An Intelligent Approach for Anti-Spoofing in a Multimodal Biometric System

Sukhchain Kaur[1], Reecha Sharma[2]
[1]Department of Electronics and Communication,Punjabi university Patiala,India
[2] Department of Electronics and Communication,Punjabi university Patiala,India

Abstract- While multimodal biometric systems are considered to be more robust than unimodal ones but traditional fusion rules are more sensitive to spoofing attempts. The proposed system is designed to overcome spoofing in worst-case scenario where impostor was able to create fake biometric traits of both face and fingerprint modalities in the presented multimodal biometric system. The paper investigates median filtering fusion rule as a spoofing resistant alternative to traditional sum rule based fusion rules. Experiments on the latest face video database (CASIA Face Anti-Spoofing Database) and fingerprint spoofing database (Fingerprint Liveness Detection Competition 2015) illustrate that the given system is more robust to spoofing attacks than the existing anti-spoofing methods even when m out of n samples of both the biometric traits to be combined are attacked.

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

I INTRODUCTION

Multimodal biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. A combination of uncorrelated modalities (e.g., fingerprint and face or two fingers of a person) provides better performance than a combination of correlated modalities (e.g., different impressions of the same finger or different fingerprint matchers).

Among all the potential attacks, spoof attacks are the most crucial threats against the security of the biometric systems. A spoofing attack is a type of attack, where a stolen, copied biometric trait is submitted to the system to gain unauthorized access to the biometric system. This kind of attack is also called as “direct attack” since it is carried out directly on the biometric sensor. The feasibility of a spoof attack is much higher than other types of attacks against biometric systems as it does not require any knowledge of the system.

An anti-spoofing method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically forged version of the original biometric trait. Anti-spoofing is a challenging engineering task as it has to satisfy certain demanding requirements [1]: (*i*) non-invasive: these techniques should not be harmful or require an excessive contact with the user; (*ii*) user friendly: users should not be reluctant to interact with them; (*iii*) fast: results should be generated in a fraction of time as users' interaction with the sensor should be kept as short as possible; (*iv*) low cost: wide use cannot be expected if the cost is excessively high; (*v*) performance: in addition to a good fake detection rate, the protection scheme should not impair the recognition performance of the biometric system. From general perspective, anti-spoofing techniques[2] can be categorized into following three groups based on biometric system module in which they are integrated-

Sensor level techniques- These are also known as hardware based techniques. As these methods add some specific device to the sensor in order to detect particular properties of a living trait(e.g., facial thermogram, blood pressure, fingerprint sweat, or specific reflection properties of the eye). such techniques are integrated in the biometric sensor.

Feature level techniques- These are also known as software based techniques. Here, in these methods fake trait is detected after it has been acquired using standard sensor. Also features used to distinguish between live and fake trait are extracted from public available datasets usually images and not directly from the human body as in the case of sensor-level techniques. Such techniques are integrated after the sensor, usually functioning as part of the feature extractor module.

Score level techniques- These techniques are much lesser in common than previous two techniques. These techniques employ fusion strategies that increase their resistance to spoofing attempts.

In this paper, proposed method for anti-spoofing focuses on feature level techniques and score level techniques as they do not require additional hardware, faster, require lesser cooperation from the user and are less intrusive.

The rest of the paper is organized as follows: In Section 2, the literature survey on anti-spoofing techniques in multimodal biometric systems is described. The proposed work for anti-spoofing is discussed in Section 3. The experimental results are discussed in Section 4. The conclusion is presented in Section 5.

II RELATED WORK

2.1 ANTI-SPOOFING IN FACE AND FINGERPRINT RECOGNITION

In fingerprint recognition, basically there are two methods to address the problem of anti-spoofing either by actively accessing the liveness based on measuring properties like pulse, blood pressure, perspiration patterns or by passively analyzing patterns of spoofed traits like analyzing textural properties which are the most commonly used static features. However latter type is the subject of interest in this paper. A good overview of feature level fingerprint counter spoofing is found in [19]. And the most robust techniques that make use of texture based static features are Gabor wavelets [3], GLCM (Gray Level Co-occurrence Matrix) [4], Fourier Transform based features [5], LPQ (Local Phase Quantization) [6]. Moreover recent developments in unimodal biometric anti-spoofing involves collaboration of more than one feature extraction techniques and the fused features are then fed to multiple classifiers whose results are combined using advanced fusion techniques [7].

In face recognition, First method involves motion based counter measure to solve the problem of anti-spoofing which involves determining head movement of the user following a random path. Second method involves analyzing textural or statistical features which is the region of interest in this paper. An excellent recent survey of anti-spoofing methods in face recognition is found in [2]. Recent techniques in face counter-spoofing involves textural based features extracted using Local Binary Patterns(LBP)[8], Histogram of Oriented Gradients(HOG)[10], Gabor wavelets[9] and Difference of Gaussian Filters(DOG)[11].

2.2 ANTI-SPOOFING IN MULTIMODAL BIOMETRICS

Empirical evidences provided in [12, 13] confirmed that spoofing a single biometric trait drastically increase the probability to circumvent the multimodal biometrics system. Subsequently in [14] multimodal systems that combine two to four modalities and use several state of art score fusion rules can be evaded simply by using one or two fake biometric traits.

All the proposed countermeasures use score fusion rules and the simplest one [14] employ modifying the criterion for choosing the threshold on the fused score. Here, a multimodal database containing face, fingerprint, iris match scores from genuine and impostors were used. The sum fusion rule was considered.

In [12,13] a biometric system combining face and fingerprint modalities was considered. Both involve modification of existing fusion rules. In [12] LR and weighted sum were used as a score level fusion rules. Contrary to [12] similar results were found in [13] when trait to be spoofed was face and for fingerprint spoofing experiments were conducted using scores coming from real spoof attacks using dataset of fingerprint liveness detection competition 2009.

Also in [15] four different traits, one face and three fingerprints were considered. The LR and sum fusion rules were used. Moreover, they point out that the LR fusion rule was found to be more vulnerable than the simplest sum rule. In [16] we found that also multimodal systems using *serial* score fusion rules exhibit the same vulnerability.

Also, in [7] 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 [17] 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%

III PROPOSED WORK

The proposed system extracts different type of feature from each biometric trait. The overall architecture of the proposed system is given in Figure 2. The modules in the system are Feature Extraction, Feature Selection, Classification and Score Fusion. In Feature Extraction, LBP (Local Binary Patterns), HOG (Histogram of Oriented Gradients) and Gabor wavelets are used to extract features from the face biometric input. And LPQ (Local Phase Quantization), GLCM (Grey Level Co-occurrence Matrix) and Gabor features are used to extract features from the fingerprint biometric input. In Feature Selection, PCA (Principal Component Analysis) is used and then it will be sent to the classification. 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.

3.1 FEATURE EXTRACTION

Fingerprint feature extraction- The proposed method extracts global properties and local texture details using three methods selected as excellent methods (LPQ [6], Gabor wavelet based [3], GLCM [18]) to make maximal use of the fusion technique.

Face feature extraction- The proposed method adopts two powerful texture features, LBP's [21] and Gabor wavelets [9] for describing micro-textures as well as macroscopic information. In addition, local shape description is provided using HOG [10].

ALGORITHM: LPQ (Local Phase Quantization)

STEP 1: Firstly, phase is examined in local M by M neighbourhood at each pixel position x of the image F(x).

STEP 2: Local fourier coefficients are computed at four frequency points for each pixel position given by:

$$F_x = [F(u_1,x), F(u_2,x), F(u_3,x), F(u_4,x)] \quad (1)$$

STEP 3: Phase information in the fourier coefficients is then journalized by remarking the signs of real and imaginary parts of each component in F_x. This can be done by simple quantizer given as:

$$q_j(x) = \begin{cases} 1, & if\ g_j(x) \geq 0 \\ 0, & otherwise \end{cases}, \quad (2)$$

Where $g_j(x)$ is the jth component of the vector $G_x = [\mathrm{Re}\{F_x\}, \mathrm{Im}\, g\{F_x\}]$.

STEP 4: Label image f_{LPQ} whose values are blur invariant is obtained simply by representing binary coefficient $q_j(x)$ as integer values between 0-255 using binary coding given by:

$$f_{LPQ}(x) = \sum_{j=1}^{8} q_j(x) 2^{j-1}. \quad (3)$$

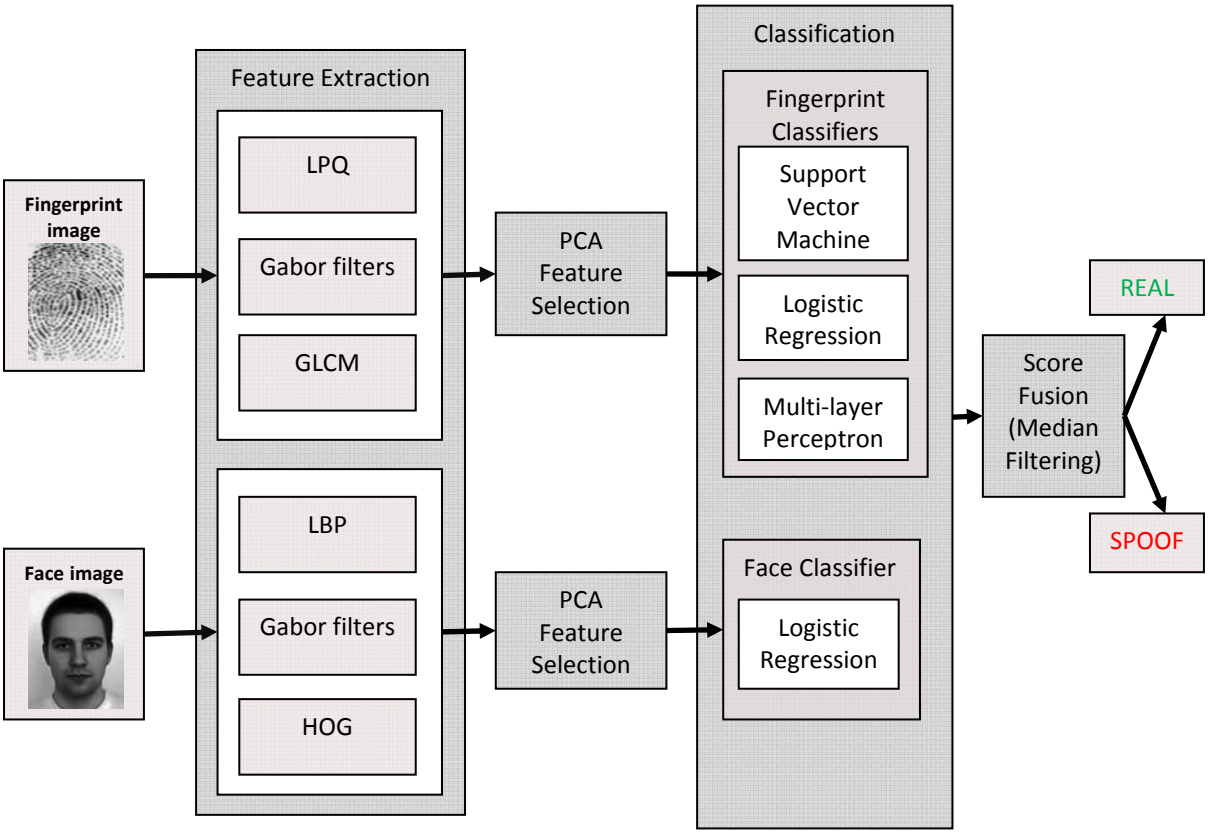

Figure 1: Overall architecture diagram of the proposed anti-spoofing approach

ALGORITHM: GLCM (Grey Level Co-occurrence Matrix)

GLCM is a n*n matrix which can be computed for various distances and orientations, where n is the number of grey levels in the image. The GLCM element P (i,j,d,θ) represents the number of pixel pairs having the gray level i and j. These pixel pairs are defined by specified distance d and direction θ. Then, from each GLCM we

compute different texture features such as angular second moment, entropy, correlation, contrast, variance, inverse difference moment, homogeneity [18].

ALGORITHM: LBP (Local Binary Patterns)

STEP 1: Divide the examined window into cells and compare each pixel in the given cell by its centre pixel value.

Also the arbitrary circular derivation of LBP operator with radius R around point(x,y), number of neighbourhood pixels P with centre c as threshold is given by T:

$$T = t(g_{0,}g_1, g_2, ..., g_{P-1}). \tag{4}$$

STEP 2: After comparison thresholding function s(z) is applied to each pixel such that T becomes:

$$T = t(s(g_0 - g_c), s(g_1 - g_c), ..., s(g_{P-1} - g_c)). \tag{5}$$

Where s(z) is thresholding step function given by:

$$s(z) = \begin{cases} 1, & z \geq 0 \\ 0, & z < 0. \end{cases} \tag{6}$$

STEP 3: Final LBP Features are obtained by summing the thresholded differences weighted by powers of two and then summed to obtain a label for the center pixel given by:

$$LBP_{P,R}(x_c, y_c) = \sum_{p=0}^{P-1} s(g_p - g_c)2^P. \tag{7}$$

ALGORITHM: HOG (Histogram of Oriented Gradients)

STEP 1: Firstly, compute gradient values using specific filter kernels or Gaussian smoothening. The magnitude and orientation of the gradient is given by-

$$|G| = \sqrt{I_X{}^2 + I_Y{}^2} \tag{8}$$

$$\theta = \arctan \frac{I_Y}{I_X} \tag{9}$$

Where I_X and I_Y are image gradients in x and y direction.

STEP 2: Second step involves creation of cell histograms. Histogram channels are evenly distributed over 0 to 180 degrees or 0 to 360 degrees, depending upon whether the gradient is “signed” or “unsigned”.

STEP 3: In order to account the changes in illumination and contrast, gradient strengths must be locally normalized which require grouping of cells into larger and spatially connected blocks.

STEP 4: last step involves block normalization.

ALGORITHM: GABOR FILTERS for FACE as well as FINGERPRINT.

A set of Gabor filters with different frequencies and orientations may be helpful for extracting useful features from an image. These filters as a product of a Gaussian and a sinusoid capturing local details are parameterized by Gaussian space constants δ_x and δ_y, frequency f of the modulating sinusoid and orientation θ.

$$G(x, y, f) = \frac{1}{2\pi\delta_x\delta_y} e^{-1/2\left(x'^2/\delta_x{}^2 + y'^2/\delta_y{}^2\right)} \cos(2\pi fx') \tag{10}$$

Where $x' = x\sin\theta + y\cos\theta \; and \; y' = x\cos\theta - y\sin\theta$

3.2 FEATURE SELECTION

The features extracted from face image and fingerprint image are concatenated to form a feature vector for classification. In feature level fusion, the feature sets originating from multiple biometric algorithms are combined into a single biometric feature set by techniques like feature normalization, feature selection and transformation. This paper uses feature selection process which selects a minimal set of relevant features that

contain most discriminant information while discarding relevant features. In the proposed work, Principal Component Analysis is used for feature selection [20].

3.3 FEATURE CLASSIFICATION

In the proposed work, three robust classifiers are used 1) SVM 2) LR and 3) Multi-layer Perceptron.

In SVM for the set of training samples each marked as belonging to one or other of two categories, SVM algorithm simply builds a model that alot new sample to one category or the other. An SVM as a classifier is a representation of the samples as a point in space in such a way that the distinct categories are divided by a clear gap. New samples are then mapped into same space and predicted to belong to a category depending upon which side of the gap they lay.

Multi-layer perceptron is a classifier based on feed-forward artificial neural network. MLPC consists of multiple layers of nodes. Each layer if fully connected to the next one. MLP uses supervised learning technique called back propagation for training of network. For learning in MLP weights are changed after each piece of data is processed on the basis of amount of error in the output compared to the expected output. Also each input node is a neuron with a non-linear activation function.

Logistic regression classification model is used to estimate the probability of a binary response based on one or more independent features. Logistic regression measures the relationship between the categorical dependent variable and one or more independent variables by estimating probabilities using a logistic function, which is the cumulative logistic distribution.

3.4 SCORE FUSION

In the proposed work, two different score level fusion rules are used to fuse scores coming from the classifiers. Following Kittler et al.'s classical framework [21], sum and median rules are given by:

$$F_{sum}(\vec{s}) = \frac{1}{n}\sum_{i=1}^{n} s_i \ ; \qquad (11)$$

$$F_{median}(\vec{s}) = \underset{i=1}{\overset{n}{med}}\, s_i . \qquad (12)$$

For an integration of counter-spoofing techniques into biometric fusion, this work introduces a variation of the median rule, called median filter for higher spoofing-resistance:

$$F_{mf}(\vec{s}) = \frac{1}{\sum_{i=1}^{n} M(\vec{s}, s_i)} \sum_{i=1}^{n} M(\vec{s}, s_i) s_i . \qquad (13)$$

$$M(\vec{s}, s_i) = \begin{cases} 1, & if \left| s_i - \underset{j=1}{\overset{n}{med}} s_j \right| < \phi, \\ 0, & else. \end{cases} \qquad (14)$$

Where Parameter ϕ is either a fixed (trained) or score-dependent threshold.

IV EXPERIMENTAL RESULTS

The description of multimodal database used for anti-spoofing is shown in Table 1.This database consists of 35 real samples of face and fingerprint modalities along with 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).

Table1: Employed test databases.

MODALITY	DATABASE	NUMBER OF SAMPLES
FACE	Antispoofing face (CASIA)	**40**
FINGERPRINT	Livedet 2015 (CROSSMATCH)	**40**

In the proposed system m is the number of spoofed samples out of n total number of samples. Also for m>0 FAR and GAR pairs refer to SFAR and GAR pairs. In a similar manner (S)EER is referred to as the (Spoof) Equal Error Rate where GAR=(S)FAR.

Table2: EER results of face and finger fusion on the test set varying the number m of spoofed samples.

METHOD	m=0	m=1	m=2	m=3	m=4	m=5
Sum rule[17]	**0**	**2.41**	**5.03**	**7.62**	**10.32**	**12.49**
Median filtering[17]	**0.47**	**0.83**	**1.07**	**1.31**	**1.67**	**1.69**
Sum rule(Proposed approach)	**0**	**1.68**	**3.32**	**4.05**	**5.27**	**6.24**
Median filtering(Proposed approach)	**0.35**	**0.48**	**0.68**	**0.82**	**0.99**	**1.05**

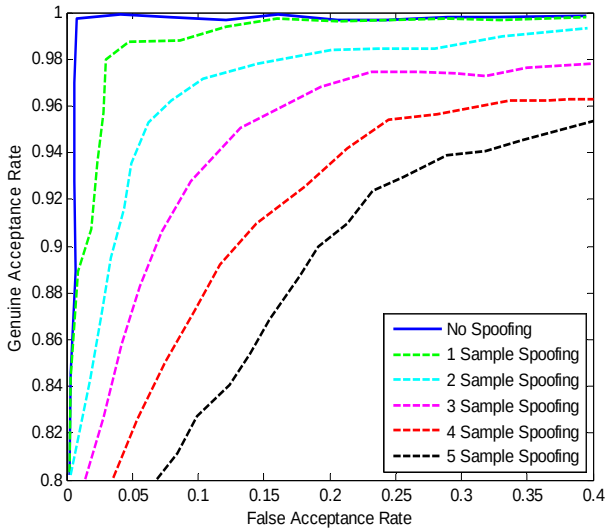

FIGURE 2: ROC for partial multibiometric spoofing using sum rule [17].

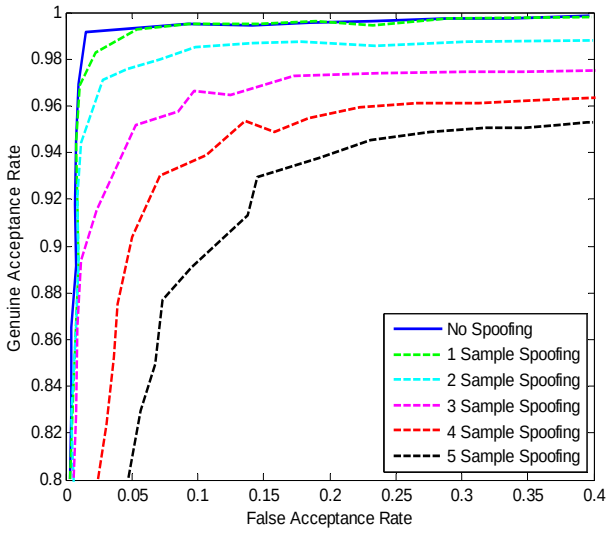

FIGURE 3: ROC for partial multibiometric spoofing using 1-median filtering [17]

From Table 2 and Fig. 2 illustrating the ROC of standard sum rule fusion it can be seen, that every additional spoofed trait increases EER by an absolute value of 2.4-3.1%. Confirming results in [17] that even a spoofing of a single spoof attempt impacts on recognition accuracy, it is observed that even 5-fake traits of both the modalities does not compulsorily signify success for imposter attempt - the overall reported sum rule EER in this case is 6.24% (vs. 1.04% for median filtering rule).

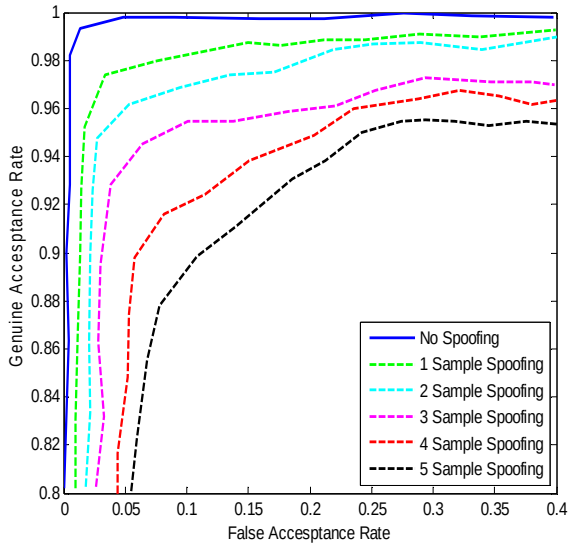

FIGURE 4: ROC for partial multibiometric spoofing using sum rule (Proposed).

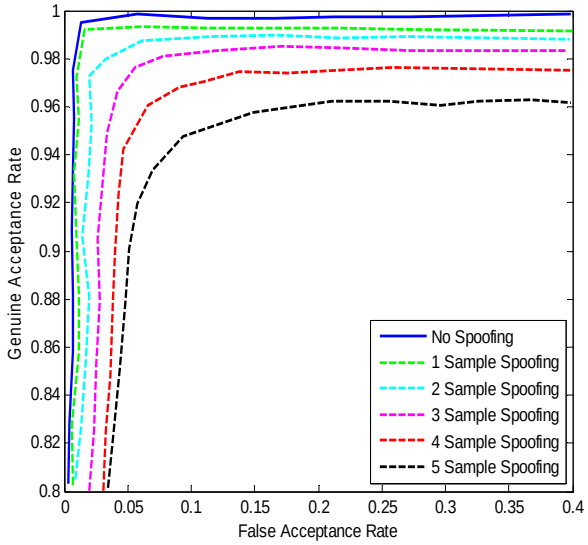

FIGURE 5: ROC for partial multibiometric spoofing using 1-median filtering (Proposed).

From the ROC curves for the median filtering fusion method as shown in Fig. 5, it can be seen that how scores in a multi-modal spoofing scenario degrade, if m out of n fingers are spoofed. While median filtering comes at the cost of slightly miniaturized 0-spoof efficacy, but it is much more effective than sum rule fusion if a minority of features is spoofed. SFAR of less than 0.05 is achieved even when the number of spoofed samples of both the biometric traits to be combined is varied.

V CONCLUSION

An Intelligent anti spoofing mechanism for a multimodal biometric system comprising face, fingerprint biometrics is implemented. Experiments on CASIA Face Anti-Spoofing Database for face and Fingerprint Liveness Detection Competition 2015 for fingerprint indicate that the proposed spoofing countermeasure employing robust techniques for feature extraction of face (Gabor wavelets, LBP, HOG) and fingerprint (Gabor wavelets, LPQ, GLCM) with multi layer classification scenario (SVM, LR, Multi layer perceptron) and integration of scores using median filtering is able to overcome the impact of spoofing in worst case scenario when both the traits to be combined are spoofed. This method is much more robust versus 3-spoof and 4-spoof attacks than both sum rule and even median filtering investigated before. For increased number of spoofed samples corresponding GARs differ minimally with stable EER's between 0.35-1.05% which illustrates the superior security performance of the proposed method compared to the other presented techniques.

REFERENCES

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Finger-print Recognition" Berlin, Germany: Springer-Verlag, 2009.

[2] Galbally, Javier, Sébastien Marcel, and Julian Fierrez,"Biometric antispoofing methods: A survey in face recognition." IEEE Access 2 ,pp. 1530-1552,2014.

[3] J.Daugman, "Complete discrete 2-d Gabor transforms by neural networks for image analysis and compression",IEEE Trans.Acoust.Speech Signal Process ,vol. no. 7, pp. 1169–1179,1988.

[4] S. Nikam and S. Agarwal, "Curvelet-based fingerprint anti-spoofing" Signal, Image and Video Processing 4, vol. no. 1, pp. 75–87,2009.

[5] H.Choi,R.Kang,K.Choi,A.Jin,J.Kim, "Fake-fingerprint detection using multiple static features", Opt.Eng.48 (2009) 047202–047202–13.

[6] L. Ghiani, G. Marcialis, and F. Roli, "Experimental results on the feature-level fusion of multiple fingerprint liveness detection algorithms" in Proceedings of the ACM Workshop on Multimedia and Security,2012.

[7] Wild, Peter, et al. "Towards anomaly detection for increased security in multibiometric systems: spoofing-resistant 1-median fusion eliminating outliers." Biometrics (IJCB),International Joint Conference on. IEEE, 2014.

[8] I.Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing", in Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG), pp. 1-7, Sep. 2012.

[9] Manjunath, B.S., Ma, W.Y, "Texture features for browsing and retrieval of image Data", IEEE Trans. Pattern Anal. Mach. Intell.,vol. no. 18,pp. 837–842,1996.

[10] Dalal, N., Triggs, B, "Histograms of oriented gradients for human detection'. Int. Conf. on Computer Vision & Pattern Recognition", vol. 2, pp. 886–893, 2005.

[11] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. IAPR Int. Conf. Biometrics (ICB), pp. 26-31, Mar./Apr. 2012.

[12] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks", Journal of Visual Languages and Computing, pp. 169–179, June 2009.

[13] R. N. Rodrigues, N. Kamat, and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system" in Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS),pp. 1–5, 2010.

[14] Johnson P,TanB, Schuckers S , "Multimodal fusion vulnerability to non-zero effort (spoof) Imposters", in: IEEE International workshop on information forensics and security (WIFS),pp. 1–5,2010.

[15] Marasco E, Johnson PA, Sansone C, Schuckers SAC , "Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism", in: Proceedings of the 10th International workshop multiple classifier systems (MCS), LNCS, vol 6713,pp 309–318, 2011.

[16] Biggio B, Akhtar Z, Fumera G, Marcialis G, Roli F , "Security evaluation of biometric authentication systems under real spoofing attacks",pp.11–24,2012.

[17] Wild, Peter, et al. "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks." Pattern Recognition 50, pp. 17-25, 2016.

[18] Nikam, Shankar Bhausabheb, and Suneeta Agarwal. "Wavelet energy signature and GLCM features-based fingerprint anti-spoofing." Wavelet Analysis and Pattern Recognition, ICWAPR'08. International Conference on. Vol. 2. IEEE, 2008.

[19] Marasco, Emanuela, and Arun Ross. "A survey on antispoofing schemes for fingerprint recognition systems." ACM Computing Surveys (CSUR) 47.2 (2015): 28.

[20] S. Chartier, G. Giguere, P. Renaud, J. Lina, and R. Proulx, "FEBAM: A Feature-Extracting Bidirectional Associative Memory". Neural Networks, IJCNN 2007, International Joint Conference on. IEEE, 2007.

[21] J. Kittler, M. Hatef, R. P. Duin, and J. Matas. On combining classifiers. IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. no. 20, pp. 226–239, 1998.