPCA		89.37	0.44	83.98	0.18	80.10	0.09
GF(DB1)+GF	FVA	90.54	3.48	87.52	3.08	85.83	2.56
GF(DB2)+GF		86.39	2.97	85.67	2.74	84.79	2.18
GF(DB3)+GF		84.15	2.34	83.43	2.10	82.64	1.78
ME(DB1)+GF	FVA	96.89	2.65	94.56	1.89	92.75	1.23
ME(DB2)+GF		95.42	2.45	92.83	1.76	90.87	1.07
ME(DB3)+GF		93.90	2.09	90.67	1.56	88.35	0.67
CF(DB1) + DPCA_2DPCA	FVA	98.53	0.95	97.21	0.56	96.46	0.22
CF(DB2) + DPCA_2DPCA		97.45	0.52	96.38	0.29	95.18	0.17
CF(DB3) + DPCA_2DPCA		96.84	0.17	95.51	0.06	93.86	0.02
CF(DB1)+GF	FVA	97.23	1.78	95.94	1.23	92.94	0.97
CF(DB2)+GF		95.67	1.31	93.48	1.06	91.34	0.84
CF(DB3)+GF		94.38	1.02	92.78	0.77	89.93	0.32

X. CONCLUSION

Biometric systems are widely used for reliable user authentication, and these systems will become the core IT infrastructure. Biometric authentication is therefore important. Current approaches and their architecture suffer from vulnerabilities and steps are vital to the security of government and commercial efficiency programmes. Sensor-level attacks on a device used for the automation of people's biometric identification have been tackled by independent and/or collaborated anti-spoofing attempts in the initial design and implementation. Modalities, latest studies on recommendations against intrusive action and the prototype facial fingerprint cryptosystem have been discussed in an assessment of data security issues.

REFERENCES

[1] A. E. Rosenberg. Automatic speaker verification: a review. Proc. IEEE, 64:475-487, 1976.

[2] A. K. Jain and A. Ross, "Learning User-specific Parameters in a Multibiometric System,"Proceedings of the IEEE International Conference on Image Processing (ICIP), vol. 1, pp.57-60,2002.

[3] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4-19, 2004.

[4] A. K. Jain, K. Nandakumar, and A. Ross, "Score normalisation in multimodal biometric systems" Pattern Recognition, vol. 38, pp. 2270–2285, 2005.

[5] A. Kale and A. R. Chowdhury, “Towards a view invariant gait recognition algorithm,” IEEE Conference on AVSS, pp. 143–150, 2003.

[6] A. Kale, A. Roy-Chowdhury, and R. Chellappa, "Fusion of gait and face for human identification," International Conference on Acoustics, Speech and Signal Processing, 2004.

[7] A. Kong, D. Zhang, and G. Lu, “A study of identical twins palmprint for personal verification,” Pattern Recognition, vol. 39, no. 11, pp. 2149–2156, 2006.

[8] A. Kong, D. Zhang, and M. Kamel, “A survey of palmprint recognition,” Pattern Recognition Letters, vol. 42, pp. 1408–1418, 2009.

[9] A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain. Personal Verification using Palmprint and Hand Geometry Biometrics. In Fourth International Conference on Audio - and Video-based Biometric Person Authentication (AVBPA), pages 669{678, Guildford, U.K., June 2003.

[10] A. L. Higgins and R. E. Wohlford. A new method for text-independent speaker recognition. In Proc. IEEE Int. Conf. on Acoust., Speech, Signal Processing (ICASSP), pages 869- 872, 1986.

[11] A. Ross and A. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, Special Issue on Multimodal Biometrics, vol. 24, pp. 2115-2125, 2003.

[12] A. Ross and R. Govindarajan. Feature Level Fusion Using Hand and Face Biometrics. In SPIE Conference on Biometric Technology for Human Identification, pages 196{204, Florida, U.S.A., March 2005.

[13] A. Ross, K. Nandakumar, and A.K. Jain, Handbook of Multibiometrics, Springer Verlag, 2006.

[14] Averbuch A, Lazar D, Israeli M. Image compression using wavelet transform and multiresolution decomposition. IEEE Transactions on Image Processing, 1996, 5(1): 4
[15] B. D. Ripley, Pattern Recognition and Neural Networks. U.K: Cambridge University 1996.
[16] B. Flury, Common Principle Components and Related Multivariate Models. USA: John Wiley and Sons, 1988.
[17] B. Gutschoven and P. Verlinde. Multi-modal identity verification using Support Vector Machines (SVM). In Proc. of Intl. Conf. on Information Fusion, FUSION, pages 3-8. IEEE Press, 2000.
[18] B.S. Atal. Automatic recognition of speakers from their voices. Proc.IEEE, 64:460-475, 1976.
[19] B.S. Atal. Efectiveness of linear prediction characteristics of the speech wave for automatic speaker identification and verification. J. Acoust. Soc. Am., 55(6):1304- 1312,1974.
[20] B. Y. Hiew, A. B. J. Teoh, and D. C. L. Ngo, Automatic Digital Camera Based Fingerprint Image Preprocessing. 2006.