DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4351

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ANALYSIS OF SPOOFING ROBUSTNESS IN A MULTIMODAL BIOMETRIC SYSTEM

Sukhchain Kaur and Reecha Sharma
Department of Electronics and Communication,
Punjabi university Patiala,India

Abstract: As modern means of communication upgrade in their potential and receptiveness, they instigate additional demands in terms of security. Biometric recognition is a new technology that has become the essence of an extensive array of highly secure identification and personal verification solutions. Unimodal biometric system suffers from inherent limitations of noise in sensor data, non universality of biometric trait, intra-class variations and unaccepted error rates. Multimodal biometric system overcome all these limitations by presenting multiple evidences of single biometric trait due to which spoofing of these simultaneously become more difficult for an imposter. In this paper, face and fingerprint are the two biometrics used to build multibiometric system. Here, fusion of two modalities is done at matching score level. An experimental result shows that the Multimodal biometric system is efficient compared to unimodal biometric system.

Keywords: Multimodal Biometrics, Anti-spoofing, Biometric feature extraction, Biometric score fusion.

1. INTRODUCTION

As modern means of communication upgrade in their potential and receptiveness, they instigate additional demands in terms of security. A wide variety of systems need reliable personal recognition schemes to either validate or determine the identity of a creature requesting their services. The prospect of such schemes is to guarantee that the rendered services are gathered only by a legitimate user and no one else. Examples of such applications comprise secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the lack of robust personal recognition schemes, these systems are vulnerable to the wiles of a deceiver. Biometric recognition is a new technology that has become the essence of an extensive array of highly secure identification and personal verification solutions [1]. By using biometrics, it is feasible to validate or authenticate an individual's identity based on "who you are," rather than by "what you have" (e.g., an ID card) or "what you know" (e.g., a password). The principal advantage of biometric systems as compared to other conventional identification systems is that it is the most secure and convenient authentication tool as passwords can be easily divulged using dictionary attacks [2], and ID cards can be shared, stolen, or borrowed by an impostor to acquire unauthorized ingress, thus counterfeiting system security. Since person is requisite to be existent at the time of authentication by the biometric system thus anticipating false abjuration claims.

Systems which incorporate evidences from two or more biometric systems in order to precisely recognize the identity of a person are known as multimodal biometric systems [3]. Such systems are more reliable for recognition purposes as they combine multiple independent pieces of information. Also some of the limitations caused by a given biometric trait are compensated by other traits [4]. These systems are less vulnerable to spoofing, as the user is required to present random subset of biometric traits in order to ensure that a "live" user is indeed present at the time of recognition. So, it becomes difficult for an intruder to simultaneously spoof multiple biometric traits of a legitimate user [5].

2. RELATED WORK

A carefully accomplished combination scheme, that has been trained and tested on a large amount of data, is believed to personate better than the best of the individual ingredient traits [6]. Further, a combination of uncorrelated modalities (e.g., fingerprint and face or two fingers of a person) is anticipated to result in a greater improvement in efficacy than a combination of correlated modalities (e.g., different impressions of the same finger or different fingerprint matchers). Further, a good overview of feature extraction techniques for face and fingerprint anti-spoofing techniques is found in [7]. Fusion at the match score level has been adequately studied in the [8],[9] ,[10] ,[11] ,[12] and is considered most robust level of fusion in multimodal biometric systems, due to ease in procuring and combining the match scores. Therefore, we also adopted fusion at the match score level.

Also, in [13] proposed a novel median filtering fusion rule, for multi-finger spoofing scenario. For liveness detection, features extracted from traits are given to multiple classifiers which enhance the GAR of the system. Results clearly indicate how scores in multi-spoofing scenario degrade if m out of n fingers were spoofed.

In subsequent work, they extended their investigation to real spoof attacks [14] where m out of n biometric traits to be combined was spoofed. The traits to be used to develop robust multimodal system were face and fingerprint. Face features are extracted using LBP whereas fingerprint features are extracted using Gabor filters, GLCM and Fourier transform. Experimental results showcase that the GAR (genuine acceptance rate) curve was deliberately

decreasing with increase in number of added spoofed traits to the database, provided EER between 0.47-1.81% .

3. SYSTEM MODEL

The architecture of a multimodal biometric system composed of a face and fingerprint modality is shown in Figure 1. The modules in the system are Feature Extraction, Classification and Score Fusion. The proposed system extracts different type of feature from each biometric trait.

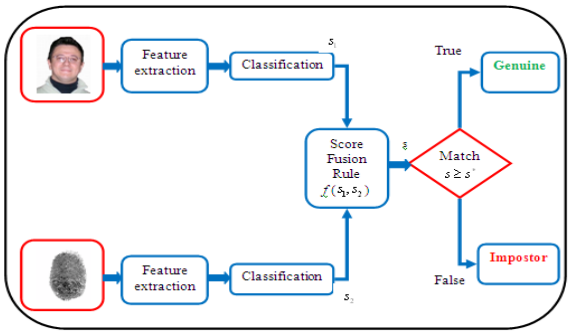

Figure 1: Multimodal biometric system composed of Face and Fingerprint modalities, whose match scores are combined using a fusion rule

In Feature Extraction, LBP (Local Binary Patterns) is used to extract features from the face biometric input. LBP's provide micro-texture analysis as it is powerful means of texture description and among its properties in real-world applications are its discriminative power, computational simplicity and tolerance against monotonic grey-scale changes [15].

And GLCM (Gray Level Co-occurrence Matrix), FT (Fourier Transform) and Gabor features are extracted from the fingerprint biometric input. Textural measures based on gray level co-occurrence matrix (GLCM) are adopted to characterize fingerprint texture. This is based on structural, orientation, roughness, smoothness and regularity differences of various regions in a fingerprint image [16]. The Fourier spectrum of ridge-valley texture in a fingerprint provides a ring pattern around the center. The amplitudes of these rings produced by live and fake fingerprint are different in spatial frequency bands in order to differentiate between the live and the fake fingerprints [17]. Further, Gabor wavelets are used to describe micro-textures as well as macroscopic information [18].

In Classification, multiple classifiers such as SVM (Support Vector Machine), LR (Logistic Regression) and Multi-layer Perceptron are used for fingerprint classification and only LR classifier is used for face biometric to classify the output as real or spoof.

The biometric traits are individually processed and correlated with the correspondent template of the claimed identity, thereby generating a real-valued match score (signified here as s_1 and s_2, respectively, for the face and the fingerprint matcher): larger the score, higher is the concordance.

Finally, the match scores are combined using a median filtering fusion rule [13] which then gives a resultant new real-valued score $f(s_1, s_2)$: the claimed identity is accepted, if $f(s_1, s_2) \geq s^*$; and the user is classified as a genuine and otherwise, the user classified as an impostor. The term s^* here is an acceptance threshold that is required to be declared in the course of design process according to application exactions in terms of false acceptance (FAR) and false rejection (FRR) rates.

4. EXPERIMENTAL RESULTS

The multimodal database used for the employed framework is CASIA Face Anti-Spoofing Database for face and Fingerprint Liveness Detection Competition 2015 for fingerprint. The database consists of 35 real and 5 spoofed samples of both the traits. The evaluation of the proposed multimodal biometric system is carried out using Receiver Operating Characteristics (ROC) by varying the system threshold η introducing the relationship between Genuine Acceptance Rate (GAR, the percentage of genuine users being accepted) and False Acceptance Rate (FAR, percentage of impostors being accepted). Here, m is the number of spoofed samples out of n total number of samples. In a similar manner (S)EER is referred to as the (Spoof) Equal Error Rate where GAR=FAR, provided lower the value of EER higher the accuracy of biometric system.

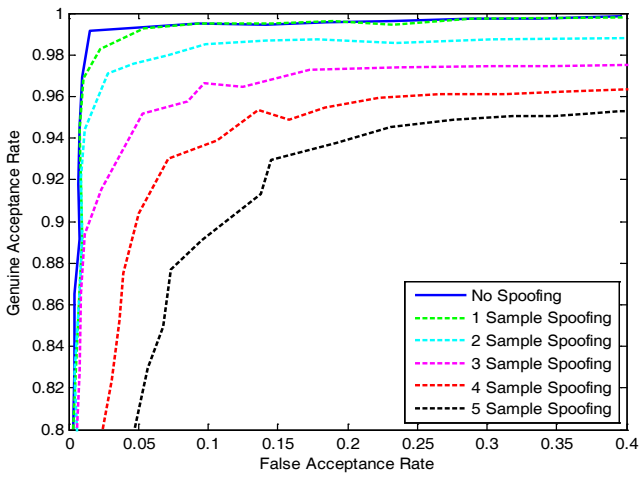

Figure 2: ROC for partial multibiometric spoofing using 1-median filtering rule

The overall reported EER in this case is 1.69% vs 1.81% in [14]. Corresponding curves of EER as a function of threshold used in fused score in case of median filtering rule are given by Figure 3.

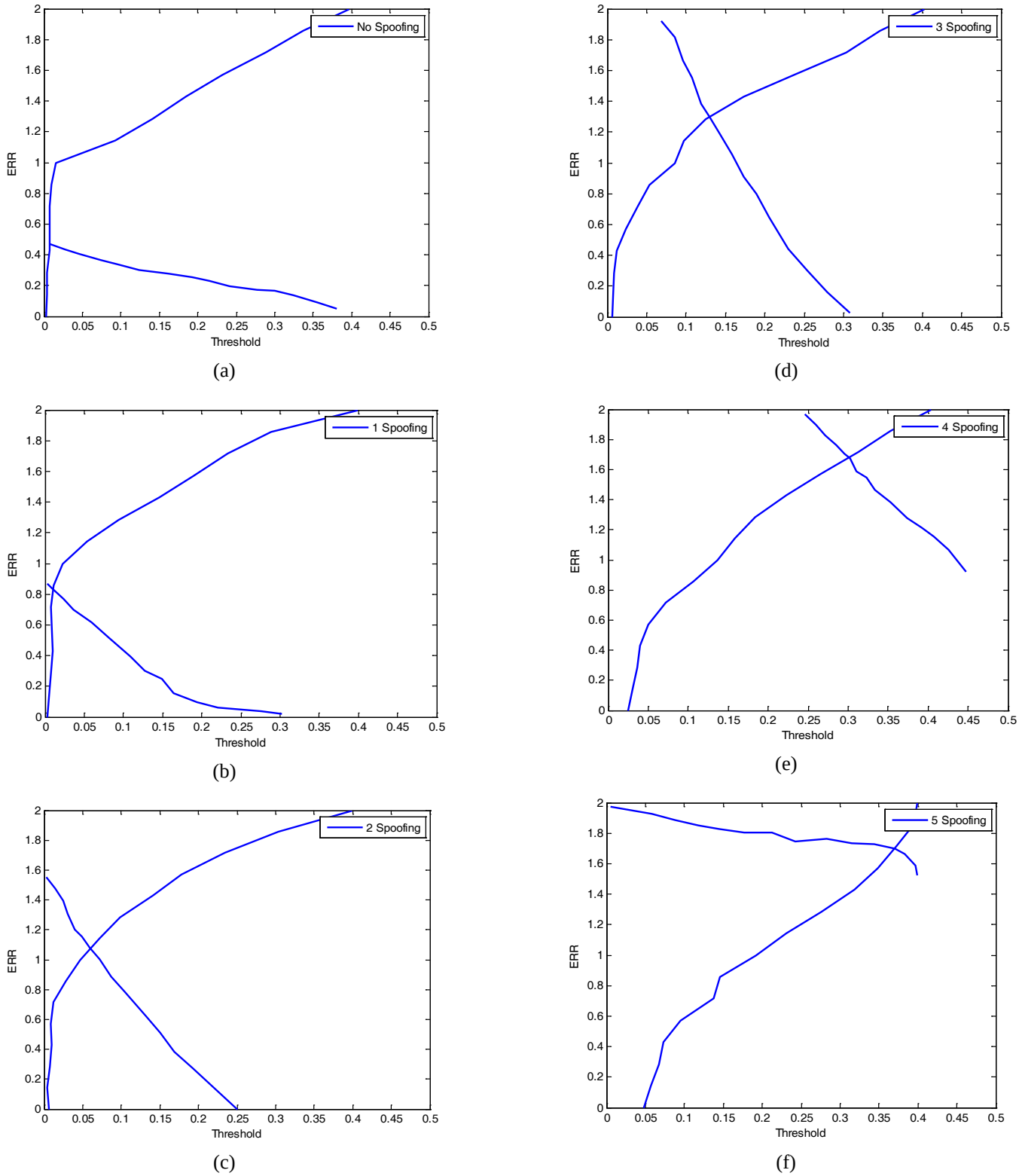

Figure 3: EER curves of face-and-finger fusion system on the test set varying the number m of spoofed samples where (m=0,1,2,3,4,5) for (a),(b),(c),(d),(e) and (f).

Table 1: EER results of face and finger fusion on the test set varying the number *m* of spoofed samples.

Number of Spoofed samples	EER (Equal Error Rate)
m =0	0.47
m =1	0.83
m =2	1.07
m =3	1.31
m =4	1.67
m =5	1.69

5. CONCLUSION

The security performance of the multimodal biometric system is evaluated by plotting EER curves of the system as a function of various threshold values to determine the point at which both FAR and FRR are equal. Lower value of EER indicates the capability of system to resist spoof attacks. The probability of imposter to circumvent the system increases with the increment in number of added fake samples of face and fingerprint modalities. In contrast to previous experiments on fusion of face and fingerprints, median filtering rule has shown to be even more successful in combining scores even though it comes at the cost of evidently degraded initial performance. In this paper, The GAR curve vary minimally with the increase in number of added fake samples of both the traits to the employed database which shows improved performance of median filtering rule.

6. REFERENCES

[1]. K. Jain, P. Flynn and A. A. Ross, Handbook of biometrics. Secaucus, NJ, USA: Springer-Verlag New York, Inc, 2007.

[2]. D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in Proceedings of the 2nd USENIX Security Workshop, 1990.

[3]. A.K. Jain, L. Hong and Y. Kulkarni, "A multimodal biometric system using fingerprint, face and speech," in Proceedings of 2nd Int'l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC, 1999.

[4]. L. Hong, A. K. Jain and S. Pankanti, "Can multibiometrics improve performance?," in Proceedings AutoID, 1999.

[5]. A.K. Jain and A. Ross, "Multibiometric systems," Communications of the ACM, vol. 47, pp. 34-40, 2004.

[6]. Z. Akhtar, "Security of multimodal biometric systems against spoof attacks," Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, vol. 6, 2012.

[7]. Sukhchain kaur, Reecha sharma, "A Survey on Anti-Spoofing Techniques for Face and Fingerprint Modalities", in International Journal of Emerging Technology and Advanced Engineering, vol. 7, no. 6,pp. 226-233, June 2017.

[8]. G. L. Marcialis and F. Roli, "Score-level fusion of fingerprint and face matchers for personal verification under" stress" conditions," in Image Analysis and Processing, 2007. ICIAP 2007. 14th International Conference on, 2007.

[9]. J. Fièrrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification," in Audio-and Video-based Biometric Person Authentication, 2003.

[10]. F. Roli, J. Kittler, G. Fumera and D. Muntoni, "An experimental comparison of classifier fusion rules for multimodal personal identity verification systems," Multiple Classifier Systems, vol. 2364, pp. 325-335, 2002.

[11]. R. N. Rodrigues, L. L. Ling and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," Journal of Visual Languages \& Computing, vol. 20, pp. 169-179, 2009.

[12]. R. N. Rodrigues, N. Kamat and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," in Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, 2010.

[13]. P. Wild, P. Radu, L. Chen and J. Ferryman, "Towards anomaly detection for increased security in multibiometric systems: spoofing-resistant 1-median fusion eliminating outliers," in Biometrics (IJCB), 2014 IEEE International Joint Conference on, 2014.

[14]. P. Wild, P. Radu, L. Chen and J. Ferryman, "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks," Pattern Recognition, vol. 50, pp. 17-25, 2016.

[15]. I. Chingovska, A. Anjos and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the, 2012.

[16]. S. B. Nikam and S. Agarwal, "Wavelet energy signature and GLCM features-based fingerprint anti-spoofing," in Wavelet Analysis and Pattern Recognition, 2008. ICWAPR'08. International Conference on, 2008.

[17]. C. Jin, H. Kim and S. Elliott, "Liveness detection of fingerprint based on band-selective Fourier spectrum," Information Security and Cryptology-ICISC 2007, pp. 168-179, 2007.

[18]. J. G. Daugman, "Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression," IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 36, pp. 1169-1179, 1988.