Detection of Face Spoofing Attacks using Printed Photo and Mimic Mask

D. Gowthami #1, T. Venipriya #2

1M.E student, Department of Computer Science, Arasu Engineering College, Kumbakonam,
2Assistant Professor, Department of Computer Science, Arasu Engineering College, Kumbakonam.
1gowthamidharmarajan@gmail.com
2veniPri@gmail.com

Abstract—Face Recognition and Verification system is the alternative and recently emerging method in biometric technique in order to provide high level security to the system or the organization. Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Printed photo, mimic mask, video replay are some of the commonly used methods for spoofing. In this paper, we propose a real time and spoofing measure in order to detect the liveness of the face. Diffusion Speed of a single image is calculated to identify the difference between live face and fake face by using Total Variation Flow. The Inter Session Variability (ISV) modelling is used to detect 2D mask and Iterative Closest Point (ICP) algorithm is used to detect 3D mask attacks. The local speed patterns of diffusion speed are extracted and these features are given as input to the linear SVM classifier. The Experimental results on various datasets like NUAA, Replay attack and Morpho show that the proposed method is effective for face spoofing detection when compared with previous approaches.

Keywords—Spoofing, Diffusion Speed, Inter session Variability, Iterative closest point, Local speed pattern.

I. INTRODUCTION

The mobile devices are provided with high level security using some biometric techniques such as Iris, Finger print, signature, hand gestures etc., [1], [2] The Iris and Finger print verification system is most commonly used biometric technique in order to provide security to the system. Vulnerability of face recognition and verification system to spoofing attacks is still an open security issue in biometrics domain. Even though they provide high level security, they need require close interaction with the user which is inconvenient to the user. The Face Recognition and Verification system is the alternative measure to these biometric techniques where our face is given as input. This is most popular method which is vulnerable to diverse spoofing attacks. Various spoofing activities using printed photo, mimic mask, screen shots, video replay attacks are shown in figure 1, in order to gain the access illegally. The attacker will also capture the video sequence such as eye blinking, head shake etc., and replay it in order to penetrate the security system. Several researchers have addressed this problem based on three approaches namely motion, spectrum and image quality information. First motion based approach, in which face motions are detected such as eye blinking [3], [4], and lip movement [5] and head rotation. Specifically in [3] the eye blinking is detected based on the undirected conditional graphical framework, in which a discriminative measure of eye state is incorporated. In [5], the optical flow line of the mouth region is detected to find the lip movement. They use velocity vector onto their intuitive stick-mouth model and extracted the statistics of the lip movement for face liveness detection.

Second the spectrum-based methods clearly explain the difference between the face and live face in spoofing attacks. In [6], the reflectance disparities between the live and fake faces are revealed based on the computed radiance under different illuminations, and these estimated values are then applied to Fisher linear discriminate. In [7] the albedo curves of different materials, i.e., skin and non skin are measured. This approach lead to correct face spoofing detection but requires some additional devices like near infrared sensor, which are not easily deployed in mobile systems.

Third image quality-based approaches are used to detect some quality features from live face and fake face and compare them to find the spoofing attacks. The fake face does not have more quality features like the live face. In [8] the Fourier transform is used to identify the spoofing attacks by observing the lose details in fake faces. In [9] Multiple DoG filters is applied to extract the features to determine the liveness of the face. In [10] the DoG filter along with texture based analysis is used to detect the face liveness.
Spoofing using mimic mask is detected using various approaches. In [11] 3D data acquired with a low-cost sensor is used to localize face and verify spoofing attacks. In [12] the planner surface for a fake face is rendered futile in case of 3D facial mask attacks. In [13], the authors conduct experiments on different mask materials like silicon, latex or skin-jell to observe the reflectance difference when compared to facial skin from the forehead region. In [14] the albedo curves of facial skin and mask materials are examined with two discriminative wavelengths (850 and 1450 nm).

To overcome the above discussed problem, we propose a novel method to detect the face spoofing activities using photo and mask from a single image. The key idea of this method is to find the difference between live and fake face by analyzing the surface properties of the image which is calculated by using diffusion speed. The mask attacks (2D mask and 3D mask) are estimated using two techniques namely Inter Session Variability (ISV) method and Iterative Closest Point (ICP) algorithm. The diffusion speed is computed using the Total Variation (TV) flow and the extracted features based on local speed patterns (LSPs). These features are given as input to the SVM classifier to determine the spoofing activities. When compared to previous approaches, the proposed method is more effective and performs well regardless of the image medium and under varying illuminations. This increases the robustness of face recognition and verification system in a wide environment. The experimental results using various datasets like NUAA, Replay attack and morpho shows reliable performance of face spoofing detection.

II. FACE SPOOFING DETECTION

A. Motivation

The proposed method states that the illumination and reflectance characteristics of live face and fake faces are different. It is easy to see that the light on live face is randomly reflected because of the 3D structures (e.g., nose, lip, etc.), where the reflectance of the light on 2D fake faces is relatively uniform. This is due to the illumination energies on a 2D surface are evenly distributed and thus are expected to diffuse slowly, whereas those on a live face tend to move faster because of their non-uniformity. The difference in pixel values between the original and diffused images provides useful clues that can be used to discriminative a live faces from a fake one in a single image. Here the total variation flow is calculated by extracting the local speed patterns of the diffused image. This LSP is used to give input to the Inter Session Variability (ISV) method and Iterative Closest Point (ICP) algorithm in order to detect the 2D mask and 3D mask in spoofing attacks.

B. Diffusion Speed Model

The main aim is to efficiently reveal the illumination characteristics clearly using diffusion speed model. First the nonlinear diffusion is conducted on the original face image I, given as

\[ u_{k+1} = u_k + \text{div}(d(\nabla u_k) \nabla u_k), u(0) = I, \]

where \( k \) denotes the iteration number. For the diffusivity function \( d(\cdot) \), we propose adopting the total variation (TV) flow.

\[ d(x) = \frac{1}{x + \epsilon} \]

where \( \epsilon \) is a small positive constant. The difference in the illumination of the original and diffused image is shown in figure 2.

In a given image, the TV flow has been proven to comply with the following rules. 1) Pixels belonging to a small region move faster than those belonging to a large region, e.g., a homogenous region, and 2) the two boundary pixels adapt their value with half that speed. These rules lead to a very useful consequence: by simply computing the difference in pixel values of the original and diffused images generated by the TV flow, we can easily estimate the relative diffusion speed of each pixel. An important issue is to solve the diffusion equation defined in (1). To this end, we use an efficient approach, called the additive operator splitting (AOS) scheme defined as

\[ u_{k+1}^{x,y} = \frac{1}{2} ((I - 2\tau A_x(u^k))^{-1} + (I - 2\tau A_y(u^k))^{-1}) u^k. \]

Where \( A_x \) and \( A_y \) denote the diffusion matrices computed in the horizontal and vertical directions, respectively. When compared to Euler scheme, this AOS scheme is unconditionally stable also able to use a large time step, e.g., \( \tau = 30 \) that provides more accuracy and efficiency, to enable fast diffusion our diffusion speed successfully reveals the illumination and reflection effects. The diffusion speed at each pixel level \((x,y)\) is calculated as below. This shows the amount of difference

\[ s(x, y) = |\log(u0(x, y) + 1) - \log(uL(x, y) + 1)|, \]

where \( L \) denotes the total number of iterations. The performance variations according to the \( L \) and \( \tau \) settings are given in Section III.

C. Inter Session Variability

Inter Session Variability (ISV) modelling is used to detect the 2D mask in spoofing detection. First 12-12 blocks are isolated from the facial image by moving a sampling window one pixel at a time. Mean and Variance normalization is applied and the first 45 2D DCT coefficients are extracted. Based on the distribution of these feature vectors, a GMM is estimated.

© 2015 IJAIR. All Rights Reserved
using background model adaptation. Finally, ISV modelling is applied to exclude the within-client variation, by assuming it is contained in a linear subspace of the GMM mean super-vector space and estimating subspaces via maximum a posteriori adaptation.

**D. Iterative Closest Point**

Iterative Closest Point (ICP) Algorithm is used to detect 3D mask attacks. In order to minimize the distance between two cloud points, ICP computes and revises the translation and rotation iteratively. This registration is used to establish Point-to-Point correspondences between two face models. The final minimized distance, ICP error, can also be employed directly to compare them. The two main shortcomings of ICP are that it needs a good initialization for an accurate result and it cannot handle non rigid transformation which is crucial in the presence of surface deformations, such as occlusions or facial expressions.

**III. EXPERIMENTAL RESULTS**

Here three benchmarking datasets are used namely NUAA, Replay Attack and Morpho datasets. NUAA is most widely used in this field. The Replay attack dataset is composed of photo and video under different lighting conditions used in attack attempt against 50 clients. The Morpho is not a public dataset which consists of mimic mask for set of users.

**A. Datasets**

1) **NUAA:** This dataset is widely adopted in this field for evaluating face liveness in order to spoofing attacks. It consists of images of 15 subjects who were asked to frontally look at the webcam with neutral expression. None of the faces contains any apparent movement, such as eye blink or head movement. To create fake examples, the authors captured the pictures using usual cannon camera and printed them on a A4 paper respectively. These faces are detected using Viola-Jones detector and geometrically normalized based on the eye localizer. Finally, these images are resized to 64 x 64 pixels with gray scale representation.

2) **Replay-Attack:** This dataset consists of 1,300 video clips and photo images under various lighting conditions are used for spoofing attacks against 50 clients. Used to identify the spoofing medium such as printed paper, smart phone or high resolution screen (Tablet). Therefore the dataset is decomposed into three subsets, as for training, development, and testing. It is mostly applied to video based spoofing attacks.

3) **Morpho Database:** This is a non-public database which consists of 207 real access and 199 mask attack images in both 2D and 3D, i.e., facial images and 3D face models. It consists of masks of 16 clients that are used for spoofing attacks, created using 3D printer. The texture of the mask is in gray scale and the shapes are accurate as live faces. A 3D scanner uses a structural light technology to capture many different shots for each user. In each shot, three manually annotated points (two for outer eye corners and one for the nose tip) are included in the database.

**B. Proposed methodology**

In the Proposed methodology (Fig. 3), the input image is given to the face recognition and verification system, the image is checked for spoofing attacks by calculating the diffusion speed of the image. Here the Pre processing processes are done first for the input image such as noise removal, enhancements activities etc. Then the face of the user is detected using facial components like eyes, nose and Lips. The Diffusion speed of the image is calculated using the Local speed patterns and these extracted features are given as input to the SVM classifier. If it is a live image then spoofing is not intimated. If it is a photo are video then it is intimated as spoofing activities and access is not allowed. The ISV and ICP techniques are used to identify the masked attacks. Finally the input image is completely analysed for liveness and provide results as live face or fake face.

**C. Performance Evaluation in NUAA Dataset**

In Diffusion Speed Model, the experiment is conducted with various time step values and iteration numbers. The image block of size 32 x 32 pixels is taken for implementation and the dimension of the feature vector is 59 x 9 = 531. These features are given as the input to the SVM classifier for training and testing. C is fixed as 100 for SVM in order to show good results on validating the proposed method of training set.

**Table.1 Performance of NUAA compared with various approaches**

<table>
<thead>
<tr>
<th>Methods</th>
<th>DoG-F</th>
<th>DoG-M</th>
<th>DoG-S</th>
<th>DoG-L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>84.5%</td>
<td>81.8%</td>
<td>87.5%</td>
<td>94.5%</td>
</tr>
<tr>
<td>Methods</td>
<td>MLBP</td>
<td>CP</td>
<td>Baseline</td>
<td>LSB-based</td>
</tr>
<tr>
<td>Accuracy</td>
<td>92.7%</td>
<td>97.7%</td>
<td>90.4%</td>
<td>98.5%</td>
</tr>
</tbody>
</table>

© 2015 IJAIR. All Rights Reserved
D. Performance Evaluation in Replay Attack Dataset

The Performance evaluation of Replay Attack Dataset is discussed in this subsection. This is mainly designed for diverse spoofing attacks and provides samples for both training and testing. The performance of evaluation of Replay-Attack Dataset is compared with various approaches such as Half total error rate (HTER), which is half of the sum of the false rejection rate (FRR) and false acceptance rate (FAR).

The threshold value for HTER is determined by computing the equal error rate (EER), which is defined in ROC curve where FAR values equal the FRR value. Hence the HTER Valus of the development and test is set as 13.72% and 12.50% respectively. The comparison of performance of Replay Attack dataset in various attacks is shown in Table 2.

<table>
<thead>
<tr>
<th>Types</th>
<th>Print attack</th>
<th>Phone attack</th>
<th>Tablet attack</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed-support</td>
<td>1.79%</td>
<td>0.63%</td>
<td>17.52%</td>
<td>12.88%</td>
</tr>
<tr>
<td>Hand-held</td>
<td>5.84%</td>
<td>2.18%</td>
<td>12.09%</td>
<td>13.97%</td>
</tr>
</tbody>
</table>

E. Performance Evaluation with Morpho Dataset

Face recognition and verification system consists of masked images of users in order to attack the security systems. The results of this morpho dataset are compared with LBP-2D, LBP-2.5 and TPS-3D algorithms. They are tested using various protocols in order establish the baseline system (ISV and ICP approach). The 2D mask attacks and 3D mask attacks are determined using two techniques namely ISV and ICP approaches. The Performance of this technique to live and fake faces is shown in Figure 5.

![Fig. 4. The comparison results of live and fake faces.](image)

IV. CONCLUSIONS

An effective and robust approach to detect the face spoofing activities was proposed in this paper. The main part of this method is the Diffusion Speed model to detect the spoofing activities using printed photos and videos. This is based on the reflection and illumination characteristics of the image. The next approaches are Inter Session Variability (ISV) and Iterative Closest Point (ICP) methods in order identify 2D masks and 3D masks respectively, in order to reveal the difference between the live and fake faces. The Local speed pattern of the image is initially computed in order to analyze these factors in spoofing attacks. Therefore it is concluded that, the proposed method will detect the spoofing attacks efficiently and can be used as an alternative method for biometric systems like, iris, fingerprint, etc. Hence provides high level security to the mobile devices like smart phones, tablets etc, and also to other security systems.

ACKNOWLEDGMENT

The research in this paper is used in Idiap Research Institute, Martigny, Switzerland. Various researches based on this face biometrics are proposed in order to provide security systems and also applied m mobile devices.

REFERENCES


