Face Recognition and Authentication using LBP and BSIF

Mask detection and elimination

Naveen S
Assistant Professor
Dept. of ECE
LBSITW
Thiruvananthapuram, Kerala
nsnair11176@gmail.com

Shihana Fathima R
M.Tech Student
Dept. of ECE
LBSITW
Thiruvananthapuram, Kerala
shihanafathima09@gmail.com

Dr. R S Moni
Professor
Dept. of ECE
Marian Engineering College
Thiruvananthapuram, Kerala
moni2006rs@gmail.com

***Abstract*— In this paper, a face recognition and authentication method that can detect and eliminate the presence of the mask is proposed. The proposed method utilizes facial features, which are captured locally and globally to distinguish between a mask and a real face. The features employed here are extracted from the whole face as well as the eye and nose regions that are expected to provide a clue on the presence of the mask. Here, Local binary pattern (LBP) and Binarized Statistical Image Features (BSIF) are utilized to extract the texture features of the face for recognition. Then for classification Euclidean distance classifier is used whose scores are fused using the weighted sum rule for making the decision about a real face or a mask attack. 3D mask database 3DMAD is used for testing the algorithm.**

***Index Terms*—Face authentication, BSIF, LBP, Mask Attack, Spectral Transformation.**

I. Introduction

Face Recognition is an emerging technology that detects face and uses facial features for identification of individuals. Authentication using face recognition system has been receiving more and more attention during the recent years. This is due to the fact that it is hands free and user friendly compared to the other well known authentication systems. However, face authentication systems are highly vulnerable to spoofing attacks using a photograph [8] or video [9] or even a sophisticated 3D mask [5]. Achieving authentication by presenting fake biometric evidence is much easier in case of facial biometric system. This vulnerability has caused significant attention in the area of spoofing attack detection.

In this paper, a face recognition system along with mask detection and mitigation is proposed. Figure 1 shows the general block diagram of the proposed method. The proposed method extracts local and global facial features for recognition and authentication. The local features reflect the variations in eye and nose region between a real face and a 3D mask [2] where as the global features are extracted for face recognition. Scores of the different features are combined using weighted sum rule. Finally, a Euclidean distance classifier is used to classify real access and mask attempt. Evaluations are carried out using 3D MAD dataset [1] [6].

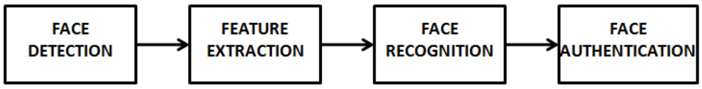

Fig. 1. General block diagram of proposed scheme

II. Proposed Idea

The proposed scheme has four stages: Face detection, Feature extraction, Face recognition and Face authentication.

A. Face Detection

Face region from 2D image and its corresponding depth map captured by the Kinect camera [6] is extracted using cascade object detector. It uses Viola-Jones algorithm for detection and a trained classification model for detection.

Depth map is made visible by normalizing with the maximum intensity value.

B. Feature Extraction

Figure 2 shows the block diagram of proposed face recognition and authentication method. Feature extraction includes extracting local and global features of the detected face region. Local features are captured from eye and nose region extracted from face using cascade object detector.

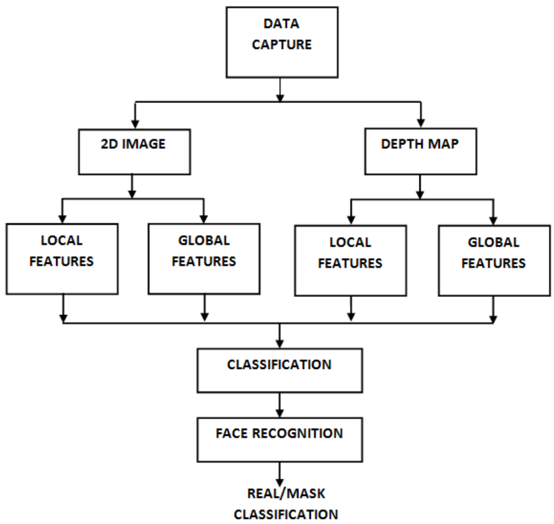

Fig. 2. Block diagram of proposed method

First local feature is obtained from 2D image and depth image of eye by transforming both into spectral domain using 2D DCT. This result in a matrix of same size and low frequency components will be prominent in the transformed data. This makes classification more reliable [3]. Spectral transformation by 2D DCT can be done using the equation (1).

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos(\frac{(2x+1)\pi u}{2M})\cos(\frac{(2y+1)\pi v}{2N}) \quad (1)$$

for a M x N image.

Area of the extracted nose region is computed as another local feature. Global features are extracted from 2D and depth image of face region. For which Binarized Statistical Image Features (BSIF) [7] and local binary pattern (LBP) [10] is employed. Figure 3 illustrates the global features obtained from 2D image and depth map of a real sample as well as mask sample. BSIF is obtained by computing a binary code for the pixels of the 2D and depth image. Histogram of this code value provides the texture properties of the image. The response of a set of n linear filters trained using statistical properties of a set of natural images provides the bits in the binary code. For a 2D face image f(x, y) and a filter $h_k(x, y)$ of same size, filter response is given by

$$r_k = \sum_{x,y} f(x,y)h_k(x,y) \quad (2)$$

Where x and y denotes the size of the image and h_k, for all k = {1, 2…n}.

Filter response r_k is binarized by

$$b_k = \begin{cases} 1, & if\ r_k > 0 \\ 0, & otherwise \end{cases} \quad (3)$$

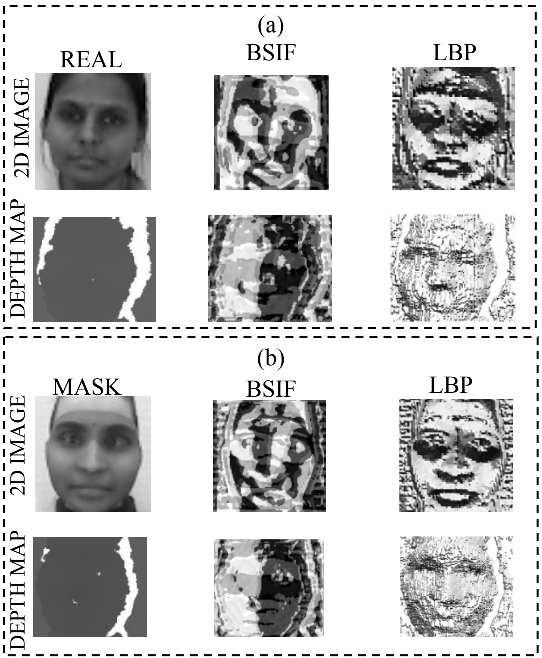

Fig. 3. Illustration of global features of (a) Real sample (b) 3D Mask sample

LBP is obtained by describing each pixel relative to the neighboring pixels. It is given by the equation (4).

$$LBP_{R,N}(x,y) = \sum_{i=0}^{N-1} s(n_i - n_c)2^i \quad (4)$$

where n_c corresponds to the centre pixel of a local neighborhood N and n_i to the gray levels of N equally spaced pixels in a circle of radius R. Here, s(x) is given by the equation (5).

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & otherwise \end{cases} \quad (5)$$

C. *Face Recognition*

Figure 4 shows the block diagram of proposed recognition method. The global features extracted from face region are utilized for face recognition.

D. *Face Authentication*

Figure 5 shows the block diagram of proposed authentication procedure. Local features are used for identifying a 3D mask from real face. Spectral information is acquired from the eye image and its corresponding depth map. Since the human eyes are more sensitive towards low frequency spectrum and the use 3D mask in which eye regions are left open may hide the rich details of the eye region.

Also computing the area of nose region also provides the clue for mask detection as the size of nose for a 3D mask is different.

E. *Score Fusion*

The different features obtained from the 2D and depth image are given to classifier for classification. Here, a well-known Euclidean distance classifier is used which computes the minimum distance between the test and reference data. This minimum distance is used for recognition.

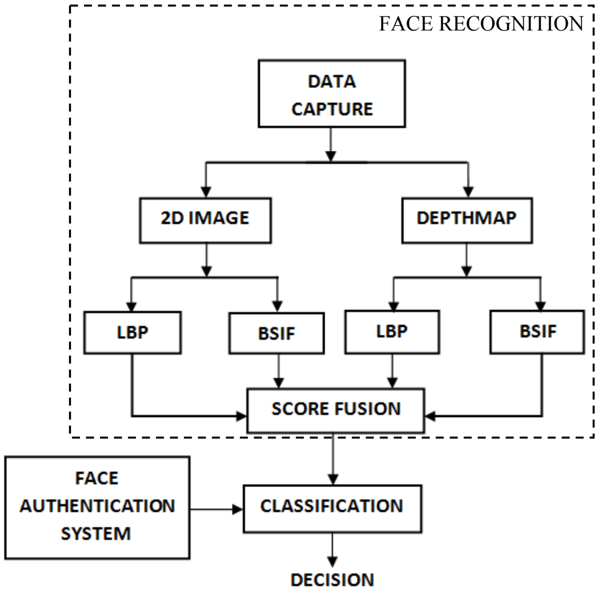

Fig. 4. Block diagram of the proposed face recognition method

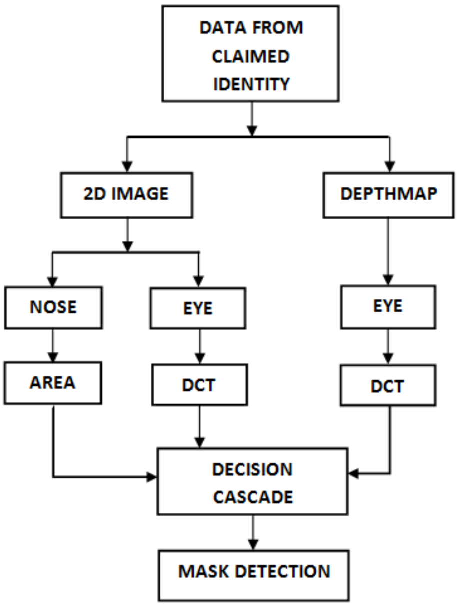

Fig. 5. Block diagram of the proposed face authentication method

Equation 6 gives the distance equation of the Euclidean distance classifier.

$$d(x,y) = \sqrt{\sum_{j=1}^{n} (x_j - y_j)^2} \qquad (6)$$

where x_j and y_j represents reference and test data respectively. Finally, decision D for face recognition by fusion is made by combining the comparisons scores of different features using weighted sum rule given by the equation (7)

$$D = \sum_{k=1}^{n} \mathrm{W_k} * \mathrm{d_k} \qquad (7)$$

where n denotes the number of features. d_k and W_k represents the score obtained and weight given to k^{th} feature.

Recognition is done using this fusion score and the result is given to authentication system for mask elimination.

III. Experiments and Results

The proposed scheme is evaluated using windows 8.1 system with 4GB RAM and Intel-i3 processor using MATLAB R2013a. For testing and analysis 3D mask database 3DMAD is used. The database is partitioned into 3 different sessions. The first two sessions are dedicated to real access samples and in third session 3D mask attacks are captured. First session is used for training and second and third sessions are used for testing. From the samples local and global features are extracted for face recognition and authentication. Here 510 mask and 510 real samples, hence a total of 1020 samples are used for testing by taking six frames of 5 video samples of 17 persons from both mask and real access. Figure 6 shows the comparison of accuracies obtained by T_fus, D_fus and their fusion at different number of samples. T_fus and D_fus represent fusion of the results obtained by employing LBP and BSIF on texture map and depth map respectively.

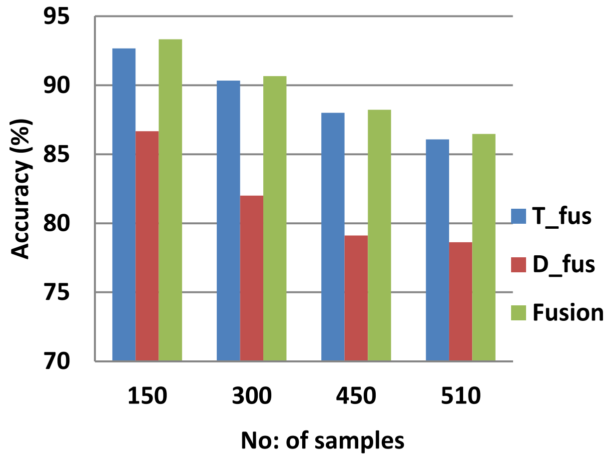

Fig. 6. Comparison of Depth, Texture and Fusion

Table I shows accuracies in face recognition obtained by employing different global features and their fusion. LBP_T and BSIF_T indicate LBP and BSIF applied on texture map or 2D image respectively. LBP_D and BSIF_D indicate LBP and BSIF applied on depth map respectively. This gives the True Acceptance Rate of the proposed method.

False Fake Rate (FFR) i.e. rate of real access assigned as fake and False Living Rate (FLR) i.e. rate of fake attempt misclassified as real is computed for performance analysis. Finally Half Total Error Rate (HTER) is computed as (FFR+FLR)/2. Table II shows the results obtained by employing different features and their fusion.

In [2], the author compares three methods of mask detection and claims to obtain HTER of 8.14, 9.16 and 0.03% for LBP using SVM classifier, LBP using LDA classifier and BSIF using SVM classifier respectively. But the number of samples used for training and testing are not mentioned. The proposed method has obtained HTER of 7.65% using 1020 real and 1020 mask samples. In [4], the author claims to obtain classification accuracy of 88.1% and 86.0% using texture and depth map respectively. Here, the results are obtained using only 100 real and 100 mask samples for testing. But the proposed method gives an accuracy of 94% and 93.3% using texture and depth map respectively for 150 real and 150 mask samples.

TABLE I. Accuracies obtained for different features

Features	Accuracy (in %)
LBP_T	84.90
LBP_D	47.84
BSIF_T	85.88
BSIF_D	77.45
Fusion	86.47

TABLE II. ERROR RATES OBTAINED FOR DIFFERENT FEATURES

Features	FFR (in %)	FLR (in %)	HTER (in %)
LBP_T	15.10	8.04	11.57
LBP_D	52.16	5.29	28.73
BSIF_T	14.12	1.96	8.04
BSIF_D	22.55	0.78	11.67
Fusion	13.53	1.76	7.65

IV. CONCLUSION

In this paper, the problem of mask attack is addressed along with face recognition to achieve authentication. Global features are used for recognition and local features are utilized along with these features for authentication. Combination of these features provides a low HTER of 7.65%.

ACKNOWLEDGMENT

Thanks to Mr. Bastien Crettol, Data Manager, Idiap Research Institute, Switzerland, for providing access to the 3D MAD database.

REFERENCES

[1] https://www.idiap.ch/dataset/3dmad.

[2] Raghavendra, R.; Busch, C., "Novel Presentation Attack Detection Algorithm for Face Recognition System: Application to 3D Face Mask Attack," in Image Processing (ICIP), 2014 IEEE International Conference on IEEE, 2014, pp. 1-5.

[3] Naveen S. and Dr. R.S Moni, "3D Face Recognition using Fourier-Cosine Transform Coefficients Fusion", International Journal of Engineering and Advance Technology Vol.4, Issue 5, June 2015.

[4] N. Kose and J. L. Dugelay, "Countermeasure for the protection of face recognition systems against mask attacks," in Automatic Face and Gesture Recognition (FG), 2013 10th IEEE International Conference and Workshops on, April 2013, pp. 1–6.

[5] Nesli Erdogmus and Sebastien Marcel, "Spoofing 2d face recognition systems with 3d masks," in Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. IEEE, 2013, pp. 1–8.

[6] N. Erdogmus and S. Marcel, "Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect," in IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–8.

[7] Juho Kannala and Esa Rahtu, "Bsif: Binarized statistical image features," in Pattern Recognition (ICPR), 2012 21st International Conference on, 2012, pp. 1363–1366.

[8] Andr´e Anjos and S´ebastien Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in Biometrics (IJCB), 2011 International Joint Conference on. IEEE, 2011, pp. 1–7.

[9] Gang Pan, Lin Sun, ZhaohuiWu, and Shihong Lao, "Eyeblinkbased anti-spoofing in face recognition from a generic webcamera," in Computer Vision, 2007. ICCV 2007. IEEE 11thInternational Conference on, 2007, pp. 1–8.

[10] Timo Ahonen and Matti Pietikainen, "Face description using Local Binary Patterns: Application to Face Recognition" inIEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 28, No 12, 2006.