A Novel Serial Multimodal Biometric Framework Based on Mixture Models

Manas Kumar Choudhury, Dr.Y Srinivas

Abstract— **This article contributes towards the study of multimodal biometric system against spoof attacks. Much of the works reported based on Parallel fusion, are subjected to the critics about the authentication, since spoofing of a single trait may lead towards the cracking of whole system. Validation of the multimodal biometric systems in serial fusion mode against spoofing is still a matter of research.. In this paper, we make an attempt to study the affect of spoofing in serial fusion mode. The concepts of fusion together with Generalized Gamma Distribution (GGD) are utilized. The performance of the model is evaluated using synthetic data and evaluation is carried out by considering metrics like False Acceptance Rate (FAR), Acceptance Rate, and False Rejection Rate (FRR).**

Index Terms— **Multimodal biometric, Serial Fusion, Spoofing, Generalized Gamma Distribution (GGD), FAR, FRR.**

I. INTRODUCTION

Biometrics is a precise methodology for establishing the uniqueness of an individual using their physiological or behavioral templates such as face, signature, fingerprint and so on. Biometrics is now widely accepted and deployed in almost all the Public and Private Sectors, to increase the security levels and counter attack security threats. Each biometric templates extracted from an individual's is believed to satisfy some of the features namely, universality, suitability and non-forgability [1], [2]. Most of the literatures in uni modal biometrics have showcased various mechanisms adopted by invaders to attack the biometric systems using the strategies like stealing, duplicating, detaining and replicating the biometric templates [3-7]. This sort of attacking the system, by creating duplicate biometric templates for the corresponding input is acknowledged as spoofing attack. Amid various advantages, certain issues that rise about the usage of biometric are related to flexibility and spoofing attacks**.** Spoofing attacks are also referred to as "direct attacks". To spoof a system, the impostors need not possess any technical knowledge or does not require precise details about the biometric system. Multimodal biometric systems are considered to be more robust than uni modal systems and many researchers have shown that these systems are capable of withstanding the spoofing attacks. The basic theory behind this consideration is that dodging multiple systems is more difficult than dodging a single system. There are two approaches in which the multimodal systems are operated, the serial fused mode and parallel fused mode.

Serial fused systems are considered to be more robust than parallel mode multimodal systems [8], [9], [10] to evade multiple traits connected serially, it is necessary to evade all the fused individual systems simultaneously.

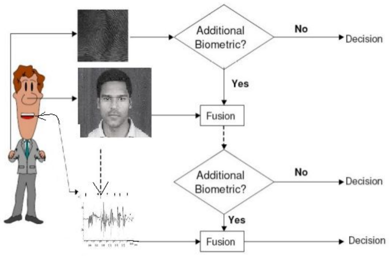

Fig-1 Serial Architecture

Multimodal systems fuse various biometrics either using Fusion prior to matching or fusion after matching. In fusion prior to matching approach, the integration of the information is considered either at sensor level or feature level. These approaches are less preferred as integrating non- homogenous traits is difficult and also concatenation of two feature vectors may lead to huge dimension which leads to curse of dimensionality problem. Hence in this paper we have considered Fusion after matching where abstract decisions based on concept of score level fusion can be arrived based on majority voting, AND - OR Rule based and Rank based decisions. In this article, traits of the finger-print, speech, and face templates fused. The features are obtained using the PDF of GGD and Mel Frequency Cepstral Coefficients (MFCC) from speech signal. The evaluation of the developed method is carried out using metrics like FAR (False Acceptance Rate) and FRR (False Rejection Rate). The organization of the paper is as follows.Section-2, of the paper deals with Generalized Gamma Distribution. In Section -3, extraction of biometric traits and feature vectors are discussed.Section-4 of the paper deals with Normalization. In the section-5, experimentation together with the results is presented. Evaluation Metrics together with conclusions are presented in section -6.

II. Generalized Gamma Distribution (GGD)

In this paper generalized gamma distribution is considered distinguishing a impostor and genuine traits. The main motto behind the consideration of GGD is that, the biometric traits considered will be non-homogenous and asymmetric in nature. Therefore, to cater these multiple patterns, it is needed to consider a model which is asymmetric, such as GGD (generalized gamma distribution) as it can handle data both in symmetric and asymmetric features.

Manuscript received Jan 20, 2015

Manas Kumar Choudhury, Assistant Professor, Department of Information Technology, Gitam Institute of Technology, Gitam University, Visakhapatnam, Andhra Pradesh, India

Dr. Y Srinivas, Professor, Department of Information Technology, Gitam Institute of Technology, Gitam University, Visakhapatnam, Andhra Pradesh, India

The PDF (Probability Density Function) of Generalized Gamma Distribution (GGD) is given

$$f(x,k,c,a,b) = \frac{c(x-a)^{ck-1} e^{-\left(\frac{x-a}{b}\right)^{c}}}{b^{ck}\Gamma(k)} \text{ ----- (1)}$$

III. Extraction of Biometric Traits

In this article we have measured the biometric templates of face, fingerprint and speech signal for the validation procedure. For the authentication purpose, each of these templates is matched against the templates in the database. The finger print extract is given to GGD as input, MFCC values are considered for extraction of amplitude sequences from the speech signals and pixels of the facial data are given as input to the GGD to extract the PDF. These features are fused using a score level fusion, which is a uses a Logical AND/ OR operation the match is indicated as ‘Y’, and mis-match by ‘N’. The confirmation process is based on the value returned.

IV. Normalization

A normalization step is usually needed before the raw scores derived from different traits are combined in the fusion stage. To distinguish the impostor and genuine individual, normalization of the scores becomes a mandate. The Min-Max (NM) concept of normalization is used in this paper. This method maps the raw scores to the [0, 1] range. Max(S) and Min(S) specify the end points of the score range (M. Indovina et al (2003)) and are calculated using the formula

$n = (s-\min(S)) / (\max(s)-\min(S))$ --- (2)

Where, s = raw matching score and S = Set of all scores for a matcher

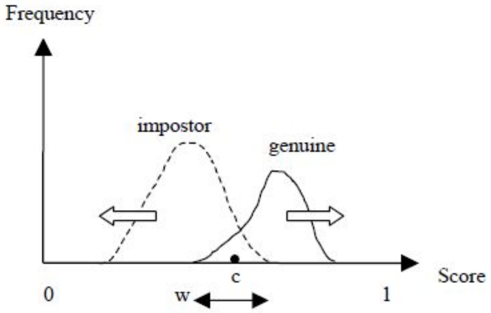

Fig-2 , Overlap of Impostor and Genuine traits

V. Experimentation

In order to evaluate the model various inputs are considered both from gender dependent and gender independent data. The database consist of 100 fingerprint, 100 facial images and also consist of speech signals of the above 100 subjects. The preprocessing is done on each of the sample and feature vectors are extracted using the concept mentioned in section-3 of the paper. The core features are extracted from each of these biometric inputs and are stored in the database. In order to extract the speech signal, each of the subject‘s speech data is recorded in .WAV format and are given as input to the MFCC for extracting the amplitude signal. MATLAB voice box is considered for the extraction of these amplitude signals. For the extraction of facial features, each face is normalized into a unit square. Preprocessing is subjected to overcome lightening or illusion effects and orientation is overcome by considering frontal face. These preprocessed faces are given as input to GGD and the PDF is obtained by using the formula given in section-2. Using the MATLAB Environment these features are fused using score level fusion, as discussed in section-4 of this paper. The various input and outputs are presented in following figures1,2 and 3.

Performance Evaluation and Conclusion

In this paper the concept of multilevel fusion is considered for authentication of a person and ensures security from private and public data. In order to evaluate the current methodology we have considered metric like FAR (False Acceptance Rate), FRR (False Rejection Rate) and Acceptance Rate. The formula for computing is given below:-

MDR= (Total No of Missed Recognition/Total Template)*100

FAR= ((Total Considered-Total Accepted)/Total Template)*100

Acceptance Rate = (Total no of Accepted Traits/Total Traits)*100

Table Showing the Performance of Proposed Model

Biometric Traits	***Technique Adopted***	***Performance of Classification in Percentage (in Serial Mode)***				***Performance of Classification in Percentage(In parallel Mode)***			
		FAR	***FRR***	***ACC RATE***	***No. of subjects***	***FAR***	***FRR***	***ACC RATE***	***No. of subjects***
FACE + Speech+ Finger Print	GMM	1.89	6.97	81	100	2.12	7.61	75	100
	Proposed Model	1.73	6.00	94	100	2.01	6.05	87	100

In this article the concept of multimodal biometric verification is considered for authentication of an individual. This paper presents a novel methodology for establishing the identity of individual by using the concept of GGD (Generalized Gamma Distribution) by applying serial as well as parallel mode of fusion. For uniform result the Normalized data is considered for verification of an individual against template. The performance is calculated evaluated using FAR/FRR both in serial as well as parallel mode and compared with the existing methodology of GMM (Gaussian Mixture Model) and is presented in the table. From the above table it can be clearly seen that the performance of the biometric systems using serial fusion using GGD (Generalized Gamma Distribution) performs far better compared to Parallel Mode.

References

[1] M. Indovina et al (2003), Multimodal Biometric Authentication Methods: A COTS Approach, Workshop on MMUA, December 2003,pp 1-8.

[2] [2] Serestina Viriri, Jules R. Tapamo,” Integrating Iris and Signature Traits for Personal Authentication Using User-Specific Weighting” Sensors 2012, 12, 4324-4338;

[3] Sona Aggarwal, Yogita Gulati, ”A Multimodal Biometric System Using Fingerprint and Face” International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012

[4] Mahdi Hariri, Shahriar B. Shokouhi,” Robustness of Multi Biometric Authentication Systems against Spoofing” Computer and Information Science Vol. 5, No. 1; January 2012

[5] Shubhangi Sapkal,” DATA LEVEL FUSION FOR MULTI BIOMETRIC SYSTEM USING FACE AND FINGER “nternational Journal of Advanced Research in Computer Science and Electronics Engineering, Volume 1, Issue 2, April 2012

[6] Rashmi Singhal, Payal Jain,” MULTI-BIOMETRIC SYSTEMS: SECURE SECURITY SYSTEMS”, IJREAS Volume 2, Issue 2 (February 2012).

[7] R. Gayathri, P. Ramamoorthy,” Feature Fusion of Palmprint and Face Biometrics” European Journal of Scientific Research Vol.77 No.4 (2012), pp.457-470

[8] R.Gayathri, P.Ramamoorthy,” Multifeature Palmprint Recognitionusing Feature Level Fusion “International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2,Mar-Apr 2012, pp.1048-1054

[9] M. P. Dale, M. A. Joshi, H. J. Galiyawala,” A Single Sensor Hand Geometry and Palm Texture Fusion for Person Identification” International Journal of Computer Applications ,Volume 42– No.7, March 2012

[10] Rashmi Singhal , Narender Singh, Payal Jain,” Towards an Integrated Biometric Technique “International Journal of Computer Applications Volume 42– No.13, March 2012.

[11] Sonam Shukla, Pradeep Mishra,” A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits” International Journal of Soft Computing and Engineering (IJSCE) Volume-2, Issue-1, March 2012

[12] Ross and A.K. Jain, “Information Fusion in Biometrics”, Pattern Recognition Letters, 24, pp. 2115-2125, 2003.

[13] S. Singh, G. Gyaourova and I. Pavlidis, “Infrared and visible image fusion for face recognition”, SPIE Defense and Security Symposium,pp.585-596, 2004

[14] Patrick Verlinde, G´erard Chollet,” Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application” CNRS URA-820 ,Ecole Nationale Sup´erieure de T´el´ecommunications/TSI Department ,F75634 Paris, France,1999

[15] Ross, A.; Jain, A.K. Information fusion in biometrics. Pattern Recogn. Lett. 2003, 24, 2115–2125.

[16] ArunRoss and RohinGovindarajanb, “Feature Level Fusion Using Hand and Face Biometrics”, SPIE Conference on Biometric Technology for Human IdentificationII, Volume, 5779, pp.196-204(Orlando, USA) March 2005.

[17] Shyam Sunder Yadav, Jitendra Kumar Gothwal, Prof. (Dr.) Ram Singh” Global Journal of Computer Science and Technology” Volume 11 Issue 16 Version 1.0 September 2011

[18] N. K. Ratha,J. H. Connell,R. M. Bolle,” Enhancing security and privacy in biometrics-based authentication systems” BM SYSTEMS JOURNAL, VOL 40, NO 3, 2001.

[19] B.Prasanalakshmi, A.Kannammal, R.Sridevi,” Multimodal Biometric Cryptosystem Involving Face,Fingerprint and Palm Vein” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[20] Mingwu Zhang , Bo Yang, Wenzheng Zhang, Tsuyoshi Takag,” Multibiometric Based Secure Encryption and Authentication Scheme with Fuzzy Extractor” International Journal of Network Security, Vol.12, No.1, PP.50–57, Jan. 2011

[21] H. Vajaria, T. Islam, P. Mohanty, S. Sarkar, R. Sankar, R. Kasturi,” Evaluation and analysis of a face and voice outdoor multi-biometric system” Pattern Recognition Letters 28 (2007) 1572–1580

[22] Sanderson, C., Paliwal, K., 2002. Information fusion and person verification using speech and face information. IDIAP-RR. 02-33.

[23] Brunelli, R., Falavigna, D., 1995. Person identification using multiple cues. IEEE Trans. Pattern Anal. Machine Intell. 10, 955–966.

[24] Ribaric, S., Fratric, I., 2006. Experimental evaluation of matching-score normalization techniques on different multimodal biometric systems. In: IEEE Mediterranean Electrotechnical Conf., pp. 498–501