A Novel Approach For Face Liveness Detection To Avoid Face Spoofing Attacks

Meenakshi
Research Scholar, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: minakshisaini26@gmail.com
Dr. Chander Kant
Assistant Professor, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: ckverma@rediffmail.com

---ABSTRACT---

Face recognition is one of the most commonly used biometric technology to recognize an individual from a digital image or a video frame from a video source. Face recognition is more user friendly and cost-effective solution than other biometric technologies. Face recognition system can be spoofed by placing photo/video/mask or dummy face of the enrolled user in front of the camera. In order to enhance the security of system and minimize the spoofing attacks, liveness detection is integrated within the system and is added just before the face recognition module. The aim of liveness detection is to verify that the data is from a live user and is not generated by the artificial sources. In the proposed approach, the facial features of human face such as eye blinking and lip movement are used for liveness detection. User is asked to perform some activities such as eye movement and lip movement according to some random challenge generated by the system and then sequence of images are captured by the camera. After that, the facial features are located and variations in these facial features are computed. If the variations are greater than threshold value and also, the given challenge is equal to the desired response, then the user is considered as a "Live User" otherwise it is considered as a "Fake User".

Keywords- Biometrics, Face Recognition, Liveness Detection, Spoofing

1. Introduction

Biometrics is a modern authentication technology that provides the highest level of security. Biometrics authenticates a person by measuring and analyzing his physical and behavioral body traits. Physical traits of a person are fingerprint, face, iris, hand geometry etc and behavioral traits of person include voice, signature, gait, keystroke pattern etc. Today, Biometrics is a need of all businesses and modern authentication applications because it can accurately distinguish between a genuine user and an imposter. It is also superior to the traditional authentication technologies (token based and knowledge based) because biometric data can't be easily shared, hampered, forgotten or stolen. (Jain, Ross, & Prabhakar, 2004)

Face recognition is a widely used biometric technology that uses human face to authenticate an individual from a digital image or video frame from a video source. The key advantage of this technology is that it does not need much attention from user i.e. user friendly. Face recognition has potential applications in access control, surveillance, ATM's, unlocking software and applications, criminal investigations, attendance systems etc.

Face recognition technology generally involves the following steps as shown in Fig.1:

- Image capture

The first step is to acquire the facial image of user from the camera.

- Face detection

At the second step, face is detected from the acquired image. It can also be normalized or enhanced for further processing.

- Feature Extraction

At the third step, face recognition process takes place in which the desired facial features are extracted.

- Matching

These extracted features are matched against the features stored in the database.

- Determine identity

Finally, the output of face recognition process is used (if there is a match or not) to determine the identity of the person.

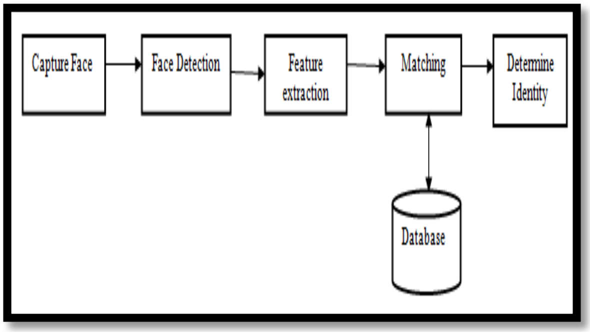

Fig 1: Various steps in face recognition

Spoofing is the major problem faced by the biometric authentication systems. Biometric spoofing is a method of fooling a biometric system by presenting an artificial object to the scanner or sensor so that system will not be able to differentiate between a real object and an artifact. Attacker can attack at any stage (sensor level, feature level, matcher level etc.) of biometric system. Sensor is the most vulnerable part of biometric system (Sharma & Kant, Fake face detection based on skin elasticity, 2013) and is accessible to every user. E.g. of sensor attack is placing fake finger at sensor made up of some material such as rubber etc.

Another kind of attack in biometrics is Replay attack. In replay attack, previously submitted biometric data of legitimate user is resent again and again to the system. Other attacks are modifying the extracted features in feature extraction module by the attacker. Similarly, matcher and decision module can be overridden by the attacker. Enrollment database can also be attacked by modifying or removing/adding templates in the database.

A face recognition system is also prone to the spoofing attacks. Our biometric facial data can be easily stolen from social sites and other personal web sites. Most common attack on face recognition system is the photograph attack i.e. placing photographs in front of camera. Other facial spoofing attacks are playing video of genuine user in front of camera and using 3D dummy faces or mask. (Chakraborty & Das, 2014)

In order to minimize such problems, Liveness detection is integrated within the system. Method of liveness detection detect physiological signs of life from face ensuring that only live face samples are stored for enrollment or authentication.

In the proposed work, eye and lip variations are detected in face for liveness. A random challenge is generated by the system. If variations in both eye and lip region is found greater than threshold value and given challenge is equal to response then the user is live otherwise it is considered as a fake user.

This paper is organized as follows: Section 2 gives an overview of face liveness detection, section 3 describes related work, Section 4 describes the proposed work and finally, section 5 gives conclusion and future scope of proposed work.

2. Face Liveness Detection

Liveness detection technique ensures that the input biometric sample is from a live user and it is not generated artificially. A liveness detection technique can be introduced in a biometric system by three ways:

- By using extra hardware

An extra hardware is used to detect the liveness in the input biometric sample of the user. This is an expansive method due to the cost of adding the extra device to detect liveness but faster than other methods.

- By using some software

In this method, software is used to detect the liveness in a biometric sample. It can be done at the processing stage. The advantage of this method is that it is less costly than hardware based methods but is comparatively slower than the first method.

- Combination of both hardware and software

We can also use the combination of both hardware and software techniques for liveness detection. (Sharma & Kant, Fake face detection based on skin elasticity, 2013)

Various intrinsic properties of human body such as absorbance, reflectance, resistance and elasticity etc and involuntary signals of human body such as blood pressure, brain wave signals etc can also be used for detection of life signs.

Liveness detection generally takes place at the acquisition stage or processing stage.

A Face recognition system can be spoofed by three ways:

- Placing photograph of valid user in front of camera.
- Playing video recording of genuine user in front of camera.
- Placing 3D mask of enrolled user in front of the camera.

Generally a face can be categorized into two classes:

- Positive class
  Positive class of faces is a genuine face. All genuine faces are made up of human skin. A genuine face has limited variation. (Parveen, Mumtaz, Hanafi, & Wan adnan, 2015)
- Negative class
  A negative class of faces is basically a fake face or spoofed face. Examples of spoofed faces vary from photographs to recorded video and dummy faces. Fake face can be made up of materials like silica gel, rubber, plastic etc. Various kind of fake faces are shown in figure 2. A fake face has much larger variations than a real face. Also, a fake face is indistinguishable under visible light by human eyes.

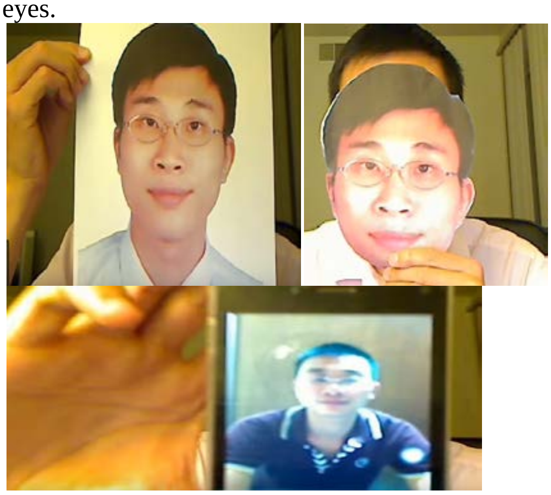

Fig 2: Examples of non real faces. From upper left to right columns, face is made up of photographs, printed mask and in below by the video replay attack as shown respectively. (Jain, Ross, & Prabhakar, 2004)

In face recognition systems, there are three types of liveness indicators:Texture, motion and life sign indicators. In texture based analysis, the texture patterns in face are used to detect the liveness in input facial image.It is a low cost method with simple implementation but can suffer from low texture attacks.

In motion based analysis, it was found that motion pattern of 2D faces was quite different from the 3D faces. It is a medium cost method and require user collaboration.

Life sign indicator method is based on detecting liveness of facial image by analyzing the life signs from face of user such as eye blinking, lip movement etc. These methods are high cost methods but harder to spoof than the other methods.

3. Related Work

In the Literature review of face recognition technology, basically there are two types of approaches: intrusive liveness detection and non - intrusive liveness detection.

Intrusive approaches require user collaboration such as smiling, chewing, rotating head etc. and in non intrusive approaches, there is no user involvement.

(Frischholz & Werner, 2003) proposed an approach in which the user is asked to rotate his head in a particular direction on the basis of the instructions that are randomly generated by the system. A pose estimation algorithm was used to compare the user movements in accordance with the given instructions.

Another approach was proposed by (Kollreider, Fronthaler, Faraj, & Bigun, 2007) that was based on the lip movement. In this approach, user had to utter a random sequence of digits from 0 to 9 and his lip movement is recorded and then recognized sequentially.SVM classifier was used for classification of lip movements.

(Bao, Li, Li, & Jiang, 2009) proposed a method which was based on optical flow field. Optical flow fields generated by 2D planar objects were found to be different than 3D objects. Various properties such as translation, rotation, swing, moving forward and backwards were used.

(Sharma & Kant,2013) proposed a method that was based on fusion of elasticity and thermal imaging. Elasticity value was computed after applying linear discriminant analysis. Thermal sensor was also used.

(Choudhury, Clarkson, Jebara, & Pentland, 1999) proposed a method that was based on the structure from motion and the depth information of the features of face. Main drawback of this method is that it is difficult to estimate the in-depth information when the head is still and also, this method is sensitive to noise.

(Lagorio, Tistarelli, et. al., 2013) proposed an approach which was based on the 3D structure of live face and a 3D scanner was used for this purpose. But the cost is high in this method because it requires an expensive 3D optoelectronic sensor.

(Sun, Pan, Wu, & Lao, 2007) proposed a method that was based on eye blinking. Eye blinking consists of two continuous sub operations i) from opening to closing and ii) from closing to opening. CRF (conditional random fields) model was used for this purpose.

Another method was based on the skin texture analysis that was proposed by (Kim, Eum, et al., 2016). In this method, local binary pattern (LBP) technique was implemented to analyze the texture patterns in the facial image.

4. Proposed Work

4.1 “Liveness Test” in the Proposed Approach

In the proposed approach, two liveness clues are used for detecting the liveness of person:

- Random challenge response method (Dynamic liveness test)
  Challenges are generated randomly by the system so that if the user is live, only he can give response to it. This technique is also called as dynamic liveness test. A challenge is generated in terms of eye and lip movement.
- Variations in the facial features i.e. eye and lip regions
  Another liveness clue that differentiates a real face from a fake face is the variations in facial features of face. Variations are generally produced in eye, lip, nose and forehead regions etc. which are absent in the fake face.

The various steps for Liveness test in the proposed approach are as follows: First of all, system generates a random challenge and asks the user for its response. Random challenges are presented in terms of their eye and lip movement such as blinking right eye, looking up and down or left and right, repeating the randomly generated sequence of digits and phrases by user etc. and then response of user is recorded by the system and sequence of images are captured by camera.

Now from the captured images, facial features of face i.e. eye and lip region are located and variations in these facial features are computed. If the response given by user is equal to the desired response and the computed variations are greater than the threshold value i.e. if both conditions are true, then the user is considered as live otherwise it is considered as a fake user.

The architecture of proposed approach is divided into two steps:
i) Enrollment
ii) Face Recognition

4.2 Enrollment

Enrollment is the process of registering a new user in the database. User must be enrolled in the database before the identification or verification process. In the enrollment phase, raw biometric sample of a user is captured and processed to extract his biometric features and then are stored as templates in the database. These templates are further used for future comparison during the face recognition phase. The proposed approach ensures that during enrollment, only the live biometric samples will be stored in the database. When a new user wants to enroll in the database, the proposed liveness test is performed on the user. If the user passes the liveness test, only then his biometric template is stored in the database otherwise user is not enrolled. Enrollment process can be seen in the flow chart of proposed approach shown in Fig. 4.

4.3 Face Recognition

In face recognition phase, identification or verification of a person is done by using his unique facial characteristics. In face recognition phase, liveness detection module is added just before the face recognition module, which acts as an external layer for enhancing the security of face recognition system. First of all, the user has to pass the liveness test, if the liveness test is passed, only then features are extracted and face recognition is performed otherwise, user is considered as fake and no further action is taken as shown in Fig.3.

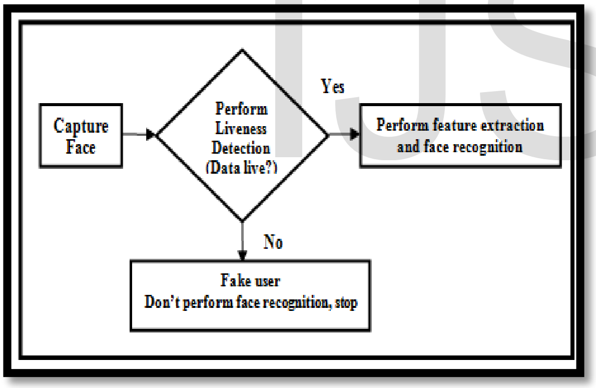
Capture Face
Perform Liveness Detection (Data live?)
Yes
Perform feature extraction and face recognition
No
Fake user
Don't perform face recognition, stop

Fig 3: Basic architecture of liveness detection and face recognition phase in proposed approach

Hence both security and performance of system can be improved because if the user is fake, it is detected by the system at the early stage. We don't need to perform matching and other steps for fake user. Basic flow chart of the proposed approach is shown in Fig 4.

4.4 Proposed Algorithm

1. A Random challenge is generated by the system. System asks the user to perform a sequence of activities containing Eye movement (e.g. open and close, blinking right eye etc.) and lip movement (e.g. Repeating a random sequence of digits & phrases).
2. Capture sequence of images by using a web camera.
3. Locate eye region and lip region of face.
4. Now Extract the edges of the eye and lip regions.
5. Compute the variations using some method such as standard deviation as given in equation 1:

$$\textbf{Standard Deviation}=\sqrt{\frac{\sum z-\bar{z}}{N-1}} \ \text{……...} \ (1)$$

Where z=individual data point, and N= total no.of data points and $\overline{z}$ = mean of vector z.

```
6.  IF (VARIATIONS >TH1 {threshold 1}
            AND
    (CHALLENGE = = RESPONSE) THEN
7.        User is "LIVE".
8.        Extract the features using some feature
          extraction technique to generate the feature
          set.
9.        Match the extracted feature set with the
          corresponding template in the database.
10.       IF (Match score >TH2 {threshold 2})
          THEN
11.       User is "Genuine".
12.       ELSE
13        User is "Not Genuine"
          END
     END
14. ELSE
15.     User is "Not Live" and Reject.
     END
16. EXIT.
```

4.5 Basic Flow Chart of the Proposed Approach

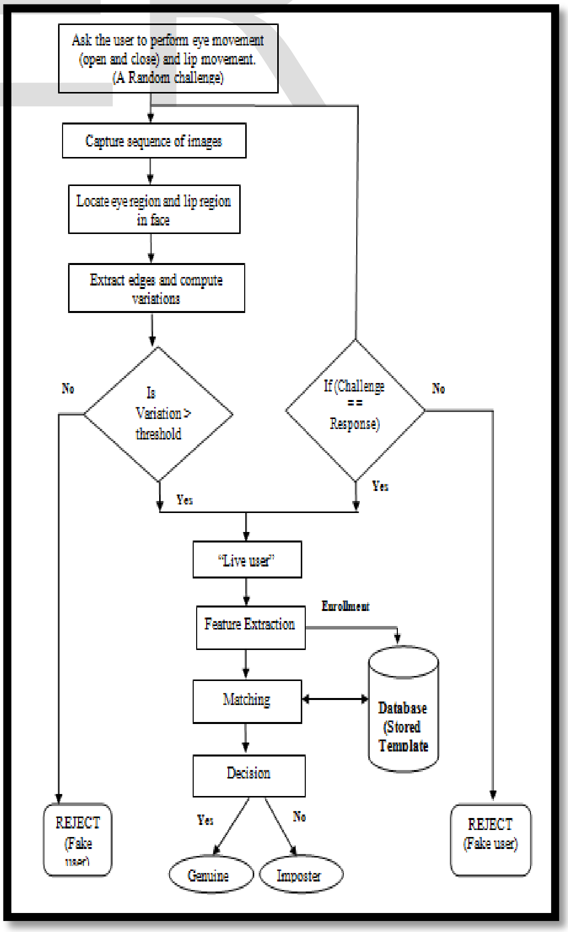
Ask the user to perform eye movement (open and close) and lip movement. (A Random challenge)
Capture sequence of images
Locate eye region and lip region in face
Extract edges and compute variations
No
Is Variation > threshold
Yes
If (Challenge == Response)
No
Yes
"Live user"
Feature Extraction
Enrollment
Matching
Database (Stored Template
Decision
Yes
No
Genuine
Imposter
REJECT (Fake user)
REJECT (Fake user)

Fig 4: Basic Flow chart of Proposed Approach

In the proposed approach, two liveness clues are used: challenge response method and facial variations. If both tests are passed, only then the user is live otherwise it is considered as fake user and rejected as shown in the Table 1:

Table 1: Overall Result for various cases of liveness clues in proposed approach

Liveness Clue 1 Result	Liveness clue 2 Result	Overall result (LIVE/FAKE)
Challenge = Response	Facial Variations>TH1 (threshold)	
YES	YES	LIVE
YES	NO	FAKE
NO	YES	FAKE
NO	NO	FAKE

5. Comparison of the Proposed Approach with Existing Techniques

Proposed approach has many advantages than the traditional approaches and is stated as given below:

- In the proposed approach, system generates a random challenge. Challenges are generated to test whether the person is live or not. If the person is live then he can move his face and facial features too, but it may not be true for some cases. This assumption will fail when attacker plays any recorded video of the genuine user, hence the random challenges are generated in such a way that only the person who is live, can only response to those. Hence this method becomes effective against video replay attacks. In the proposed approach, challenges are presented in terms of their eye and lip movement.
- Facial variations are also used as a liveness indicator in this approach, which helps in fighting against photograph and printed mask attacks because a photograph and printed mask is not able to produce facial variations.
- In the proposed approach, Liveness module is added before the face recognition module. If liveness test is passed, then only face recognition take place. For fake users, we don't need to perform further steps. Hence, both security and performance of system can be improved.

6. Conclusion & Future Work

Liveness detection technique is necessary because it determines whether the user to be recognized is live or not. If the user is live, only then the person is enrolled or recognized, otherwise it is rejected. In the proposed approach, two liveness clues are used: (i) random challenge response method (also called as dynamic liveness test) and ii) variations of facial features for checking the liveness of individual. Both these techniques when together applied, give a better solution to fight against the photograph attacks and video replay attacks in face spoofing. In future, this approach can be further implemented practically on the set of large database.

References

- Bao, W., Li, H., Li, N., & Jiang, W. (2009). liveness detection method for face recognition based on optical flow field. *International Conference on Image Analysis and Signal Processing IASP* (pp. 233–236). IEEE.
- Chakraborty, S., & Das, D. (2014). An overview of face liveness detection. *International Journal on Information Theory (IJIT) , 3* (2), 11-24.
- Choudhury, T., Clarkson, B., Jebara, T., & Pentland, A. (1999). Multimodal person recognition using unconstrained audio and video. *International Conference on Audio- and Video-based Biometric Person Authentication,(AVBPA'99)*, (pp. 176–181).
- Frischholz, R. W., & Werner, A. (2003). Avoiding Replay-Attacks in a Face Recognition System using Head-Pose Estimation. *IEEE International Workshop on Analysis and Modeling of Faces and Gestures(AMFG'03)*, (pp. 234–238).
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *Circuits and Systems for Video Technology. 14.* IEEE Transactions on.
- Kim, G., Eum, S., Suhr, J. K., Kim, D. I., Park, K., & Kim, J. (2016). Face Liveness Detection Based On Texture And Frequency Analysis. *5th IAPR International Conference on Biometrics (ICB)* (pp. 67-72). New Delhi: IEEE.
- Kollreider, K., Fronthaler, H., Faraj, M., & Bigun, J. (2007). Real time face detection and motion analysis with application in liveness assessment . *Trans. Infor. Forensics and Security* (pp. 548-558). IEEE.
- Lagorio, A., Tistarelli, M., Cadoni, M., Fookes, C., Clinton, B., & Sridha, S. (2013). Liveness detection based on 3D face shape analysis. *International Workshop on Biometrics and Forensics (IWBF)* (pp. 1-4). Lisbon: IEEE.
- Parveen, S., Mumtaz, S., Hanafi, M., & Wan adnan, W. A. (2015). Face anti spoofing methods. *Current Science , 108* (8), 1491-1500.

- Sharma, N., & Kant, C. (2013). Fake face detection based on skin elasticity. *International Journal of Advanced Research in Computer Science and Software Engineering , 3* (5), 1048-1051.
- Sharma, N., & Kant, C. (2013). Fake Face Recognition using Fusion of Thermal Imaging and Skin Elasticity. *IJCSC , 4* (1), 65-72.
- Sun, L., Pan, G., Wu, Z., & Lao, S. (2007). Blinking-Based Live Face Detection Using Conditional Random Fields. *International Conference, ICB* (pp. 252-260). Corea: Springer.