International Conference on Automation, Control Engineering and Computer Science (ACECS)
Proceedings of Engineering and Technology – PET
Vol.20 pp.77 -80

A new method for 3D maskdetection in face recognition systems

Bensenane Hamdan[#1] , Keche Mokhtar[#2]
Laboratoire Signaux et Images,
Dept. d'Electronique, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf,
USTO-MB,BP 1505, 3100 Oran, Algérie
[1]bensenane1300@gmail.com, [2]m_keche@yahoo.com

***Abstract*— In this article, we propose a method forthe detection of hackers who try todeceive face recognition systems,by using 3D masks of people belonging to the system database.We first test the robustness of a well-established recognition method to attacks by 3D masks, using 3DMAD database which consists of real faces and faces with 3D masks.A recognition system essentially consists of two steps, the characteristic extraction step and the classification step.The method used for the extraction of characteristics is the polynomial decomposition,that yields the Legendre Moment Invariants (LMI), and the classifier is the well-known Support Vector Machines classifier.The obtained results prove that facial recognition systems can easily be deceived by 3D masks.To solve this fatal problem, a verification step, posterior to the recognition stepis proposed to reject fake faces.In this step, the Legendre moments invariantsare combined withthe Linear Discriminant Analysis (LDA). This allowed us to reducethe error rate in discriminating between a real face and a face mask toapproximately 0.90%.**

***Keywords*—Face recognition, 3D face mask detection, Legendre Moment Invariants(LMI).**

I. Introduction

In the everyday life, biometric systems are used in all fields, for example: access control to computers, e-commerce, Identity control, public transport, etc.

A biometric systems is a pattern recognition system that uses biometric characteristics of an individual.

Several parts of the human being may be used as biometric features,among which are: the eyes, the face,and the fingerprints.

The face is one of the most used biometric modalities. That is because it is contactless, natural, well accepted and requires only a very inexpensive sensor (Webcam), present on all electronic devices. A face recognition system essentially consists of two steps, the characteristic extraction step and the classification step. Face recognitionhas been one of the most treated subjects by the researchers sincethe 90s.

Several methods for face recognition have beenpublished. The most popular are thePrincipal Component Analysis(PCA)[1],and theLinear Discriminant Analysis (LDA)[2].

Unfortunately, the progress in thisdomain is threatened by the fact that face recognitionsystemscanbe easily deceived by hackers.The experiments showed that hackers can easily fool facial recognition systems in the acquisition phase with a simple photo[3] or video record of the face.Fortunately, these two piracymethods havebeen neutralized.

Several works that aim to distinguish a true face from a 3D mask were published. In [4],the luminance of beams of light (685nm-850nm) is measuredand used to forma feature vector that is classified by LDA.A 97.78% of good classification was reported.The drawback of this method is that the experiments were carried out directly on the material of masks and not on the masks.

In [5] the challenge was pushed further, sincehigh resolution 3D masks,realized with 3D printers, were used.The masks are replicas of real subjects after extraction of the face details by a 3D scanner.The authors propose a method based on different Linear Binary Pattern (LBP) techniquesto extractionthe characteristicsfrom two types of images (color and depth). They claima Half Total Error Rate (HTER) of 0.95% and 1.27%, for the color and depth images.

In our work we will also prove that a facial recognition system can easily be hacked by people who wear high resolution3D masks.Then, we will propose a method to remedy this problem.

ISSN 2356-5608

The proposed secured face recognition system is composed of two stages: a recognition stage and a verification stage. Both stages consist of a feature extraction phase and a verification phase.For the extractionof the facecharacteristics,we opted in the face recognition stage, for the2DLegendre Moment Invariants(LMI),as in [6], whereas in the verification stage, we opted for a combination of the LMI and the LDA.

For the classification in both the recognition and verification stages, two methods, the Next Neighbor Classifier (NNC) and the Support vector Machine (SVM) [7],were tested.

To prove that a facial recognition system is vulnerable to attacks with 3D mask we will test our recognition system on a database that is composed of people with real face and others who wear 3D masks.As a database we use, after the owners'authorization, the 3DMAD databasethat contains 3D masksof the real subjects.

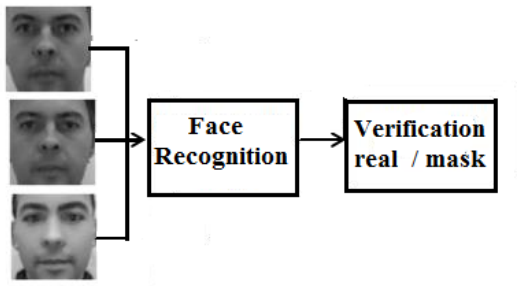

Figure 1: The principle of detecting impostors in a face recognition system.

II. Face Feature Extraction

Many 2D face feature extraction techniques have beendeveloped in recent years. As stated earlier, we have opted for the LMI and LDA based techniques, for their efficiency and simplicity.

a. The Legendre Moment Invariants

The LMIfacefeature vectors, $L_{m,n}$,extracted from a squared NxNimage, I(i,j),is given by the following equation:

$$L_{m,n} = \lambda_{m,n} \sum_{i=1}^{N} \sum_{j=1}^{N} I(i,j) \cdot P_m(x_i) \cdot P_n(y_j) \quad (1)$$

The normalization coefficient $\lambda_{m,n}$ is given by:

$$\lambda_{m,n} = \frac{(2m+1)(2n+1)}{(N-1)^2} \quad (2)$$

where the polynomial moment , $P_m(x)$, denotes the Legendre polynomial of order m, given by:

$$P_n(x) = \frac{1}{2^n(n)!} \frac{d^n(x^2-1)^n}{dx^n} \quad (3)$$

$$\begin{aligned} P_0(x) &= 1 \\ P_1(x) &= x \\ P_{n+1}(x) &= \frac{2.n+1}{(n+1)} x.P_n(x) - \frac{n}{(n+1)}.P_{n-1}(x) \end{aligned} \quad (4)$$

b. Linear Discriminant Analysis

We have found that combining the polynomial decomposition methodsLMI with LDA to extract characteristics allows to discriminate between a face and a mask. LDA projection by the eigenvectors of the data dispersion matrix, aims to maximize inter-class variations while minimizing the intra-class variations.We must find an optimal W projection base that maximizes the intra-classdispersion related to the matrix Sw, and minimize the inter-class dispersion related to the matrix Sb.

To resolve this problem,we must find W whichminimizes the Fisher optimization criterion Fisher J(W):

$$\begin{aligned} W &= \arg\max\left(J(W)\right) \\ &= \frac{|W^T S_b \ W|}{|W^T S_w \ W|} \end{aligned} \quad (9)$$

W can be foundby the resolution of the following eigenvalue equation:

$$Sb.W = \lambda.W.Sw.W \quad (10)$$

This problem reduces to a search problem of the eigenvectors of the matrix $S_w^{-1}.Sb$.

III. Classification

Two classifiers were tested for the recognition and verification phases: the Next Neighbor Classifier (NCC) and the SVM classifier. The first one uses the Euclidean distance, whichfor two vectors, $X = (x_1, x_2,...,x_N)$ and $Y = (y_1, y_2, ..., y_N)$, is defined by:

ISSN 2356-5608

$$L2 = \sqrt{\sum_{i=1}^{N} |x_i - y_i|^2} \qquad (11)$$

Support Vector Machines (SVM) may be used to solve discrimination problems, that is to say to decide to which class belongs a sample. It is originally a binary classification method that aims tofind an optimal hyperplane that separates two classes, such that the margin (distance) of the elements of the two classes to this hyperplane is maximized. Using the training data the equation of the hyperplane may be formed and its solution may be found by using the Lagrange multipliers method. The original SMV requires that the data are linearly separable. When they are not, the problem can be solved by using the kernel functions. The most used ones are: the linear, the polynomial, and the Gaussian (RBF) kernels.
Several methods may be used for the extension of the SVM to the multi-class classification problem. The one-versus-all method uses M binary classifiers, each classifier compares one class to the rest, whereas the one-versus-one method uses M.(M-1)/2 binary classifiers, each classifier compares one class to another class.

IV. Performance Evaluation

A. *Protocol*

1. The recognition phase

To prove that facial recognition systems are vulnerable to attacks by 3D masks,three sets were formed: a training set,a probe set, and a validation set.
-The training set is composed of 12 subjects out of the 17 subjects of the database.For each subject, we randomly selected 20 images of realface.This set is used to calculate the characteristic vectors.
- The validation set is composed of 240 different face images of the 12 same subjects used in the training phase, used to calculate False Rejection Rate (FRR), and 240 face images of the 5 subjects not used in the training phase, to calculate the False Acceptance Rate (FAR). Using this set
Then Equal Error Rate (EER), i.e. the mean of theFAR and FRR, iscalculated todetermine the decision threshold, for the NCC classifier.
-Theprobe set is composed of 2 subsets:the first subset is composed of 240 differentrealface images of all of the17subjects in the database, to find the recognition rate.The second subset, composed of 240 face images with 3D masks of the 12 same subjects used in the training phase, is used to calculate the Spoof False Acceptance Rate(SFAR).

2. The verification phase

To evaluate our verification method, we formed a training set, a validation set and a probe (test) set. Each set consists of two subsets: a subset with subjects with real faces and another with masks. Each subset contains 20 images of each one of the 12 subjects used in the recognition phase.
The training set allows us to form our feature vectors matrix and the probe set allows us to calculate the False Fake Rate (FFR), where the real accesses are classifiedasmaskattacks andthe FalseLiving Rate (FLR),wherethe mask attacks are classified as real accesses.The average of these two rates, called the HalfTotalErrorRate(HTER), is used as a criterion of evaluation.
The validation set is used to calculate the Equal Error Rate (EER), in order to fix the threshold for the NNC classifier.

B. Results

1. Recognition results

Therecognition rates, for the two sets (probe, validation),obtained by the LMImethod are shown in Table 1.

Table 1: The recognition rates obtained with the LMI method

	Validation Set	**Probe Set**
LMI SVM	97.20%	96.50%
LMI NNC	96.80%	96.95%

It can be said that this method of recognition gives good results on the 3DMAD database. The recognition rate is generally higher than 96% and the best results are obtained by the LMI method with classification by SVM.
The effectiveness of this recognition method has already been proved on databases with faces slightly inclined, like the ones used in our work [7].We now present the results

ISSN 2356-5608

of testing its immunity to 3D mask attacks. These results are presented inTable 2.

Table 2: The Spoof False Acceptance Rate of the LMI method

	LMI SVM	**LMI NNC**
SFAR	66.80%	60.00%

It can be observed that the obtained spoof false acceptance rates are very high.Such high SFARs are unacceptable for a recognition system. A verification step is therefore necessary for its reduction.

2. Verification results

To evaluate the performance of the proposed verification method, the HTERswere calculated for the two sets (probe, validation) and for the two classifiers. TheseHTERs, together with the one obtained by another method, which uses the LBP and LDA [9] are given in Table 3.From this table, it can be stated that the proposed verification methodmanages to reject almost all fake faces and is therefore effective in protecting a recognition system against 3D mask attacks. It can also be observed that LMI+LDA with the SVM method slightly outperforms the LBP+LDA method.

Table 3: Comparison between the HTERs of the LMI+LDA and the LBP+LDA methods.

Method	**LMI+LDA SVM**	**LMI+LDA NNC**	**LBP+LDA NNC**
HTER	0.92%	1.10%	0.95%

VI. Conclusion

Nowadays, it is easy to mislead a recognition system by using high-resolution 3D masks, which can be easily designedthanks to the advances made in 3D printing technology.

In this article, we proposed a verification method to discriminate between a real face and a 3D mask to protect face basedbiometric systems, against spoofing. We have validated our method on the 3DMAD, which is the only database that gives images of the subjects with real face and mask.The obtained results show the effectiveness of the proposed method as a countermeasure to attempts to spoof a face recognition system by3D masks attacks. As perspective to this work, we plan to improve the method by merging the recognition and the verification steps.

References

[1] M. Turk, A. Pentland,"Eigenfaces for recognition".J. Cognitive Neurosci.Vol. 3, issue 1, pp. 71–86, 1991.

[2] R.O. Duda, P.E. Hart, D.G. Stork,"Pattern Classification.John Wiley &Sons".Inc., New York etc., 2001.

[3]N. Erdogmus and S. Marcel. Spoofing 2d face recognition systemswith3dmasks. InConferenceoftheBiometricsSpecial Interest Group (BIOSIG), 2013.
Software available at:https://www.idiap.ch/dataset/3dmad.

[4] I. Cox, J. Ghosn, and P. Yianilos, "Feature-based face recognition using mixture-distance". Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 209–216, 1996.

[5] G. Guo, S. Z. Li, and K. Chan., "Face recognition by support vector machines", Proceedings of the Fourth IEEE International Conference on Automatic Face and Gesture Recognition, pp. 196–201, 2000.

[6] S.H. Lee,S.Sharma, L. Sang, J. Park, and Y.G.Park,"An Intelligent Video Security System using Object Tracking and Shape Recognition", ACVIS LNCS Springer-Verlag, Berlin Heidelberg, Vol. 6915, pp. 471-482, 2011.

[7]H.Bensenane ,M. Keche," Face Recognition Using Angular Radial Transform",Journal of King Saud University - Computer and Information Sciences(2016),10.1016/j.jksuci.2016.10.006.

ISSN 2356-5608