A Survey Paper on Different Algorithms used for Fake Biometric Detection

Madhavi B. Danane[1] Vikram A. Mane[2]
[1]Student [2]Assistant Professor
[1,2]Department of Electronics & Telecommunication Engineering
[1]Shivaji University, Kolhapur [2]Annasaheb Dange College of Engineering, Ashta Affiliated to Shivaji University, Kolhapur, India

Abstract— The objective of this study is to compare different algorithms which make use of image quality measures for fake biometric detection. Recently, many applications are based on face recognition techniques including video surveillance, law enforcement, and identity authentication. These systems are widely used online and provide a very fast recognition rate. Face recognition is very important especially in uncontrolled environment. It is a challenging task to recognize faces due to illumination, occlusion, pose variation, expressions, aging factors and alignment etc. There are different methods used to identify whether the object is fraudulent or genuine. This paper gives idea about previous researches and their findings.

Key words: Face Recognition Techniques, Biometrics, Linear Binary Pattern (LBP), Support Vector Machine (SVM), Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Difference of Guassian Method (DoG), Grey Level Co-Occurrence Matrix Methods (GLCM), Quadratic Discriminant Analysis (QDA)

I. INTRODUCTION

In recent years biometric systems have been deployed in numerous security applications. Biometric systems are vulnerable to the different attacks that emerged as a challenge to assure the reliability in adopting these scenarios. Different algorithms are used for image quality assessment to detect whether the object being introduced in front of biometric device is fraud or genuine. The key feature of all these algorithms is to find out set of discriminant features which permits to build appropriate classifiers which gives probability of image realism. The aim is to find quality difference between standard image present in database and object placed in front of biometric device. This paper gives comparison between different algorithms and in all cases results are reported in terms of false genuine rate (FGR) which gives probably of number of false samples considered as genuine and false fake rate (FFR) which gives probability of samples coming from genuine image considered as fake. The half total error rate (HTER) is computed as

HTER= (FGR+FFR)/2 [2][4].

II. CLASSIFICATION OF FACE RECOGNITION METHODS

Basically face recognition can be done by the two main methods.

- Image-based face recognition.
- Video-based face recognition.

Table 1 shows different methods of face recognition and depending upon cost effectiveness, liveness indicator and advantages and disadvantages shown in table 2 the suitable method is chosen.

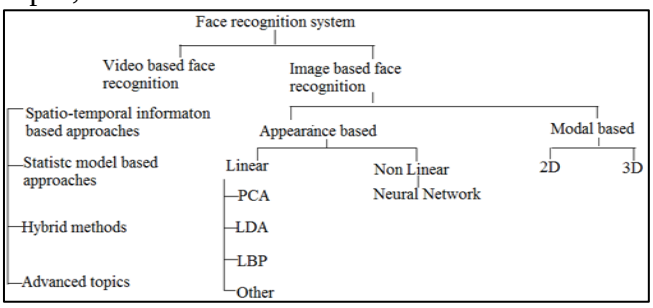


Table 1: Classification of Schemes [8]

Cost of system	Liveness indicator	Advantages	Disadvantages
Low level	Texture	• Simple implementation. • Good result in known scenarios. • Possible decision from one frame. • No user collaboration needed (non-intrusive).	• Needs data that covers all possible attacks. • Problem with low textural attacks. • Low video or image quality.
Medium level	Motion and life sign	• Difficult to spoof. • Texture independent. • Low user collaboration needed (intrusive).	• Needs video sequence. • Needs high quality image. • Challenged by videos with low motion activity. • Illumination may affect on system performance
High level	Life sign and additional sensor device	• Impossible to spoof. • Texture independent. • Cover all types of attacks. • Good performance under bad illumination conditions. • Independent from user collaboration (non-intrusive)	• Depends on landmark detection in the face. • Needs video sequences. Need extra device.

Table 2: Classification of Schemes [8]

III. COMPARATIVE STUDY OF ALGORITHMS USED TO DETECT FRAUDULENT ENTRY

Different algorithms are used for fake biometric identification. The algorithms used for fake biometric detection are Local binary patterns (LBP), Support vector machine method (SVM), Difference of Gaussian method (DOG), Linear discriminant analysis (LDA) for face recognition and for iris recognition image quality measures like local and global contrast, grey level co-occurrence matrix methods (GLCM), Qadratic discrimnant analysis (QDA)are used.

A. Linear Binary Pattern

Face recognition using Local Binary Pattern was proposed by Ahonen et al. The method provides information about the shape and the texture. The original LBP operator labels the pixels of an image by thresholding the 3*3 neighborhood of each pixel with the center value and considers the results as a binary number, and we make a histogram to describe the image. Here we use the extension to original operator called uniform pattern. A LBP is called uniform if it contains at most two bitwise transitions from 0 to 1 [3][8].

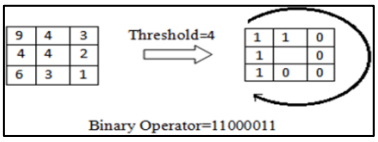


Fig. 1: Showing 3*3 matrixes

Original uniform pattern Nonuniform pattern
Fig. 2: Face image split in an image with only pixels with uniform patterns and in an image with only non-uniform patterns.

1) Advantages

– LBP method is simple. Histogram in local regions tolerates pixel misalignment.

2) Disadvantages

– Image dividing is problematic when pose variation is large [3][8][9].

B. Support Vector Machine

Initially, it was proposed as per a binary classifier. It computes the support vectors through determining a hyper plane. Support Vectors maximize the distance or margin between the hyper plane and the closest points. Support Vector Machine (SVM) is very popular binary classifier as methods for learning from examples in science and engineering. The performance of SVM is based on the structure of the Riemannian geometry induced by the kernel function. Amari in 1999 proposes a method of modifying a Gaussian kernel to improve the performance of a SVM. The idea is to enlarge the spatial resolution around the margin by a conformal mapping, such that the separability between classes is increased. Due to the encouraging results with modifying kernel, this study proposes a novel facial expression recognition approach based on improved SVM (iSVM) by modifying kernels.

1) Advantages

– They are very effective when we have very high dimensional spaces.
– When number of dimensions becomes greater than the existing number of samples, in such cases too SVM is found to be very effective.
– SVM uses a subset of training point also known as support vectors to classify different objects hence it is memory efficient.
– Support Vector Machines are versatile, for different decision function we can define different kernel as long as they provide correct result.

2) Disadvantages

– The disadvantage of SVM is that if the number of features is much greater than the number of samples, the method is likely to give poor performances.
– SVM gives efficient result for small training samples as compared to large ones. SVMs do not directly provide probability estimates, so these must be calculated using indirect techniques[8][9].

C. Principal Component Analysis (PCA)

PCA for face recognition is based on the information theory approach. It extracted the relevant information in a face image and encoded as efficiently as possible. It identifies the subspace of the image space spanned by the training face image data and decorrelates the pixel values. The classical representation of a face image is obtained by projecting it to the coordinate system defined by the principal components. The projection of face images into the principal component subspace achieves information compression, decorrelation and dimensionality reduction to facilitate decision making. In mathematical terms, the principal components of the distribution of faces or the eigenvectors of the covariance matrix of the set of face images, is sought by treating an image as a vector in a very high dimensional face space [7] [8][9].We apply PCA on this database and get the unique feature vectors using the following method Suppose there are P patterns and each pattern has training images of m x n configuration. The database is rearranged in the form of a matrix where each column represents an image. With the help of Eigen values and Eigen vectors covariance matrix is computed. Feature vector for each image is then computed. This feature vector represents the signature of the image. Signature matrix for whole database is then computed. Euclidian distance of the image is computed with all the signatures in the database. Image is identified as the one which gives least distance with the signature of the image to recognize.

1) Advantage

– It completely decorrelates any data in the transform domain.
– It packs the most energy (variance) in the fewest number of transform coefficient.
– It minimizes the MSE (mean square error) between the reconstructed and original data for any specified data compression.
– It minimizes the total entropy of the data.

2) Disadvantages

– There is not fast algorithm for its implementation. PCA are time consuming as compared with LDA.
– The PCA is not a fixed transform but has to be generated for each type of data statistics. There is considerable computational effort are needed for generation of Eigen values and Eigen values of the covariance matrix [9][10][11]

D. Linear Discriminant Analysis

Linear Discriminant Analysis (LDA) is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximum between class (across users) variance and minimum within class (within user) variance. In these techniques a block represents a class, and there are large variations between blocks but little variations within classes. It searches for those vectors in underlying space that best discriminate among classes rather than those that best describe the data. More formally given a number of independent features relative to which the data is described. LDA creates a linear combination of these which yields the largest mean difference between desire classes.

In face recognition, each face is represented by a large number of pixel values. Linear discriminant analysis is primarily used here to reduce the number of features to a more manageable number before classification. Linear discriminant analysis (LDA) is a method used in statistics, pattern recognition and machine learning to find a linear combination of features that characterizes or separates two or more classes of objects or events. The resulting combination is used as a linear classifier.

To reduce the error rate and improve security and privacy along with simplicity and generality the proposed system using 25 general image quality features extracted from one image to distinguish between legitimate and impostor sample. The parameterization proposed in the present work comprises 25 image quality measures both reference and blind. The results are considered in terms of grand test. The protection method is trained sing data from print, mobile and high definition scenarios and tested also on samples coming out from the tree types of attacks as we can't know type of artifact is print or mobile replay used to break into system [1][8].

1) Advantages

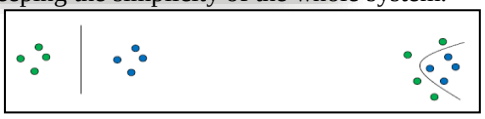
- The Fisher face projection approach is aimed to solve the illumination problem by maximizing the ratio of between-class scatter to within class scatter.
- LDA based algorithms outperform PCA based ones, since the former optimizes the low dimensional representation of the objects with focus on the most discriminant feature extraction while the latter achieves simply object reconstruction.

2) Disadvantages

An intrinsic limitation of classical LDA is the so called singularity problem, that is, it fails when all scatter matrices are singular. In face recognition area, is the Small Sample Size problem. This problem is encountered in practice since there are often a large number of pixels available, but the total number of training samples is less than the dimension of the feature space. This implies that all scatter matrices are singular and thus the traditional LDA algorithm fails to use [1][8][9]

E. Quadratic Discriminant Analysis

Quadratic Discriminant Analysis (QDA) shows better performance for iris than Linear Discriminant Analysis (LDA), which will be used in the face-related experiments, while keeping the simplicity of the whole system.



Linear decision Quadratic decision

Fig. 3: Showing linear decision boundary in LDA and quadratic decision boundary in QDA.

1) Advantage

- More flexible (quadratic decision boundary).

2) Disadvantage

- Many parameters to estimate; less accurate [1].

F. Grey Level Co-Occurrence Matrix Method

The feature extraction of iris was done by biometrics GLCM (Gray Scale Co-occurrence Matrix). The BGM (Biometric Graph Matching) algorithm is used, which is used to match the graph between the training image and test image of the iris biometric. The BGM algorithm uses graph topology to define different feature values of the iris templates. A SVM (Support Vector Machine) classifier is used to distinguish between genuine and imposter [6].

G. Results and Observations

To improve the results combination of different algorithms are used.

Table 3 gives quantitative performance of different algorithms on face and Table 4 gives quantitative performance of different algorithms on iris.

Sr. No.	Algorithm	HTER (%)
1.	LBP-LDA [3]	15.02
2.	LBP-SVM [3]	13.09
3.	DOG-SVM [4]	26.72
4.	Proposed system[1] (IQA using LDA)	15.02

Table 3: Results for Face Recognition

Sr. No.	Algorithm	HTER (%)
1.	Quality features [5]	3.10
2.	GLCM [6]	5.60
3.	Proposed system[1] (IQA using QDA)	2.2

Table 4: Results for Iris Recognition

The competition held on countermeasure to 2D facial spoofing act. Numbers of algorithms were presented to competition. These algorithms are based on motion detection of face and therefore ability to detect fake access attempts carried out with replayed motion video. Table 3 shows results of different participants sing different algorithms. The results are mentioned in terms of print and motion

Algorithm	FFR	FGR	HTER
AMILAB(Motion)	0.0	1.2	0.6
CASIA(Motion)	0.0	0.0	0.0
IDIAP (Print)	0.0	0.0	0.0
SIANI (motion)	0.0	21.2	10.6
UNIAMP(Motion)	1.2	0.0	0.6
UOULU (Print)	0.0	0.0	0.0

Table 5: Results for Print and Video subsets

Comparison of methods which are mentioned in table 5 with the proposed method is not possible as only print and video subsets are used and images are not necessarily cropped and normalized. Again classification is carried out on video basis and not on frame basis [7].

IV. CONCLUSION

By the literature review it is seen that in all algorithms quality difference hypothesis is used. We have presented a review of different anti-spoofing techniques for face liveness detection systems. These approaches make face recognition systems flexible to various types of spoof attacks. Different anti-spoofing methods have been developed and implemented that may significantly raise the difficulty level for photo, video and synthesis attacks. To date, the outcome of research efforts on anti-spoofing appears to be making a significant progress to find out more reliable and secure system. According Anti-spoofing measures make it more difficult for intruders to attack face biometric systems.

REFERENCES

[1] Javier Galbally, and Julian Fierrez Sébastien Marcel, "Image Qualit Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition" IEEE transactions on image processing, vol. 23, no. 2, February 2014.

[2] 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.

[3] Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE Int. Conf. Biometric Special Interest Group, Sep. 2012, pp. 1–7

[4] Zhiwei Zhang, Junjie yan, sifei Li, Zhen Lei ,Dong Yi, and S. Z. Li, "A face antispoofing database with diverse attacks, " in 5th IAPR International Conference on biometrics (ICB), March 2012, pp. 26-31.

[5] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271–276

[6] Ana F. Sequeira, Juliano Murari, and Jaime S. Cardoso, "Iris liveness detection methods in mobile applications," in 9th international conference on Computer Vision Theory and Applications,2013, pp. 1-5.

[7] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda,et al., "Competition on countermeasures to 2D facial spoofing attacks," in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.

[8] Sajida Parveen, Sharifah Mumtazah Syed Ahmad, Marsyita Hanafi1 and Wan Azizun Wan Adnan, "Face antispoofing methods", in Current Science, Vol. 108, No. 8, 25 April 2015.

[9] Ahmed Raga, Christina Albert, Mohamed B. Senousy, "A Comparative Study of Face Recognition Techniques" in International Journal of Electronics Communication and Computer Engineering Volume 6, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209, 2015.

[10] P. J. B. Hancock, V. Bruce and A. M. Burton, "Testing Principal Component Representations for Faces", Proc. of 4th Neural Computation and Psychology Workshop, 1997.

[11] Deepali H. Shah, Dr. J. S. Shah and Dr. Tejas V. Shah3, "The Exploration of Face Recognition Techniques," in International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, ISSN 2319 – 4847, 2014.

