ISSN: 2320-1363

Images Quality Assessment for Fake Biometric Detection Using Kurtosis and Standard Deviation

K.Saraswathi [*1], S.Geetha [*2], I.Anette Regina [*3]

M.phil. Research Scholar, Muthurangam Government Arts College, Vellore.

Assistant Professor, Muthurangam Government Arts College, Vellore.

Head, Associate Professor, Department of CS, Muthurangam Government Arts College, Vellore

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.

ISSN: 2320-1363

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].

LITERATURE SURVEY

Among the different threats analyzed, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type 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 behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks is 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

ISSN: 2320-1363

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).

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 machine learning, **support vector machines** (**SVMs**, also **support vector networks**) are supervised learning models with associated learning algorithms that analyze data and recognize patterns, used for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong

ISSN: 2320-1363

to a category based on which side of the gap they fall on.

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.

DefinitionMore 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. The hyperplanes in the higher-dimensional space are defined as the set of points whose dot product with a vector in that space is constant. The vectors defining the hyperplanes can be chosen to be linear combinations with parameters α_i of images of feature vectors that occur in the data base. With this choice of a hyperplane, the points x in the feature space that are mapped into the hyperplane are defined by the relation: $\sum_i \alpha_i k(x_i, x) = \text{constant}.$

Note that if $k(x, y)$ becomes small as y grows further away from x, each term in the sum measures the degree of closeness of the test point x to the corresponding data base point x_i. In this way, the sum of kernels above can be used to measure the relative nearness of each test point to the data points originating in one or the other of the sets to be discriminated. Note the fact that the set of points x mapped into any hyperplane can be quite convoluted as a result, allowing much more complex discrimination between sets which are not convex at all in the original space.

Classifying data is a common task in machine learning. Suppose some given data points each belong to one of two classes, and the goal is to decide which class a *new* data point will be in. In the case of support vector machines, a data point is viewed as a p-dimensional vector (a list of p numbers), and we want to know whether we can separate such points with a $(p-1)$-dimensional hyperplane. This is called a linear classifier. There are many hyperplanes that might classify the data. One reasonable choice as the best hyperplane is the one that represents the largest separation, or margin, between the two classes. So we choose the hyperplane so that the distance from it to the nearest data point on each side is maximized. If such a hyperplane exists, it is known as the *maximum-margin hyperplane* and the linear classifier it defines is known as a *maximum margin classifier*; or equivalently, the *perceptron of optimal stability*

ISSN: 2320-1363

IRIS RECOGNITION

In iris recognition image acquisition is an important step. Since iris is small in size and dark in color, it is difficult to Acquire good image. Also all the subsequent steps depend on it. A Panasonic camera has been used to take eye snaps while trying to maintain appropriate settings such as lighting, distance to the camera and resolution of the image. The image is then changed from RGB to gray level for further processing.

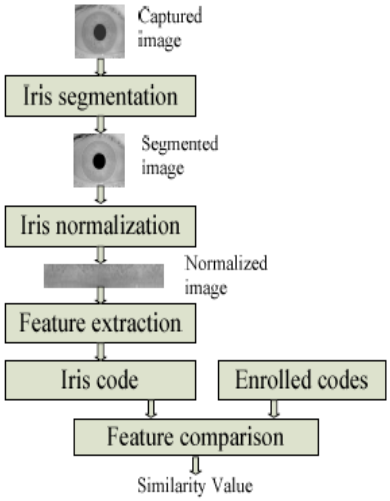
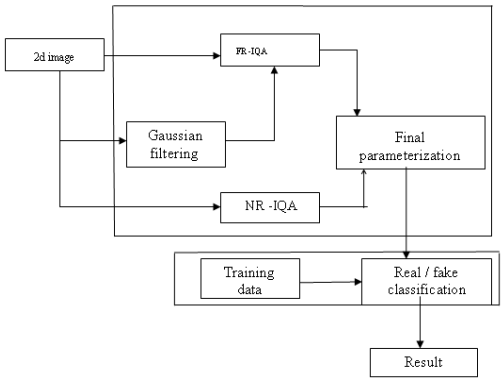


Fig.1 Block Diagram of general iris recognition system

FACE RECOGNTIION CONVENTIONS

FACE recognition has attracted more and more attention for both its scientific challenges and its wide potential applications. Much progress has been made in the last decade. However, the general problem of face recognition remains to be solved, since most of the systems to date can only successfully recognize faces when images are obtained under constrained conditions. Machine recognition of faces is gradually becoming very important due to its wide range of commercial and law enforcement applications, which include forensic identification, access control, border surveillance and human computer interactions. Face recognition is an important part of today's emerging biometrics and video surveillance markets. Recent years have witnessed an exploding interest in the development of face recognition algorithms and products. Currently, face recognition systems are usually implemented on general purpose processors. As face recognition algorithms move from research labs to the real world, power consumption and cost become critical issues. This motivates searching for implementations using a digital signalprocessor (DSP). Face recognition has been recognized for years now as an important task in computer vision and an excellent area in which machine learning can participate. Face recognition has developed into a major research area in pattern recognition and computer vision. Face recognition is different from classical pattern recognition problems such as character recognition. In classical pattern recognition, there are relatively few classes, and many samples per class. With many samples per class, algorithms can classify samples not previously seen by interpolating among the training samples.



ISSN: 2320-1363

Fig.2 Block Diagram of general iris recognition 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]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
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]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$
8	FR	RAMD	R-Averaged MD	[29]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{i=1}^{R}\max_{ij}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
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]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
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]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-\lvert 1-\alpha_{i,j}\rvert\lvert 1-\frac{\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{255}\rvert)$
13	FR	TED	Total Edge Difference	[33]	$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{E}_{\mathbf{I},i,j}-\mathbf{E}_{\hat{\mathbf{I}},i,j}\rvert$
14	FR	TCD	Total Corner Difference	[33]	$TCD(I,\hat{I}) = \frac{\lvert N_{cr}-N_{\hat{c}r}\rvert}{\max(N_{cr},N_{\hat{c}r})}$
15	FR	SME	Spectral Magnitude Error	[34]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{F}_{i,j}\rvert-\lvert\hat{\mathbf{F}}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error	[34]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{F}_{i,j})-\arg(\hat{\mathbf{F}}_{i,j})\rvert^2$
17	FR	GME	Gradient Magnitude Error	[35]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{G}_{i,j}\rvert-\lvert\hat{\mathbf{G}}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error	[35]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{G}_{i,j})-\arg(\hat{\mathbf{G}}_{i,j})\rvert^2$
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]	$SME(\mathbf{I}) = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{N_1}\lvert\mathbf{F}_{i,j}\rvert-\sum_{i=N_2+1}^{N}\sum_{j=N_2+1}^{M}\lvert\mathbf{F}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{F}_{i,j}\rvert}$
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.

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.

OUTPUTS

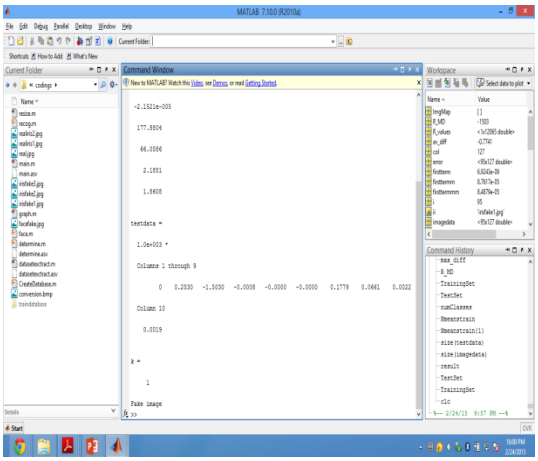


Fig.3 Snapshot of the command window in detection process

Fig.4 Input fake iris image

Fig.4 Input Real face 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

ISSN: 2320-1363

FUTURE SCOPE

- The project may be extended into a real time hardware based system to identity the fake and real for authentication purpose.
- The data base size may be increased to several 1000s of images.
- Any other biometric image can be added. Ex. Palm prints, vein prints etc.

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 10 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.

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," *EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 113–129, Jan. 2008.

[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.