International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-5, June 2013

A Hybrid Approach for Securing Biometric Template

Shweta Malhotra, Chander Kant Verma

Abstract-Biometrics authentication provides highest level of security. It allows the user to get authenticated using his or her own physical or behavioral characteristics. Unimodal biometrics have several problems such as noisy data, spoof attacks etc. which cause data insecure. To overcome these problems multimodal biometrics is used. Multimodal biometrics allows fusing two or more characteristics into single identification. It leads to more secure and accurate data. In this paper, we have combined two characteristics –one physical and one behavioral and further a key is added to the template to make it more secure. The template is finally stored in database.

Keywords-Biometric template protection, multimodal biometrics, biometric cryptosystem, hybrid approach for biometric template protection.

I. INTRODUCTION

Biometrics has long been known as a robust approach for person authentication [1]. With new advances in technologies, biometrics has becoming emerging technology for authentication of individuals. Biometric system identifies or verifies a person based on his or her physiological characteristics such as fingerprint, face, palm print, iris etc or behavioral characteristics such as voice, writing style, and gait. Theoretically, any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies features like universality, uniqueness, permanence and finally collectability.

The biometric authentication system uses two kinds of approaches- Unimodal and Multimodal. Biometric systems used in real world applications are unimodal [2]. These unimodal biometric systems rely on the evidence of a single source of information for authentication of person. A unimodal biometric system has sensor module to capture the trait, feature extraction module to process the data to extract a feature set that yields compact representation of the trait, classifier module to compare the extracted feature set with reference database to generate matching scores and decision module to determine an identity or validate a claimed identity as shown in figure 1.

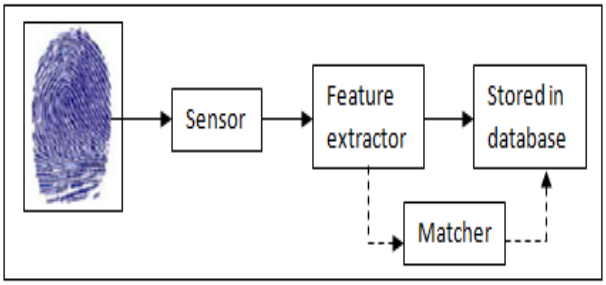

Figure 1: Unimodal biometric system

Though these unimodal biometric systems have many advantages, it has to face with variety problems like: Noise in sensed data, biometric data can be contaminated by noise due to imperfect acquisition conditions which may lead to false rejections. Non universality, meaningful data from a subset of individuals could not be acquired which results in failure to enroll error. Spoofing, behavioral traits are usually vulnerable to spoof attacks where an intruder mimics the trait corresponding to the enrolled subjects. Intra class variation, the biometric data acquired during verification will not be identical to the data used for generating template during enrollment for an individual. This is known as intra-class variation. Large intra-class variations increase the False Rejection Rate (FRR) of a biometric system. Interclass similarities, the overlap of feature spaces corresponding to multiple individuals. Large Inter-class similarities increase the False Acceptance Rate (FAR) of a biometric system.

These problems were addressed by introducing multimodal biometric approach. It consolidates multiple sources of biometric information. This can be accomplished by fusing. Fusion can be done at different levels. The various levels of fusion in multimodal biometric are described in figure 2. A decision made by a multimodal biometric system is either a “genuine individual" type of decision or an “imposter" type of decision.

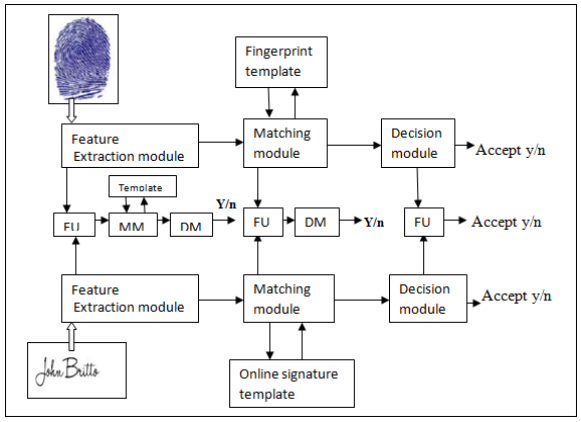

Figure 2: Multimodal biometric system.

Manuscript published on 30 June 2013.
* Correspondence Author (s)
Shweta Malhotra, M Tech student, DCSA, kuk, kurukshetra, have published two more papers except this paper.
Dr.Chander Kant Verma, Assistant professor, DCSA, KUK, kurukshetra.He is phd in field of biometrics from DCSA, kuk. He is on the role of editor chief in IJITKM, associate editor in IJCSC and in IJEE. He is also member of editoral board in IJCA, IJSC, IJISP and IJCIRP.

Based on the type of information available in a certain module, different levels of fusion can be defined. [3][4]. Sensor level fusion, this fusion refers to the consolidation of raw data obtained using multiple sensors or multiple snapshots of biometric using a single sensor. Feature level fusion, this fusion refers to the consolidation of features sets from different biometric traits into single feature set of features. Score level fusion, in this level of fusion, the match scores output by multiple matchers are combined to generate a new match score that can be subsequently used by verification or identification modules for rendering an identity decision. Decision level fusion, this fusion combines multiple decisions. This is most feasible. It uses simply "AND", "OR", majority voting etc. for combing decisions.

The multi-biometric system relies on the evidence presented by multiple sources of biometric information. Based on nature of these sources, a multi-biometric system can be broadly classified into one of the following six categories: [5]. Multi-sensor systems, these systems employ multiple sensors to capture a single biometric trait of an individual. The use of multiple sensors can result in acquisition of complementary information that can enhance the recognition ability of the system. Multi-algorithm systems: Invoking multiple feature extraction and /or matching algorithms on the same biometric data can result in improved matching performance. This can enhance identification rate of the biometric system. But on the other hand can increase the computational complexity of the systems. Multi-instance systems, these systems use multiple instances of the same body trait for ex: left and right index fingers, or left or right iris of an individual which may be used to verify an individual's identity. Multi-sample systems, in this system a sensor may be used to acquire multiple samples of the same biometric trait in order to account for variations that occur in the trait for ex: a face system may capture the frontal profile of a person's face along with the left and right profiles in order to account for variations in the facial pose. Multi-modal systems, these systems establish identity based on the evidence of multiple biometric traits. The identification accuracy can be significantly improved by utilizing number of traits but can be restricted by practical consideration such as cost, enrollment time, throughput time, expected error rate, etc. Hybrid systems, the term hybrid are used to describe systems that integrate a subset of five scenarios discussed above. Thus the system is multi-algorithmic and multimodal in its design.

II. RELATED WORK

Till date many multimodal systems have been implemented and deployed for commercial use, these systems are implemented according to different fusion levels and different algorithms. Hariprasath. S et al. has given an approach of multimodal system with iris and palmprint using Wavelet Packet Transform [WPT] and score level fusion. It has found that WTP gives high accuracy [6]. A. Kumar et al. proposed a multimodal framework based on face and ear modalities, using Haar wavelet and Scale Invariant Feature Transform [SIFT] features are extracted. Finally integration of their ranks has been done with modified Borda count and Logistic regression method. According to A. Kumar et al. logistic regression is better than borda count method [7]. S. Jahanbin et al. proposed a novel multimodal framework for (2D+ 3D) face recognition using Gabor Wavelet. Gabor coefficients are first computed and finally decision has made with fusion at matching score level [8]. T. Murakami et al. proposed multimodal biometric system based on face, fingerprint and iris modalities with Bayes decision rule- score level fusion technique and Permutation based indexing technique for identification of these modalities [9]. Y. Zheng et al. have proposed system using multispectral face images with four different fusion methods i.e. mean fusion, Linear Discriminent Analysis [LDA] fusion, k-nearest neighbor [KNN] fusion, and hidden Markov model [HMM] and according to Y. Zheng et al. HMM fusion is the most reliable score fusion method [10]. N. Gargouri Ben Ayed et al. have developed system using fingerprint and face using Gabor wavelet and Local Binary patterns [LBP]. Finally fusion has done at match- score level with weighted sum method and found to be excellent method giving higher performance [11]. Mahesh P.K. et al. proposed the multimodal biometrics system using two traits speech and palm print, Wavelet-Based Kernel PCA and Mel Frequency Cepstral Coefficients (MFCC) is used to extract features of signal. Finally decision has made by fusion at matching score level with weighted sum [12]. A. P. Yazdanpanah et al. has proposed system using face, ear and gait with the use of gabor wavelet and fusion at matching score level with weighted sum and weighted product approaches [13]. F. A. Fernandez et al. proposed quality-based conditional processing in multi biometrics with fusion at rank level using linear logistic regression approach [14]. A. Cheraghian et al. has proposed system based on 2D and 3D face image by applying gabor wavelet transformation with fusion at decision level fusion [15]. A. Bhattacharjee et al. have proposed multimodal approach with iris and speech modalities with Daubechies wavelet for feature extraction and decision has made by fusion at feature level [16]. D. R. Kisku et al. has addressed multimodal biometric system using face and palm print modalities. Md. M. Monwar et al.has given new approach for multimodal biometric system using face, ear and signature modalities, Principle Component Analysis [PCA] has been used with fusion at rank level- using highest rank, borda count and logistic regression approaches and logistic regression [17]. P. Kartik et al. have proposed system using face, speech and signature features. Principal Component Analysis [PCA], Linear Discriminant Analysis [LDA] and Mel Frequency Cepstral Coefficients [MFCC] used for feature extraction. Finally decision has made at matching score level with sum rule [18]. F. Yang et al. have proposed ultimodal biometric systems based on fingerprint, palmprint and hand geometry modalities using Support Vector machine [SVM] and wavelet transform with fusion at matching score itself [19]. Xiao-Na Xu et al. have presented a novel method of feature-level fusion based on Kernel Fisher Discriminant Analysis (KFDA) with Average rule, Product rule and Weighted-sum rule respectively and applied it to multimodal biometrics based on fusion of ear and profile face biometrics [20]. S. Ribaric et al. evaluated different techniques of matching score fusion level like Bayes-based normalization, min-max, zscore, median-MAD, double-sigmoid, tanh, and piecewiselinear on different multimodal biometric systems with fingerprint, face and palmprint modalities [21]. A. Jain et al. have developed multimodal biometrics using face, fingerprint and hand geometry modalities with matching score level fusion.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

As in case of matching score level fusion normalization of match score is important aspect, A. Jain et al. have done normalization of match scores of these modalities with different such as min-max, z-score and tanh technique [22].

III. PROPOSED WORK

Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In this proposed work, we have combined one physical and one behavioral approach for identification or verification to uniquely identify a person. The approach takes two different biometric traits. One finger print as physiological and other online signature as behavioral biometric trait. Both are sensed by sensor, features are extracted by feature extractor modules, matcher module matches the traits with stored template, each decision module decide the perfect matches. Finally decisions are combined in fusion unit using simple "AND" and decision is taken whether the individual is not intruder.

A. Fingerprint recognition

A fingerprint is the representation of epidermis of a finger. It consists of a pattern of interleaved ridges and valleys. Using designing algorithm, we can easily increase the clarity of ridge structure so that the minutiae and reference points are easily and correctly extracted. As this is a physical trait and hence never gets changed, still in some accidental cases it gets changed, the template need to enroll again.

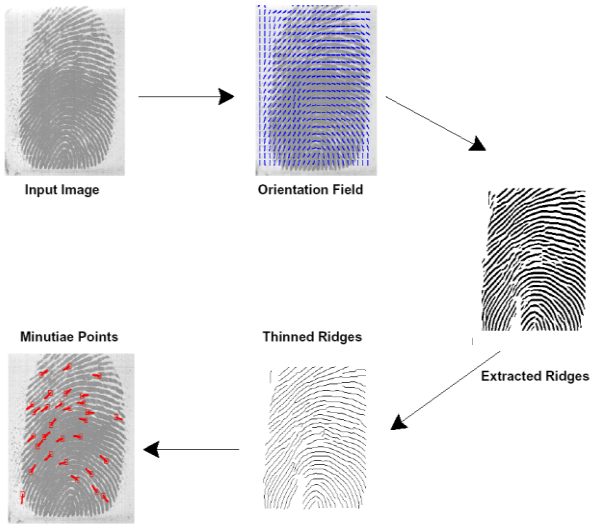

Figure 3: steps involved in fingerprint recognition.

Figure 3 shows steps involved in fingerprint features extraction. Fingerprint image is sensed, placed in orientation field, ridges and valleys of fingerprint are extracted, ridges are thinned and finally minutiae points are discovered.

B. Online signature recognition

It is an important authentication method as it is easily acquired and of its widespread use. During acquisition of the online signature a high resolution scanner is required and noise removal operation is also performed to eliminate extra dots on the image. It is behavioral trait and hence can change with time. If the individual changes his or her signature it needs to be enrolled again.

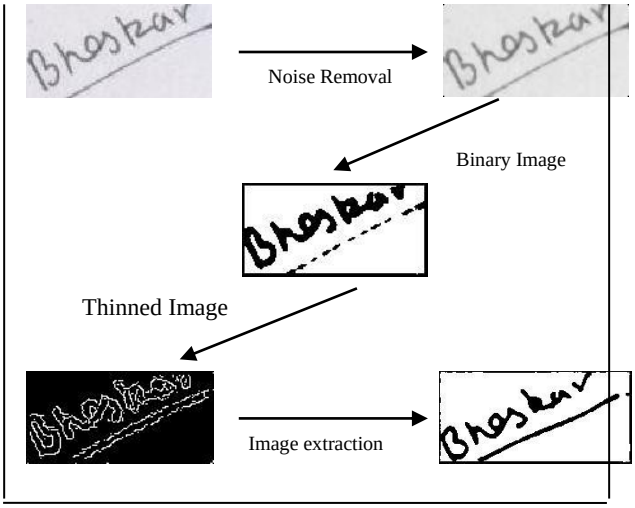

Figure 4: steps involved in online signature extraction.

Figure 4 shows steps invoved in extracting online signatures. Online signature is sensed by sensor. Noise is removed by eliminating extra dots anywhere nearby signature. Real image is converted to binary image. Binary image is thinned. Finally, image is extracted.

C. Key binding biometric cryptosystem

The biometric cryptosystem require the storage of biometrics data with some key to provide protection. The combination of the biometrics data and key is known as helper data. It can be formed using two techniques either key binding or key generation. In key binding biometric cryptosystem, helper data is obtained by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication. Since cryptographic keys are independent of biometric features these are revocable while an update of the key usually requires re-enrollment in order to generate new helper data. The technique can be easily understood using figure 6.

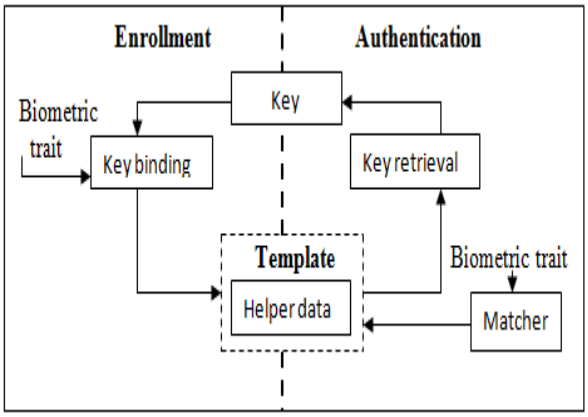

Figure 5: Key binding biometric cryptosystem.

D. Architecture of proposed approach

The architecture of the proposed approach is described as in figure 7 and figure 8. The approach has two phases: enrollment phase and authentication phase.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In enrollment phase the biometric traits are extracted and a random key is generated which is bound with the features using key binding algorithm and helper data is created. The enrollment phase is described in figure 7. During authentication, after extracting feature the template is matched with the stored helper data. Using key retrieval algorithm key is retrieved and matched with the previous key. After that the decision is taken. The two decisions are fused to one single decision.

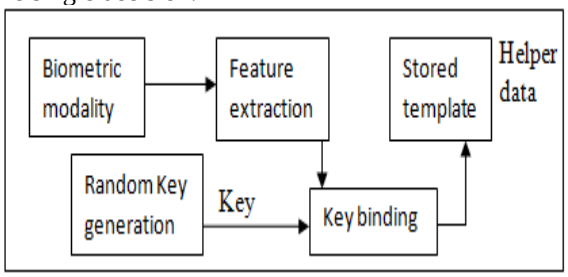

Figure 6: General enrollment for proposed approach.

During authentication, two different unimodal biometric are used. Each unimodal biometric trait has its own feature extraction module, matcher module, stored database and decision module.

The various modules of authentication in proposed approach which is shown in figure 8 are described as follows:

(1). Feature extraction module: The goal of extracting features of biometric trait is to increase the clarity of internal structure and get proper minutiae features. The features of the fingerprint can be extracted using reference point algorithm [23] or minutiae matching approach. The features of online signature are extracted using extraction global and local features [24] [25]. Global features are extracted by taking the signature as a whole and extracting the width and length of the signature. Local features are extracted by extracting every small point, hence computation is large and grid notification is done very carefully.

(2). Matching module and the stored database: The matching of the biometric trait with the stored template is done at this module. The working of the module for the proposed approach is described in figure 4. During enrollment, the biometric trait is extracted and key is bounded with it to make it more secure. During authentication, biometric trait is matched with the stored template using a matcher [26] [27]. If retrieved key matches with the key bounded at the time of enrollment the individual is same person otherwise not.

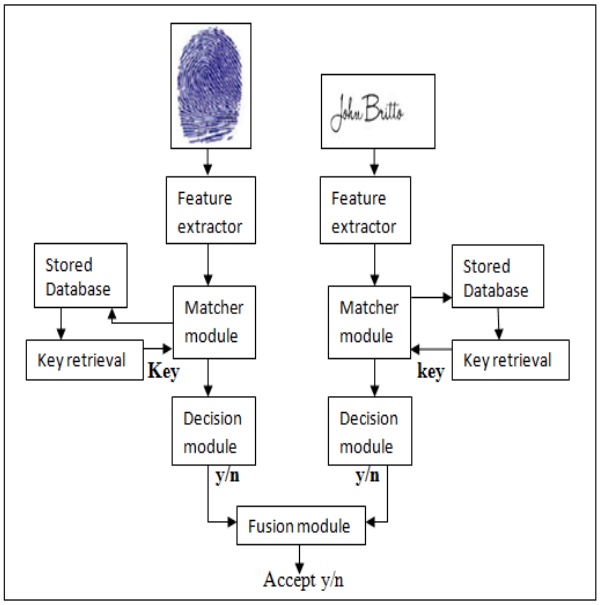

Figure 7: Authentication in proposed approach

(3). Decision module and fusion module: The decision module exposes the decision after the matching. If the individual is the same person then the decision is yes (y) otherwise not (n). The decision from both the decision modules is fused in the fusion module. The fusion at this level is feasible and simple to access. The fusion is done using simply "AND". The fusion module finally results in acceptance or rejection of individual. The working of the "AND" is described in the below table.

Table: fusion of decisions in proposed approach.

Fingerprint decision	online signature decision	Fusion decision
y	y	y
y	n	n
n	y	n
n	n	n

E. *Comparison of proposed approach with other approaches*

(1). Proposed approach is an ideal approach as it satisfies the entire required properties of template protection scheme. It is diverse, secure, and revocable and provides high performance.

(2). The key binding cryptosystem approach provides enhanced secure templates and does not allows the real template to get exposed and hence retains advantage of cancelable biometrics.

(3). The multimodal approach is used which helps to uniquely identify a person accurately and the fusion level are chosen at decision, hence made the approach simple and not complicated.

IV. CONCLUSION

In this research paper, unimodal and multimodal biometrics are introduced. Various level of fusion in multimodal biometrics and classification of multibiometris have also been included. Further, an approach is introduced which includes multimodal biometrics and also key binding which helps to keep the templtes secure and uniquely identify a person. With these two concepts the approach is called hybrid and can be used to accurately identify an individual. There are many multimodal biometric systems in existence for authentication of a person but still selection of appropriate modals, choice of optimal fusion level and redundancy in the extracted features are some challenges in designing multimodal biometric system that needs to be solved.

V. ACKNOWLEDGMENT

I would like to express my deep sense of indebtedness ans sincerest gratitude to Dr. chander kant verma for his in -valuable guidance and appreciation throughout the work.

REFERENCES

[1] M. Deriche, "Trends and Challenges in Mono and Multi Biometrics," in *Proc. of Image Processing Theory, Tools and Application (IPTA), Sousse*, pp.1-9, 23-26 Nov 2008.

[2] M. S. Ahuja and S. Chabbra, "A Survey of Multimodal Biometrics**",** *International Journal of Computer Science and its Applications*, pp. 157-160.

[3] A. Ross and A. Jain, "Information Fusion in Biometrics," *Journal of Pattern Recognition Letters*, vol. 24, pp. 2115-2125, 2003.
[4] Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013 DOI: 10.5121/sipij.2013.4105 57 AN OVERVIEW OF MULTIMODAL BIOMETRICS P. S. Sanjekar and J. B. Patil.
[5] A.ross, K.nandakumar, and A.K. jain. Handbook of multibiometrics, springer, newyork, USA,ist edition, 2006.
[6] S. Hariprasath and T. Prabakar, "Multimodal Biometric Recognition using Iris Feature Extraction and Palmprint Features," in Proc. of International Conference on Advances in Engineering, Science and Management (ICAESM), Nagapattinam, pp. 174-179, 30-31 March 2012.
[7] A. Kumar, M. Hanmandlu and S. Vasikarla, "Rank Level Integration of Face Based Biometrics," in Proc. of Ninth International Conference on Information Technology: New Generations (ITNG), Las Vegas, pp. 36-41, 16-18 April 2012.
[8] S. Jahanbin, Hyohoon Choi and A. Bovik, "Passive Multimodal 2D+3D Face Recognition using Gabor Features and Landmark Distances," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 4, pp. 1287-1304, Dec. 2011.
[9] T. Murakami and K. Takahashi, "Fast and Accurate Biometric Identification Using Score Level Indexing and Fusion," in *Proc. Of International Joint Conference on Biometrics (IJCB), USA*, ,pp. 978-985, 2011.
[10] Y. Zheng and A. Elmaghraby, "A Brief Survey on Multispectral Face Recognition and Multimodal Score Fusion," *in Proc. of IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Bilbao, pp. 543-550, 14-17 Dec 2011.
[11] N. Gargouri Ben Ayed, A. D. Masmoudi and D. S. Masmoudi, "A New Human Identification based on Fusion Fingerprints and Faces Biometrics using LBP and GWN Descriptors," in *Proc. Of 8th International Multi-Conference on Systems, Signals and Devices (SSD), Sousse*, pp. 1-7, 22-25 March 2011.
[12] P. K. Mahesh and M. N. S. Swamy, "A Biometric Identification System based on the Fusion of Palmprint and Speech Signal," in *Proc. of International Conference on Signal and Image Processing (ICSIP), Chennai*, pp. 186-190, 15-17 Dec. 2010.
[13] A. Yazdanpanah, K. Faez and R. Amirfattahi, "Multimodal Biometric System using Face, Ear and Gait Biometrics," in *Proc. of 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), Kuala Lumpur*, pp. 251-254, 10-13 May 2010.
[14] F. A. Fernandez, J. Fierrez and D. Ramos, "Quality-Based Conditional Processing in Multi- Biometrics: Application to Sensor Interoperability," *IEEE Trans. On Systems, Man, And Cybernetics—Part A: Systems and Humans*, vol. 40, no. 6, pp.1168-1179, Nov. 2010.
[15] A. Cheraghian, K. Faez, H. Dastmalchi and F. Oskuie, "An Efficient Multimodal Face Recognition Method Robust to Pose Variation," in *Proc. of IEEE Symposium on Computers & Informatics (ISCI), Kuala Lumpur*, pp. 431-435, 20-23 March 2010.
[16] A. Bhattacharjee, M. Saggi, R. Balasubramaniam, A. Tayal and Dr. A. Kumar, "A Decision Theory Based Multimodal Biometric Authentication System Using Wavelet Transform," in *Proc. of the 8th International Conference on Machine Learning and Cybernetics , Baoding*, pp. 2336-2342, 12-15 July 2009.
[17] M. Monwar and M. Gavrilova, "Multimodal Biometric System using Rank-Level Fusion Approach," *IEEE Trans. On Systems, Man, and Cybernetics-Part B: Cybernetics*, vol. 39, no. 4, pp. 867-878, August 2009.
[18] P. Kartik, R. V. S. S. Vara Prasad and S. R. Mahadeva Prasanna, "Noise Robust Multimodal Biometric Person Authentication System using Face, Speech and Signature Features," in *Proc. Of Annual IEEE India Conference (INDICON), Kanpur*, vol. 1, pp. 23-27, 11-13 Dec. 2008.
[19] F. Yang and Baofeng M. A, "Two Models Multimodal Biometric Fusion Based on Fingerprint, Palm-Print and Hand-Geometry," in *Proc. of 1st International Conference on Bioinformatics and Biomedical Engineering (ICBBE), Wuhan*, pp. 498-501, 6-8 July 2007.
[20] Xiao-Na Xu, Zhi-Chun Mu and Li Yuan, "Feature-Level Fusion Method based on KFDA for Multimodal Recognition Fusing Ear and Profile Face," in *Proc. of International Conference on Wavelet Analysis and Pattern Recognition, Beijing*, vol. 3, pp. 1306-1310, 2007.
[21] S. Ribaric and I. Fratric, "Experimental Evaluation of Matching-Score Normalization Techniques on Different Multimodal Biometric Systems," in *Proc. of IEEE Mediterranean Electrotechnical Conference*, Malaga, pp. 498-501, 16-19 May, 2006.
[22] A. Jain, N. Karthik and A. Ross, "Score Normalization in Multimodal Biometric Systems,"*Journal of Pattern Recognition*, vol. 38, no.12, pp. 2270-2285, 2005.
[23] A. Ross, A. K. Jain & J.A. Riesman, *Hybrid fingerprint matcher*, Pattern Recognition, 36, pp. 1661–1673, 2003
[24] M. Ammar, T. Fukumura, & Y. Yoshida, *A new effective approach for off-line verification of signature by using pressure features*. 8th International Conference on Pattern Recognition, pp. 566-569, 1986
[25] M. A. Ismail, S. Gad, *Off-line Arabic signature recognition and verification*, Pattern Recognition, 33 pp. 1727-1740, 2000
[26] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," Proc. of the IEEE, vol. 92, no. 6, pp. 948–960, 2004.
[27] A Survey on Biometric Cryptosystems and Cancelable Biometrics by Christian Rathgeb and Andreas Uhl.

Shweta Malhotra, mtech student, DCSA, kuk, kurukshetra, have published two more papers except this paper.

Dr.Chander kant verma, Assistant professor, DCSA, KUK, kurukshetra.He is phd in field of biometrics from DCSA, kuk. He is on the role of editor chief in IJITKM, associate editor in IJCSC and in IJEE. He is also member of editoral board in IJCA, IJSC, IJISP and IJCIRP.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)