A Robust Multimodal Biometric System VIA Multiple Svms

Komal, Chander Kant

Abstract— Generally single Support Vector Machine (SVM) is employed in existing multimodal biometric authentication techniques, and it assumes that whole set of the classifiers is available. But sometimes it is not possible due to some circumstances e.g. injury, some medical treatment etc. This paper includes a robust multimodal biometric authentication system that integrates FKP (Finger-Knuckle Print), face and finger-print at matching score level fusion using multiple parallel Support Vector Machines (SVMs). Multiple SVMs are applied to overcome the problem of missing biometric modality. Every possible combination of three modalities (FKP, face and finger-print) are taken into consideration and all combinations have a corresponding SVM to fuse the matching scores and produce the final score set for decision making. Proposed system is more flexible and robust as compared to existing multimodal biometric system with single SVM. The average accuracy of proposed system is estimated on a publicly available dataset with the use of MUBI tool(Multimodal Biometrics Integration tool) and MATLAB 2017b.

Keywords: Face recognition, Finger knuckle print recognition, Finger print recognition, Support Vector Machines (SVMs).

I. INTRODUCTION

Unimodal biometric recognition systems suffer from many limitations; some of them are non universality, noisy data, spoof attacks, intra-class variations, interoperability, and distinctiveness issues [1]. Multi-biometric systems are much more consistent due to the availability of a number of sources of information[2]. Depending upon the input data, a multi-biometric system is classified into various categories i.e. multiple sensors, multiple algorithms, multiple instances, multiple samples and multimodal systems as shown in Fig. 1. Multimodal biometric authentication devices and systems address non-universality by providing multiple modalities or classifier. Noisy data problem can be address by using multiple sensors and multiple traits. Problem of distinctiveness or Intra-class variations can be address with the help of multiple instances of same modality.

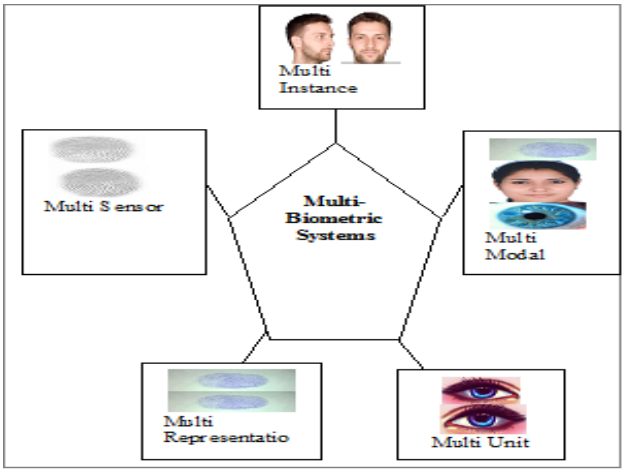

Fig. 1.Various sources of the biometric information

Multimodal biometric authentication devices and systems address non-universality by providing multiple modalities or classifier. Noisy data problem can be address by using multiple sensors and multiple traits. Problem of distinctiveness or Intra-class variations can be address with the help of multiple instances of same modality. Spoof attack can be prevented with multimodal systems because spoofing of multiple biometrics modalities at same time is very difficult [3].

Generally four modules are used in biometric system – (i) sensor module, (ii) feature extraction module, (iii) matcher module, and (iv) decision module. According to K. K. Paliwaland C. Sanderson, [4]two broad categories of the different level of fusion are: fusion-before-matching and fusion-after-matching. These categories of fusion are totally based upon the fact that the total amount of related information available before matching is more than the information available after matching. Fusion before matching includes the fusion at two levels i.e. sensor level and feature extraction level. Fusion after matching contains the fusion of the other two levels which are match score level and decision level. In general, fusion applied at sensor level or feature extraction level is more effective since the amount of information available at these levels is more reliable and accurate than information present at other levels. The amount of information goes on decreasing when someone moves from sensor module to the next decision module.

Noise and other climatic influences in the raw data cause the problem in the sensor level fusion. A large number of feature sets in the feature level fusion corresponding to a

Revised Manuscript Received on September 10, 2019.

Ms. Komal, Research Scholar, Department of Computer Science & Applications, K.U., Kurukshetra, Haryana, India.

Dr. Chander Kant, Assistant Proffessor, Department of Computer Science & Applications, K.U., Kurukshetra, Haryana, India.

number of modalities gets combine and give further result. Feature set contains rich or accurate information about the raw data, so in terms of accuracy it is concluded that feature level fusion provide better result than match score or decision level fusion. But, feature level fusion is quite tough as compared to others. There are some reasons for not preferring feature level fusion, which are as follows (i) due to incompatibility of the feature set of different biometric traits (e.g. eigen-values of face and minutiae points of fingerprints) (ii) sometimes do not have the knowledge of the relationship between the different modalities feature spaces (iii) concatenating two large feature vectors may lead to the curse of dimensionality problem and (iv) for large concatenated feature vector might be operated by a more complex matcher[5]. Thus sensor or feature levels fusion requires extra processing complexity. After these levels, match scores level has high quality of information about data. Hence, match score level fusion is preferredover others [6]. Decision level contains the least amount of information. This type of fusion is performed only when system provide access to the final output only [7].

Accuracy of the biometric system has been effectively improved with the use of multimodal biometric techniques. But they also have some limitations. For example, most of the existing multimodal biometric system with single machine learning strategies assumes that whole set of the classifiers is available. But sometimes it is not possible due to some circumstances e.g. injury, some medical treatment etc. A robust multimodal biometric system has been proposed that integrates finger-print, finger-knuckle print and face at match score level fusion using multiple parallel Support Vector Machines (SVMs). Multiple SVMs are applied to overcome the problem of missing biometric classifier. Every possible combination of three classifiers (finger-print, face and FKP) are considered and each combination has a corresponding SVM to fuse the match scores and produce the score set for decision making.

Organization of the rest of the paper is as follows: Section 2 presented the related works. Section 3 describes the proposed system architecture and fusion performed. Section 4 shows the resultsfor all the possible cases of biometric classifier. In last section, the summary and future work is included.

II. RELATED WORK

In last few years, multimodal biometric Fusion has achieved significant attention because it increases the performance of system. Lots ofeffort has been done in multimodal biometric areathat yieldsmature hybrid multimodal biometric systems. Literature has been studied and finds that match score is most widely used fusion level in multimodal systems.

Feng et al. [8] fused palmprint and faceat feature extraction level. Fusion is performed by adding the features extracted by using ICA and PCA with the support vector machine and nearest neighbor classifier.

Luca et al. [9] fusedface and fingerprint at tmatching level. They used LDA and PCA for the biometric feature extraction process, Fusion was performed using techniques like product rule, mean rule and bayesian rule with FRR of 0.6% to 1.6% and FAR of 0%.

Meraoumia et.. al. [10] proposed a system by integrating FKP&palmprintwith EER = 0.003 %.

Kartiket. al. [11] fused speech and signature at the match score level. System gets the accuracy rate of 81.25% with the help of sum rule fusion and min-max normalization technique.

Rodriguez et al. [12] fused iris and signature by usingsome fusion techniques (eg. sum rule, product rule etc.). Neural Network classification technique is used with EER (Equal Error Rate) below than 2.0%.

Kiskuet. al. [13] proposed asystem by integratingpalmprint and face at feature extraction phase.Accuracy rate of proposed system is 98.76%.

Tohet al.[14] fused fingerprint, hand geometryand voice and get 85% to 95% accuracy performance.

Ortega-Garcia and Fierrez-Aguilar [15] proposed a multimodal system fusing finger print, face and online signature at match score level with 0.5% of EER (Equal Error Rate).

Viriri and Tapamo [16] presented a multimodal biometric system fusing signature and iris at matching level with 0.08% of FRR and 0.01% of FAR.

Kazi.and Rode [17] developed a systemthat integrates signature and face at matching level. The bimodal system improves accuracy rate of proposed system by 10%.

Aboshosha and kamal [18] fused fingerprint, iris and face at match score level and experimental results shows better performance of purposed system than unimodal.

S chaudhary and R nath [19] presented a robust multimodal system using multiple SVMs that fuses iris, face and fingerprint at match score level. This system addresses the problem of missing biometric modalities at authentication time.

K vishi and V mavroeidis [20] fused fingerprint and finger vein with the help of TanH normalization and sum rule fusion technique at matching score level. This multimodal system has accuracy rate of 99.98% with EER of 0.00010%.

K shinde and S tharewal [21] integrates face, fingerprint and iris at match score level and result shows that multimodal systems is better than unimodal biometric systems.

III. PROPOSED WORK

Biometric system performance requirement does not meet with the use of single biometric classifier. Performance or recognition accuracy of the biometric systems are enhanced with the use of multimodal system by combining multiple sources of information. If any one of the classifier is missing at the time of authentication than performance and recognition accuracy of the biometric system greatly degrades. Single SVM based fusion technique cannot solve this type of issue. To overcome the problem of missing classifier, a robust multimodal fusion technique is presented in this paper.

A. Feature Set Extraction of Biometric Modalities

Sensor collects the initial raw sample of three modalities (finger print, face and finger knuckle print), and an appropriate technique is carried out to extract desired features of a modality and detailed features extraction process is as follows:

- *FKP Feature Set Extraction*: Three bones are presented in human finger: (i) proximal, (ii) middle and (iii) distal phalanx. Proximal phalanx is that where both finger and hand joins. Other two joints are called middle and distal phalanx. The creases or lines on back of finger joints are called Finger knuckles as shown in Fig. 2 [22].

Fig. 2.Finger joint and finger knuckle print

Every person has unique creases or line pattern.At the very first phase, capture the input images through sensors or any acquisition device. After acquisition, localize the region of interest. Edge detection approach has been used to extract region of interest and finally gives segmented FKP image. An enhancement method can be used for enhancing the quality of images. 2D gabor filters method is used to extract the final feature set. Feature extractionprocess of FKP is shown in Fig. 3 [23].

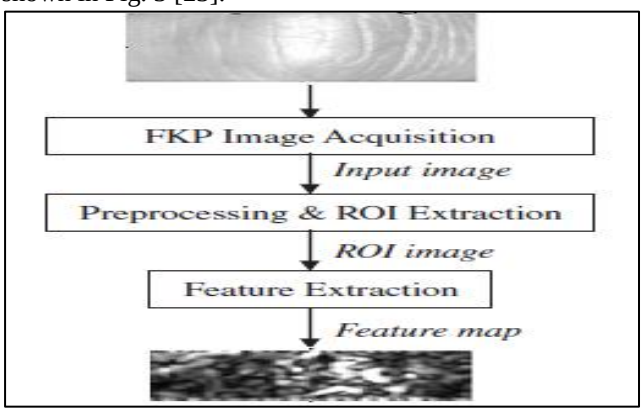

Fig. 3.Finger knuckle print feature set extraction process

- *Face Feature Set Extraction:* Face spatial extent has been determined during face detection process of given image followed by feature extraction process. First step of face feature set extraction process is face detection process. There are some organs like nose, eyes, ear, mouth etc which makes the human face[24]. Every organ of the face is different in structure and size. Characteristics of these organs with their geometric distribution are extracted to recognize a human face. Human faces are different because of difference in size shape or structure of these organs. Relative distance between them makes some different patterns. These features are called principal component or eigenfaces in face recognition biometric system. First step is the exaction of feature points and then features set of faceis extracted using eigenface approach [25]. PCA is applied to compute feature vector on reduced eigenspace that is projection of original input image [26]. Euclidean distance between detected face features and stored template is used to create the matching score**.** Fig. 4 shows the whole process of feature extraction in facial recognition system [27].

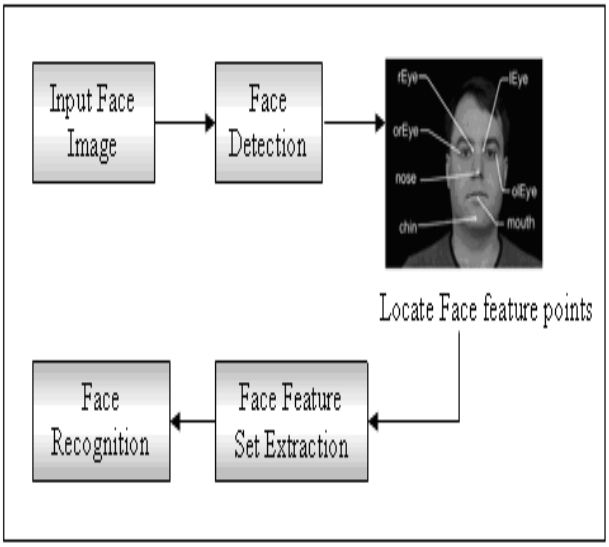

Fig. 4.Face feature set extraction process

- *Fingerprint Feature Set Extraction:* Fingerprint pattern is made up of valleys and furrows. First step is to take an image of fingerprint pattern through an acquisition device. After capturing image of fingerprint there are several steps required to follows to extract desired feature set and these steps are as follows: acquisition process, image enhancement process, ridges extraction process thinning process and extract minutiae points as shown in Fig. 5 [28]. Quality of ridges pattern can be increase by enhancement process so that minutiae point extraction can be easily done. Enhanced image is binarized and then apply thinning algorithms to reduce the thickness of the ridges to one pixel for precise ending. Minutiae point localization can be start with process fingerprint image. Ridges endings and bifurcation is used as minutiae points in processed image.The matching process is consists of findings alignment between input minutiae set and template and gives maximum no. of minutiae pairing [29].

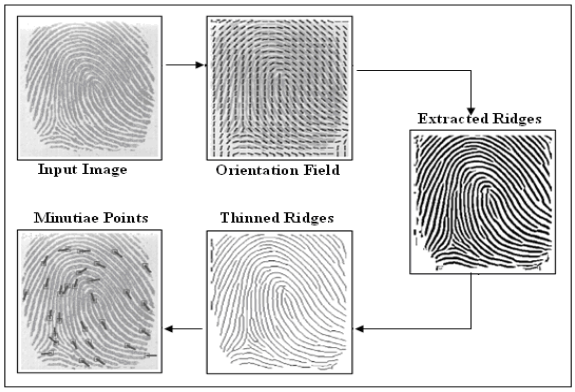

Fig. 5.Fingerprint feature set extraction process

B. Architecture of Proposed System

Proposed multimodal biometric system architecture is shown in figure 6. Proposed system integrates FKP, face and fingerprint at matching score level. Biometric recognition system of FKP, face and fingerprint consists of four phases e.g. image capturing, feature set extraction, matching and decision making. Initial step is to acquire the raw image or data of the authorized person with the help of appropriate sensors. After then corresponding feature extraction module is used to process these raw images and generate biometric templates. These templates are matchedwith the templates already stored in the database with the help of matcher module.Match scores of these biometrics are fed to the fusion module for further process.Now, an appropriate SVM choose by fusion module to carry out further fusion process depending upon the individual biometrics matching score. Fused matching score will be generated by the chosen SVM with the helpofavalaible matching scores of biometrics. Fused score then passed to the decision module for final result. Fixed threshold used by decision module to declare a person as genuine or not genuine.

- *Score normalization:* Let us suppose that matching scores generated by MS_{FKP}, MS_{face} and $MS_{finger}$are the matching scores generated by FKP, face and finger print biometrics respectively. Sum rule fusion technique is used to integrates FKP, face and finger print at matching score level. Score normalization is the primary step involved in biometric fusion. All biometric produced heterogeneous matching score output because geometrical range of all are different. So, a normalization technique is needed to transform matching scores into common range. Min-max normalization technique is used to normalize the match score and transform the all match scores into common domain or range [0, 1]. The matching scores output of every input modality has different numerical range [30]. So, Min-Maxtechnique is applied to convert the matching scores in to domain of [0, 1]. Following equations are used to generate normalized match score [30]:

$$N_{FKP} = \frac{MS_{FKP} - \min_{FKP}}{\max_{FKP} - \min_{FKP}}$$

$$N_{face} = \frac{MS_{face} - \min_{face}}{\max_{face} - \min_{face}} \quad (1)$$

$$N_{finger} = \frac{MS_{finger} - \min_{finger}}{\max_{finger} - \min_{finger}}$$

The minimum and maximum match scores for FKP, face and finger print biometrics are [$mini_{FKP}$, max_{FKP}], [min_{face},max_{face}] and [min_{finger}, max_{finger}]respectively.

The normalized match scores of FKP, face and finger print biometrics $N_{FKP,}N_{face}$ and $N_{finger}$are respectively.

- *Fusion strategy:* Multiple parallel SVMs based fusion strategy is used after score normalization. This fusion strategy overcomes the problem of missing biometric modality. It integrates FKP, face and finger print biometric modalities. Possible combinations of these modalities are{FKP, face}, {FKP, finger print}, {face, finger print}, {FKP, face, finger print}. According to these combinations, four SVMs are used (one for each combination) as shown in Fig. 6. An appropriate SVM is selected depending upon the currently available biometric modalities.

Simple sum rule [30] is used to combine the match scores generated by different matchers and its formula is given below:

$$MS_{final} = \sum_{i=1}^{m} N_i \quad (2)$$

Where, N_i is normalized match score of i^{th} biometric modality, value of i can be 1 to m according to the currently available modalities.

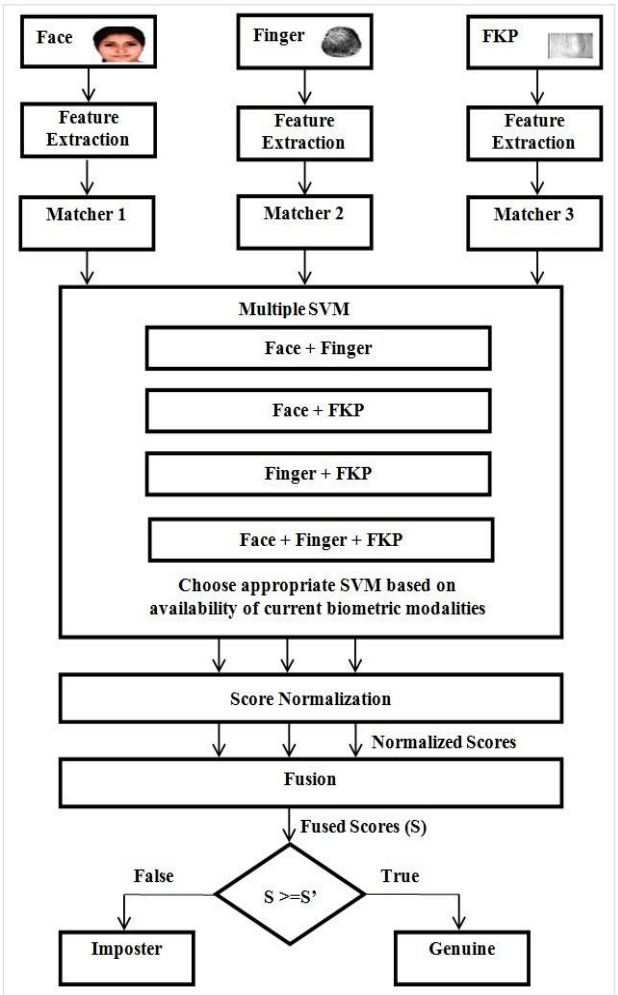

Fig. 6.Proposed multimodal biometric system integrating Face, Fingerprint and FKP

Hence, the chosen SVM perform the fusion of currently available biometric modalities and generates the final matching score (MS_{final}). The authenticated person is accepted as genuine person, if the match scores are greater than decision threshold. And, the authenticated person is rejected as imposter, if match scores is less than decision threshold.

IV. RESULTS AND DISCUSSION

A robust multimodal biometric system is presented in this paper that integrates FKP, face and fingerprint. Matching score level fusion is carried out on these three biometric modalities. Final decision is generated by multiple SVMs based fusion technique.Effectiveness of the proposed fusion strategy is evaluated with the help of MATLAB. The sample data for FKP was taken from PolyU database [31] andface and fingerprint data was taken from NIST website [32]. Multiple parallel SVMs based fusion strategy is used to overcome the problem of existing multimodal biometric fusion techniques. Existing techniques assumes that all the biometric modalities are available at time of authentication. These techniques have some flexibility problem as these are not able to add new biometric modality to the system. This process will require biometric data to be gathering for biometric modality from all the registered persons in the system.This will change the entire architecture of the system. In contrast to these systems, a flexible multiple parallel SVMs based fusion strategy is used. New modality can be easily added without effecting already registered persons in the system and the existing SVMs.For the new combination of modalities, a new SVM can be added to existing fusion module.

Receiver Operating Characteristic (ROC) curve is used to represent the performance of the system. A ROC curve is plotted between FAR (False Accept Rate) and GAR (Genuine Accept Rate) for different decision threshold values [2]. FARis the percentage of unauthorized persons whose matching score is equal to or greater thandecision threshold and GAR is the percentage of authorized persons whose matching scores is more than threshold and FRR (False Reject Rate) is the percentage of authorized personswhose matching scores is less than decision threshold. The ROC curve is the trade-off between FAR and GAR or FRR. The point where FAR=FRR on ROC curve is called EER (Equal error rate) point. This point indicates that false acceptance is equal to false rejections. Accuracy of the system is dependent on the EER. Lower the value of EER, higher will be the accuracy of the system.ROC curves for the multimodal biometric system are shown in the Fig. 7. Four ROC curves corresponding to the four combinations of the biometric modalities are shown in Fig. 7. One ROC curve is corresponding to the fusion of FKP, face and finger print with EER=0.19% and other three curves are corresponding to the cases where one of the biometric modality is missing with 1.1%, 0.42% and 0.54% respectively. The performance corresponding to the missing cases is slightly worse than the case where all the biometric modalities are available. But the multiple parallel SVMs based fusion strategy overcomes the problem of missing biometric modality. Hence, multiple SVMs based system is more realistic or flexible than most of the existing systems which requires that all biometric modalities must be present at the time of authentication.

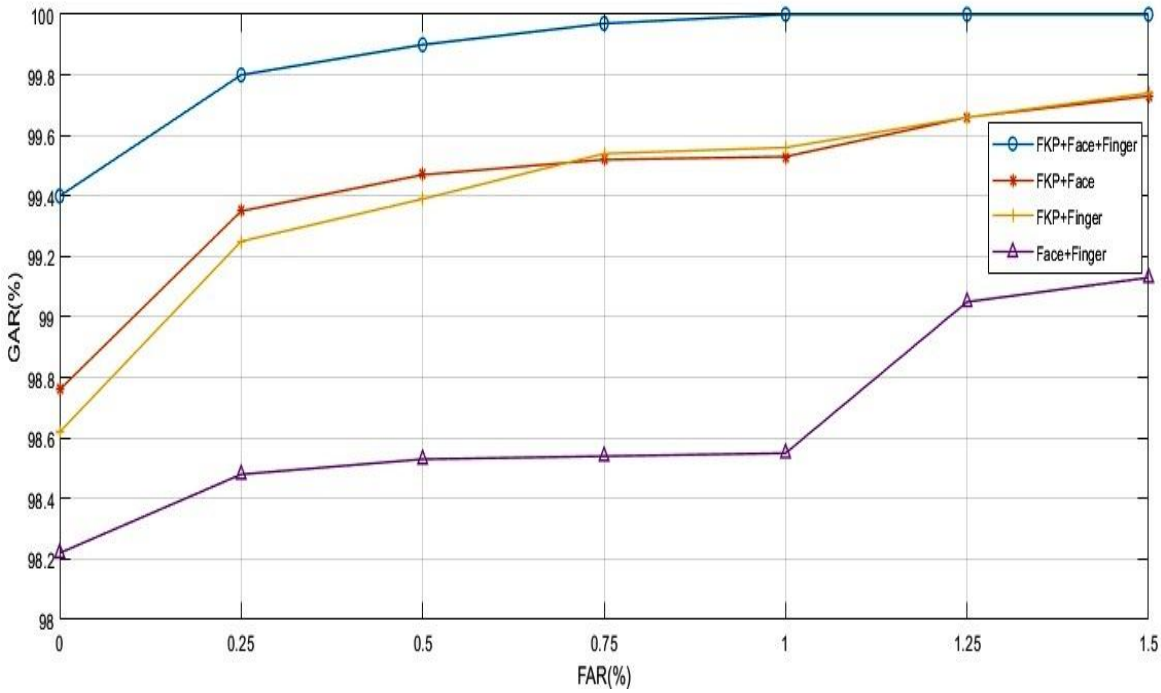

Fig. 7.ROC curves for proposed system

The average accuracy of SVMs is described in the Table 1. The SVM corresponding to {Face, Finger} has the lowest average accuracy because both biometric modalities are less reliable than FKP. And SVMs that include FKP has better accuracy. Fig. 8 shows the bar chart which represents the accuracy of different SVMs.

Table I. Accuracy of all SVMs

Modalities		***Accuracy***
A	SVM for {FKP, Face, Finger}	99.85
B	SVM for {FKP, Face}	99.43
C	SVM for {FKP, Finger}	99.04
D	SVM for {Face, Finger}	97.72

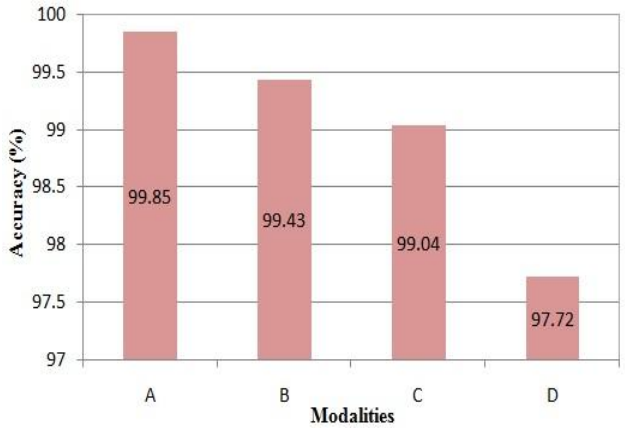

Fig. 8.Bar chart showing accuracy of each SVM

Multimodal systems achieves better accuracy and more reliable than unimodal systems. The proposed multiple parallel SVMs based fusion strategy is more robust, realistic and retain high average accuracy when any biometric modality is not available at the time of authentication.

V. CONCLUSION

This paper presents a robust multimodal biometric system which addresses the limitation of missing biometric modality. This system fuses the three biometric modalities (FKP, face and fingerprint)at the match score level.Multiple parallel SVMs based fusion strategy is applied in the proposed system. All possible combinations of available biometric modalities are taken into consideration. There is an appropriate SVM corresponding to each case or combination. In contrast, existing multimodal systems assumes that all the biometric modalities should be present at authentication time. If the biometric modality is missing at authentication time, the accuracy of the systems greatly degrades. Thus, the proposed multimodal fusion strategy overcome the problem of existing system by using multiple parallel SVMs. Experimental result also shows that this fusion strategy is more realistic, robust, flexible and fault tolerant.Future work will involve the integration ofliveness detection with the multimodal biometric recognition systems since it will increase the security requirements of the systems.

VI. REFERENCES

1. A. Ross and AK. Jain, **"**Multimodal Biometrics: An Overview",*appeared in Proceeding of 12th European Signal Processing Conference (EUSIPCO),* (Vienna, Austria), pp. 1221-1224, September 2004.
2. A.K. Jain, A. Ross, S. Prabhakar, "An Introduction To Biometric Recognition", *IEEE Transactions on Circuitsand Systems for Video Technology*, vol.14, pp. 4-20 2004.
3. A K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, JUNE 2006.
4. C. Sanderson and KK. Paliwal, "Information Fusion and Person Verification Using Speech and Face, Information", *IDIAP*, September 2002.
5. A. Ross. and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", *In Proceedings of SPIE Conference on Biometric Technology for Human Identification II.*, vol 5779, pp. 196–204, Orlando, USA, March 2005.
6. A.K. Jain, A. Ross, "Multibiometric systems, Communications of the ACM", *Special Issue on Multimodal Interfaces*, vol. 47, pp. 34-40, January 2004.
7. L. Hong, A. Jain & S. Pankanti, "Can Multibiometrics Improve Performance", *Proceedings of AutoID 99*, pp. 59-64, 1999.
8. G. Feng, K. Dong, D. Hu and D. Zhang, "When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy in Biometric Authentication", vol. 307, 2004.
9. Gian Luca Marcialis and Fabio Roli, "Serial Fusion of Fingerprint and Face Matchers", *M. Haindl, Springer-Verlag*, vol. 4472, pp. 151-160, Berlin Heidelberg 2007.
10. A. Meraoumia, S. Chitroub and A. Bouridane, "Fusion of Finger-Knuckle-Print and Palmprint for an Efficient Multi-biometric System of Person Recognition", *IEEE ICC* 2011.
11. Kartik.P, S.R. MahadevaPrasanna and Vara.R.P, "Multimodal biometric person authentication system using speech and signature features," *in TENCON 2008 - 2008 IEEE Region 10 Conference*, pp. 1-6, 2008.
12. Rodriguez.L.P, Crespo.A.G, Lara.M and Mezcua.M.R, "Study of Different Fusion Techniques for Multimodal Biometric Authentication," in Networking and Communications", *IEEE International Conference on Wireless and Mobile Computing*, 2008.
13. D. Kisku, P. Gupta and J. Sing, "Multibiometrics Feature Level Fusion by Graph Clustering", *International Journal of Security and Its Applications*, vol. 5, no. 2, April, 2011.
14. Toh.K.A, J. Xudong and Y. Wei-Yun, "Exploiting global and local decisions for multimodal biometrics verification," *Signal Processing, IEEE Transactions on Signal Processing*, vol. 52, pp. 3059-3072, 2004.
15. J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez Rodriguez, " A comparative evaluation of fusion strategies for multimodal biometric verification," *in Proc. 4th Int, Conf,Audio-video-based Biometric Person Authentication* , J. Kittler and M. Nixon, Eds., vol. 2688, pp. 830–837, 2003.
16. S. Viriri and R. Tapamo, "Integrating Iris and Signature Traits for Personal Authentication using User-Specific Weighting", 2009.
17. M. Kazi and Y. Rode, "Multimodal Biometric System using Face and Signature: a score level fusion approach," *Advances in Computational Research*, vol. 4, no. 1, 2012.
18. AAboshosha and A Kamal, "Score Level Fusion for Fingerprint, Iris and Face Biometrics", *International*

Conference on Pattern Recognition and Image Analysis, 2015.
19. S Chaudhary and R Nath, "A Robust Multimodal Biometric System Integrating Iris, Face and Fingerprint using Multiple SVMs", *International Journal of Advanced Research in Computer Science*, vol. 7, no. 2, pp. 108-113, 2016.
20. KVishi and V Mavroeidis, "An Evaluation of Score Level Fusion Approaches for Fingerprint and Finger-vein Biometrics", *Norwegian Information Security Conference, Oslo Norway*, Nov 2017.
21. K Shinde and S Tharewal, "A Study of Multimodal Biometric Person Identification System Using Face, Fingerprint and Iris", *International Journal for Research in Engineering Application & Management (IJREAM)*, pp. 51-54, 2018.
22. S Neware et.al. "Finger Knuckle Surface Biometrics", *International Journal of Emerging Technology and Advanced Engineering*, vol 2, no. 12, pp 452-455, 2012.
23. Kong et al.,"A hierarchical classification method for Finger Knuckle Print recognition", *EURASIP Journal on Advances in Signal Processing*, 2014, http://asp.eurasipjournals.com/content/2014/1/44.
24. DirkColbry, George Stockman, and Anil Jain, "Detection of Anchor Points for 3D Face Verification", 2009.
25. M. Turk and A. Pentland, "Eigenfaces for recognition," *Journalof Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, Mar. 1991.
26. S. Chaudhary, R. Nath, "A Multimodal Biometric Recognition system Based on Fusion of Palmprint, Fingerprint and Face," *In Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, IEEE Xplore*, pp. 596-600, October 2009.
27. Lu, X.; Wang, Y. & Jain, A.K., "Combining Classifiers for Face Recognition," *In IEEE Conference on Multimedia & Expo*, vol. 3, pp. 13-16, 2003.
28. L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Patt. Anal. Machine Intell.*, vol. 20, pp. 777-789, Aug. 1998.
29. A.K. Jain, S. Prabhakar, and L. Hong, "A multichannel approach to fingerprint classification," *PAMI*, vol.2, no. 1, pp. 348–359, 1999.
30. A. K. Jain, K. Nandakumar, & A. Ross, "Score Normalization in multimodal biometric systems," *The Journal of Pattern Recognition Society*, vol. 38, no. 12, pp. 2270-2285, 2005.
31. PolyU FKP Database., available at: http://www.comp.polyu.edu.hk/~biometrics/FKP.htm.
32. National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

VII. AUTHORS PROFILE

Ms. Komal is a research scholar in the Department of Computer Science & Applications, K.U., Kurukshetra, Haryana, INDIA. Her research interests include Biometrics Security, Multimodal Biometrics.

Dr. Chander Kant is working as assistant professor in the Department of Computer Science & Applications, K.U., Kurukshetra, Haryana, INDIA since 2004. He received his Doctorare Degree in the field of Biometrics form Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana, INDIA. His research interests include Biometrics Security, Cloud Computing, Data Mining and Warehousing, Web Technologies. He has published more than 120 publications in various International/ Nationals Journals and Conferences. Dr. Kant has also completed One UGC- Project during 2011-2013. He has also received National Excellence Award; "Educationist of the Year-2017" by National Institute for Education & Research, New Delhi, on 23rd Sept. 2017.