ISSN: 2320-1363

SPOOFING ATTACK DETECTION ON FACE, IRIS, AND FINGER USING KURTOSIS AND SD

S. Karthiga[*1], Prof. Chandrasekaran[*2]
Research Scholar, Dept of Computer Science, PSV College of Engineering & Technology, Elathagiri, TN, India
Assistant professor, Dept. of Computer Science, PSV College of Engineering & Technology, Elathagiri, TN, India

ABSTRACT

In all authentication systems, cheating has become a vital importance, because it challenges the overall authentication process using biometrics. An original image captured in real time can be again acquired as a photographic snapshot in a digital camera which is a fake image. Even the images designed in Photoshop also considered to be a fake image, because nowadays we have lots of software to produce synthetic images. The authentication system may not know whether it is a real image or fake image. To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 12 general image quality features extracted from one image. The project is implemented using MATLAB software ver. 2014 using image processing, statistical, mathematical and graphical tool boxes using support vector machines for classifying the original and fake images related to iris, fingerprint and face images.

INTRODUCTION

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research [1]: the publication of many research works disclosing and evaluating different biometric vulnerabilities [2], [3], the proposal of new protection methods [4], [5], related book chapters [6], the publication of several standards in the area [7], [8], the dedication of specific tracks,sessions and workshops in biometric-specific and general signal processing conferences [9], the organization of competitions focused on vulnerability assessment [10], [11], the acquisition of specific datasets [12], [13], the creation of groups and laboratories specialized in the evaluation of biometric security [14], or the existence of several European Projects with the biometric security topic as main research interest [15], [16].

EARLIER WORKS

Among the different threats analyzed, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type

ISSN: 2320-1363

of fraudulent actions in modalities such as the iris [2], the fingerprint [17], the face [13], the signature [18], or even the gait [19] and multimodal approaches [20]. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behaviour of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective. The aforementioned works and other analogue studies, have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems.

Besides other anti-spoofing approaches such as the use of multibiometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [21]: (i) non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user; (ii) user friendly, people should not be reluctant to use it; (iii) fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; (iv) low cost, a wide use cannot be expected if the cost is excessively high; (v) performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

Liveness detection methods are usually classified into one of two groups (see Fig. 1): (i) Hardware-based techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye);

(ii) Software-based techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).

The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the

ISSN: 2320-1363

sensor and the feature extract. Although, as shown above, a great amount of work has been done in the field of spoofing detection and many advances have been reached, the attacking methodologies have also evolved and become more and more sophisticated. As a consequence, there are still big challenges to be faced in the detection of direct attacks.

One of the usual shortcomings of most anti-spoofing methods is their lack of generality. It is not rare to find that the proposed approaches present a very high performance detecting certain type of spoofs (i.e., gummy fingers made out of silicone), but their efficiency drastically drops when they are presented with a different type of synthetic trait (i.e., gummy fingers made out of gelatin). This way, their error rates vary greatly when the testing conditions are modified or if the evaluation database is exchanged. Moreover, the vast majority of current protection methods are based on the measurement of certain specific properties of a given trait (e.g., the frequency of ridges and valleys in fingerprints or the pupil dilation of the eye) which gives them a very reduced interoperability, as they may not be implemented in recognition systems based on other biometric modalities (e.g., face), or even on the same system with a different sensor.

- Perform 1-D signal extension and truncation using periodic, symmetric, smooth, and zero padding methods
- Perform 1-D signal clustering and classification using wavelet analyses (with Statistics Toolbox, available separately)

For 2-D signals, you can use the GUI tools to:

- Perform discrete wavelet analysis of images
- Fuse two images
- Perform translation-invariant denoising of images, using the stationary wavelet transform.

SUPPORT VECTOR MACHINES (SVM)

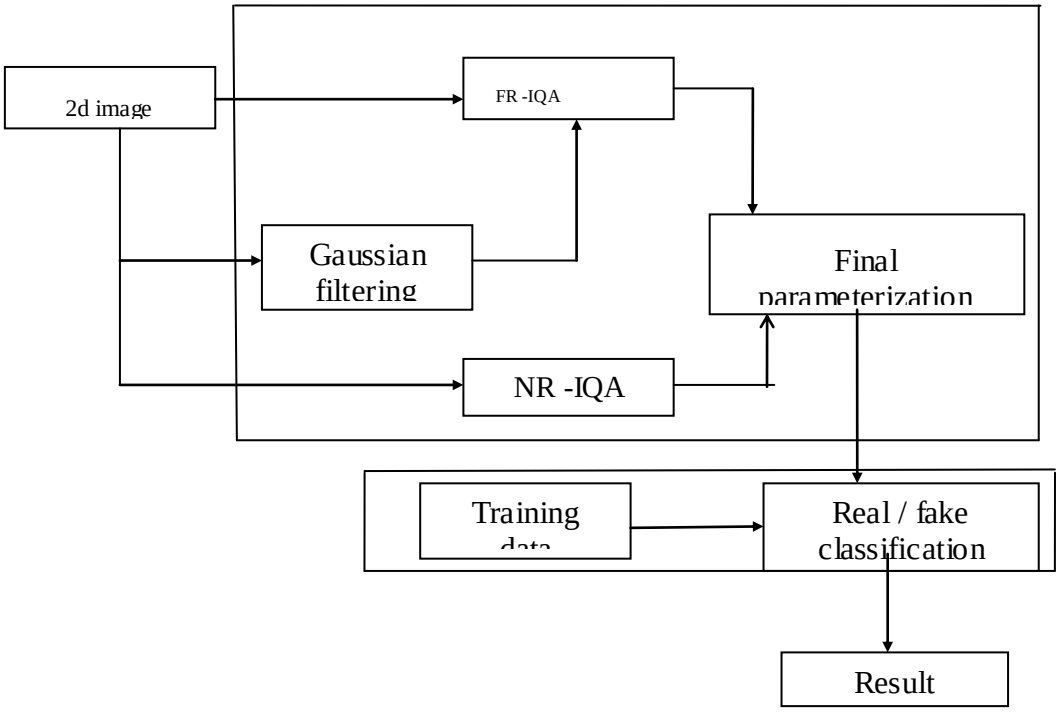
In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces.

More formally, a support vector machine constructs a hyperplane or set of hyperplanes in a high- or infinite-dimensional space, which can be used for classification, regression, or other tasks. Intuitively, a good separation is achieved by the hyperplane that has the largest distance to the nearest training data point of any class (so-called functional margin), since in general the larger the margin the lower the generalization error of the classifier.

Whereas the original problem may be stated in a finite dimensional space, it often happens that the sets to discriminate are not linearly separable in that space. For this reason, it was proposed that the original finite-dimensional space be mapped into a much higher-dimensional space, presumably making the separation easier in that space. To keep the computational load reasonable, the mappings used by SVM schemes are designed to ensure that dot products may be computed easily in terms of the variables in the original space, by defining them in terms of a kernel function $k(x, y)$ selected to suit the problem.

ISSN: 2320-1363

BLOCK DIAGRAM OF THE SYSTEM



#	Type	Acronym	Name	Ref.	Description
1	FR	MSE	Mean Squared Error	[29]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	[30]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	[31]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	[32]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[32]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|$
6	FR	AD	Average Difference	[32]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[32]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|}{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{i,j}\|}$
8	FR	RAMD	R-Averaged MD	[29]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|$
9	FR	LMSE	Laplacian MSE	[32]	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	[32]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	[29]	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1-\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity	[29]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-[1-\alpha_{i,j}][1-\frac{\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|}{255}])$
13	FR	TED	Total Edge Difference	[33]	$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{\mathbf{E}i,j}-\hat{\mathbf{I}}_{\mathbf{E}i,j}\|$
14	FR	TCD	Total Corner Difference	[33]	$TCD(I,\hat{I}) = \frac{\|N_{cr}-\hat{N}_{cr}\|}{\max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error	[34]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\|\mathbf{F}_{i,j}\|-\|\hat{\mathbf{F}}_{i,j}\|)^2$
16	FR	SPE	Spectral Phase Error	[34]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\arg(\mathbf{F}_{i,j})-\arg(\hat{\mathbf{F}}_{i,j})\|^2$
17	FR	GME	Gradient Magnitude Error	[35]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\|\mathbf{G}_{i,j}\|-\|\hat{\mathbf{G}}_{i,j}\|)^2$
18	FR	GPE	Gradient Phase Error	[35]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\arg(\mathbf{G}_{i,j})-\arg(\hat{\mathbf{G}}_{i,j})\|^2$
19	FR	SSIM	Structural Similarity Index	[36]	See [36] and practical implementation available in [37]
20	FR	VIF	Visual Information Fidelity	[38]	See [38] and practical implementation available in [37]
21	FR	RRED	Reduced Ref. Entropic Difference	[39]	See [39] and practical implementation available in [37]
22	NR	JQI	JPEG Quality Index	[40]	See [40] and practical implementation available in [37]
23	NR	HLFI	High-Low Frequency Index	[41]	$SME(\mathbf{I}) = \frac{\sum_{i=1}^{i_t}\sum_{j=1}^{j_t}\|\mathbf{F}_{i,j}\|-\sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\|\mathbf{F}_{i,j}\|}{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{F}_{i,j}\|}$
24	NR	BIQI	Blind Image Quality Index	[42]	See [42] and practical implementation available in [37]
25	NR	NIQE	Naturalness Image Quality Estimator	[43]	See [43] and practical implementation available in [37]

Table 1 : Statistical parameters considered for differentiating real and fake.

ISSN: 2320-1363

MEASURES

The following are the parameters used to differentiate the real and fake images. Mathematical parameters and their formula have been shown in table 1. Out of those 26 parameters, only the following parameters are taken into account in our proposed work. In addition, kurtosis and skewness has been added in our proposal. The mathematical formula for certain parameters have been shown in subsequent description.

- Mean1
- Mean square error
- Psnr
- Max difference
- Average difference
- Normalized absolute difference
- Standard deviation - nr
- Kurtosis - nr
- Skewness - nr
- Normalized cross correlation
- R averaged max difference

KURTOSIS

Kurtosis is a measure of whether the data are peaked or flat relative to a normal distribution. That is, data sets with high kurtosis tend to have a distinct peak near the mean, decline rather rapidly, and have heavy tails. Data sets with low kurtosis tend to have a flat top near the mean rather than a sharp peak. The formula for the kurtosis of the gray levels is

$$kurtosis = \left\{ \frac{(M \times N) \times (M \times N + 1)}{(M \times N - 1) \times (M \times N - 2) \times (M \times N - 3)} \times \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left(\frac{u(x,y) - \overline{u}}{std} \right)^4 \right\} - \frac{3(M \times N - 1)^2}{(M \times N - 2) \times (M \times N - 3)}.$$

STANDARD DEVIATION

$$std = \sqrt{\frac{1}{(M \times N)(M \times N - 1)} \left((M \times N) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} u(x,y)^2 - \left(\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} u(x,y) \right)^2 \right)}$$

SKEWNESS

- Skewness is a measure of the asymmetry of the data. Qualitatively, a negative skewness indicates that the tail on the left side of the GLH is longer than the right side, and the bulk of the values (including the median) lie to the right of the mean. A positive skewness indicates that the *tail* on the right side is longer than the left side and the bulk of the values lie to the left of the mean. The formula for the skewness of the gray levels is

$$skewness = \frac{M \times N}{(M \times N - 1)(M \times N - 2)} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \times \left(\frac{u(x,y) - \overline{u}}{std} \right)^3.$$

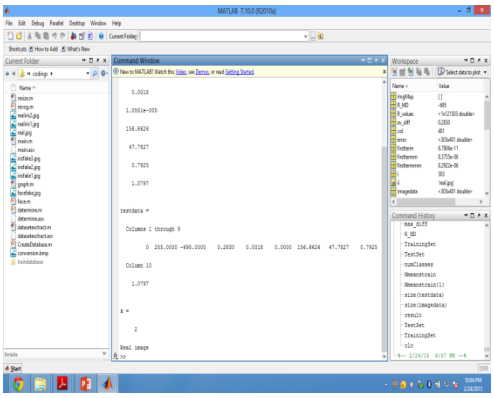
ALGORITHM

1. Images are read from database.
2. Converted into gray level images.
3. I' is calculated using median filtering operation.

ISSN: 2320-1363

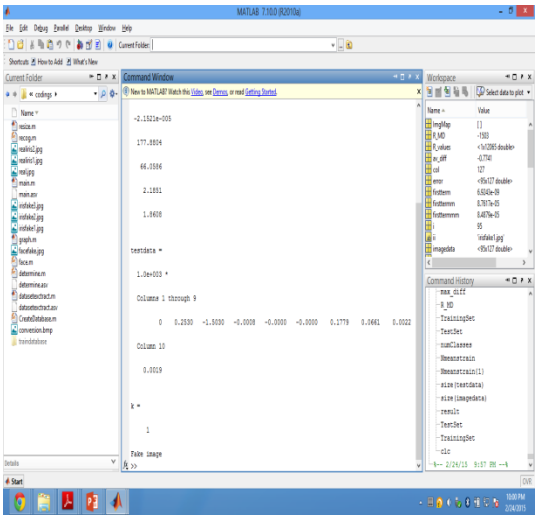
4. Several parameters are calculated including kurtosis, skewness and standard deviation.
5. The obtained values of all images are applied to SVM training.
6. Test image is applied to SVM testing and the truthness of the image is displayed based on the SVM output.
7. Availability of the images in data base is detected by comparing the feature vectors in the data bases.

N number of images are taken with arbitrary size and color images are taken into account. The codings are shown in appendix.



Real image

OUTPUTS



Input image

Fake image

Input image

The execution time while considering only 10 parameters have been shown in table 2.

Method	Proposed (S)	IQA(S)
FACE	0.15	0.13
IRIS	0.156	0.12
Average	0.153	0.125

Table 2. Execution time comparison

APPLICATIONS

- All parties involved in the development of biometrics (i.e., researchers, developers and

ISSN: 2320-1363

industry) to the improvement of the systems security to bring this rapidly emerging technology into practical use.

- Used in bank lockers and house locks automation technology.
- Mainly used for security purpose to avoid fraudulent access attempts.

CONCLUSION

In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this "quality-difference" hypothesis, in the present research work we have explored the potential of general image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing).

For this purpose we have considered a feature space of 25 complementary image quality measures which we have combined with simple classifiers to detect real and fake access attempts. The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face, using publicly available databases with well defined associated protocols. This way, the results are reproducible and may be fairly compared with other future analogue solutions.

Several conclusions may be extracted from the evaluation results presented in the experimental sections of the article:

The proposed method is able to consistently perform at a high level for different biometric traits ("multi-biometric"); ii) The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack"); iii) The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios; iv) The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in*Proc. AWB*, 2004.

[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," *Pattern Recognit.*, vol. 43, no. 3, pp. 1027–1038, 2010.

[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security,"

[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generat. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, 2012.

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.