A Study of Liveness Detection in Face Biometric Systems

S.Hemalatha
Assistant Professor
Department of Computer Applications
Sri Ramakrishna Engineering College
Coimbatore-22, India

Amitabh Wahi, Ph.D
Professor
Department of Information Technology
Bannari Amman Institute of Technology
Sathyamangalam, India

ABSTRACT
"Biometrics" refers to the technologies that measure and analyze human body characteristics for security purposes. The need of privacy and security in our daily life leads to this new area. Biometric systems have more accuracy when compared to traditional methods (password, key etc). It identifies and verifies the identity of a person based on one or more physiological and behavioral characteristics. That is Human body as password. The most common physical biometric traits includes fingerprint, face, ear, iris, retina, hand geometry, palmprint, DNA etc. Behavioral biometric traits include signature, gait, key strokes, speech patterns etc. Each biometric has its own strength and limitations and accordingly each biometric is used in identification (authentication) application. This paper concentrates on spoof attack against face recognition system, i.e. in this type of attack a fake biometric can be presented to sensor.

This paper discusses about Introduction to The Face biometric system, Spoofing attack in Face recognition system, Liveness detection in face recognition system, Literature survey on Face Liveness detection and conclusion.

Keywords
Image processing, biometric system, liveness detection, spoofing attack

1. INTRODUCTION
Face recognition systems are part of facial image processing applications. It has been an active research topic in the last two decades and its techniques are currently deployed in access control systems. It is the most natural means of biometric identification and has the advantage of non-intrusiveness over the other biometric techniques such as irises and finger prints. So these systems can be used for crime prevention, video surveillance, person verification, and similar security activities. But even though the biometric systems add an additional layer of security than traditional methods by secure identification and authentication, they are still vulnerable to attacks. These attacks are grouped into 8 classes.

1) Spoof attack (a fake biometric sample to the sensor), 2) Replay attack (Replay of stored biometric signals), 3) Substitution attack, 4) Attack on genuine feature values (Spoofing the biometric feature), 5) Trojan horse attack (Denial of feature extraction), 6) Attacks on template database(i.e. spoofing templates in database). Database are the very important parts of biometric systems and attacker mostly attack on template and database. So securing them is a very crucial issue [13]), 7) Transmission attack(Attacking the channel between the database and matching), 8) Attack on final result(accept/reject) [12].

Among those attacks here discussion is about spoofing attack. That is due to technological advancement one can easily spoof into a biometric system and reduces the security as well as the reliability of biometric system. Spoofing attack is especially relevant to behavioral traits (voice, signature), but physical traits such as fingerprint, face, iris are also susceptible to spoof attack [7]. Examples are artificial fingerprint made from silicon, by using face mask, lens including iris texture etc.

Though biometric provides high level of security, sound principles of system engineering are still required to guarantee a high level of security [9].

2. SPOOFING ATTACK IN FACE RECOGNITION SYSTEM
There are two types of spoofing attacks. They are i) digital (vulnerable data path) and physical attacks(clone of legitimate user)[7].

Using any of the method, biometric identifiers can be copied and used to destroy many existing biometric systems. Therefore the challenge is to find the biometric traits on which effective liveness detection can be performed and its mechanism [7].

In face recognition system, the usual attack methods are stolen photo, stolen face photos, recorded video, 3D face models with the abilities of blinking and lip moving, 3D face models with various expressions. That is the biometric traits are made up of silicon, gelatin, play-doh etc.

Among that the facial photograph is the most common way to spoof face recognition systems, because it is relatively easy to obtain a valid user's photos from public and also spoofing face recognition systems with photos or videos of someone else is very easier (figure 1).The main characteristic of the photograph is that it is a planar object without varying facial expressions and three dimensional information.

Fig 1: Spoofing attack using photograph

Videos of valid users are also not difficult to get nowadays. Spoofing videos have more physiological clues than photos, such as eye blinks, facial expressions, and head movements. High quality spoofing videos are almost the same as live faces

in a non-intrusive scenario. 3D models of a valid user, such as wax, are much more difficult to obtain than videos and photos. But it has distinct 3D structure which videos and photos do not have. 3D model can imitate rigid head motions by rotation.

So spoofing attacks is a major problem for face recognition system to be used as a biometrics for high-security applications. Actually in the face recognition environment, numerous recognition approaches are available, but the efforts on anti-spoofing are still very limited. So nowadays the research is going mainly on anti-spoofing part of face recognition system. The most accurate methods in literature to address this problem, depends on the estimation of the three-dimensionality of faces, which heavily increase the whole cost of the system[11].

3. LIVENESS DETECTION IN FACE RECOGNITION SYSTEM

To make face recognition as a successful biometric technology, it is needed to overcome the spoofing attack problem. Thus to overcome spoofing problems, liveness detection is the only method of solution. It is a technique that can be used for validating whether the data is actually from a valid user or not. It gives a strong guarantee for reliable face recognition system.

So Liveness detection plays important role here. That is anti-spoofing measures are highly desirable. Liveness detection denotes the methods capable in discriminating real human traits (live or non-live) from synthetic human traits made by silicon, gelatin or play-doh etc. and photos or videos of someone else. This detection can take place either at acquisition stage or at processing stage. This part could be integrated into an existing face recognition system. The research on liveness detection is highly desirable.

Liveness detection using facial features in biometric system is a method that captures the image of the person and test for his/her liveness after getting authenticated. [8]

In a biometric system there are three ways for introducing liveness detection: Here fake and real images are classified by either

1. Using extra hardware: This approach is an expensive but fast approach(Deploying an excessive and costly system configuration (e.g several cameras including stereo, heat sensitive cameras, etc.)[10].
2.Using software: It is done at processing stage. It is less costly but takes much time in comparison to first.
3. Using combination of hardware and software: This is expensive as well as time consuming. But it provides a good high end solution for livenesss detection which is difficult to breech[4].

Thus Liveness detection technique can be a hardware based or software based or a combination of both.

To detect liveness, various approaches have been proposed. These approaches are classified into four groups. They are 1. Exploiting inherent characteristics of a live face without any user interaction e.g., eye blinking (i.e to bye pass client interaction, few images containing some natural motion is sufficient for reliable liveness detection.[10] 2. Using additional light sources or sensing devices, e.g., thermal imaging sensors 3. Multi-modal approach e.g., Fusion of more than one source (face & finger print) 4. User interactions i.e. demanding real time responses e.g., mouth movement [10].

4. LITERATURE SURVEY ON FACE LIVENESS DETECTION

August 2010 Gang Pan, Lin Sun, ZhaohuiWu and YuemingWang[1] developed a non- intrusive face liveness detection system by combining eyeblink and scene context. Anti spoofing clues i.e both inside a face (eye blinks) and outside a face(scene context) are used in this system. Eyeblinks are employed for anti-spoofing of photographs and 3D models while the scene contexts are used for anti-spoofing of video replays. Outside-face clues can serve as an effective supplement to inside-face clues. Here eyeblink behaviors are modeled in a Conditional Random Field framework and incorporated with a discriminative measure of eye states. There are three-state set for eyes, $Q = \{\alpha : open, \gamma : close, \beta : ambiguous\}$. Thus, a typical blink activity can be described as a state change pattern of $\alpha \rightarrow \beta \rightarrow \gamma \rightarrow \beta \rightarrow \alpha$. With the idea of the adaptive boosting algorithm, a real-value discriminative feature for the eye image, called *eye closity*, *U(I) is defined as* measuring the degree of Eye's closeness. If the value of *closity is higher*, then the degree of eye closeness is also higher.

For scene context analysis, left and right parts beside the detected face are taken as scene region for its rich anti-spoofing clues. The choice of region selection is based on : (1) The top and bottom parts near a face are hair and neck but not the scene; (2) The region far from a face is not considered as scene context, because the spoofing video scene does not appear in that selected region. Scene context analysis has to work fine even though a noise is present in the video, such as changes of illumination, for robust scene comparison.

Thus here a set of key Points called fiducial points in the scene are extracted for comparison. These points represent the uniqueness of the scene as much as possible. This fiducial point-based representation can also reduce computational cost in the subsequent post-processing steps. After setting fiducial points the local texture characteristics at each fiducial point in both an input image *Ii* and a reference scene image *IR are described* for scene matching. Here S is Face Image sequence and *IR is reference image(scene image without any person), N* is the number of fiducial points for each frame. Therefore, whether the scene of image sequence S matches the reference scene can be determined by comparing the scene matching score with a predefined threshold η.

Then results from eyeblink and scene context are combined to give final result of Liveness detection (Figure 2). Thus the clues of eyeblinks and scene context in combination, improves the liveness detection rate to 99.5% .

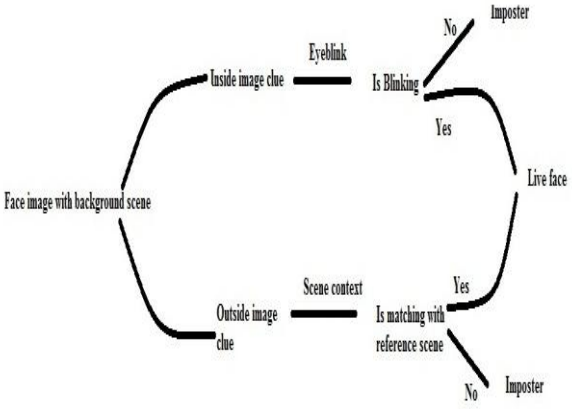

Fig 2: Liveness detection using eyeblink and scene context

In may 2011 Younghwan Kim, Jang-HeeYoo and Kyoungho Choi[2] developed a Face Recognition system in which a motion and similarity-based fake detection algorithm is used for Liveness detection. This approach is based on the idea that there should be a difference in the amount of motion obtained in a video sequence between fake and live situations. It shows that the motion and similarity of the background region contains lot of information for liveness detection. In a live video, the motion is only on the foreground region but not on the background region. Here first initial background image is captured. Then from the current video, face is detected using AdaBoost algorithm and the background image part is also captured from that video. The foreground region is extracted using a simple mask. Then structural similarity index measure (SSIM) is used to compare two background regions, that is, initial and current. If the output of SSIM [20] is one then two images are identical else it is fake image. Then background motion index (BMI) is calculated which shows the amount of motion in the background region compared with the foreground region. If the value of BMI is small, it shows that the background region has less motion, that is the current video is live video but if the value of BMI is close to 1, then there is lot of motion on background region which shows that the current video is fake.

This is a novel fake detection approach using just a regular USB camera without using any additional hardware. This system shows that a motion and similarity of the background region contains key information for liveness detection. They concluded that the performance of this system will be improved when the foreground object is extracted more accurately using more sophisticated object detection approach.

In 2012 Maciejsmiatacz[3] developed a new method to measure the liveness of face images using combination of optical flow estimation and SVM classifier. Optical flow is a set of translations describing the motion. It represents motion in a form of a vector field that allows to transform one image from the video sequence into the next one, by moving the blocks of the first image in the direction given by the vector field components. Even though this technique provides good results, motion field gets noisy when artificial objects are subjected to this technique (figure 3).Thus best algorithm must be selected and prepared to handle the unstable data.

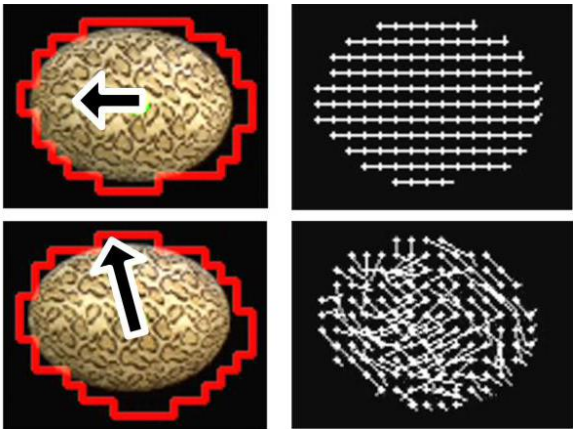

Fig 3: Ideal motion field & Distorted motion field

So in this paper liveness detection procedure calculates optical flow value of face region by using tensor based algorithm proposed by Farneback (figure 4).At first the sequence of frames containing face images are extracted, then optical flow is calculated. To calculate optical flow, calculate the velocity vector v for each pixel which gives the information about the speed and the direction in which the pixel is moving. The optical flow converts each frame of the video sequence into a set of vectors which indicates the direction and velocity of motion between consecutive frames that contains important information about the type of motion and the object itself. After determining motion vector, velocity information is the only parameter used here i.e the length of the motion vector. Thus motion of the object is given by optical flow. So the optical flow is the most effective motion description. Then the motion information is converted into images and the initial data selection is taken. Thus optical flow gives only motion information. But the goal here is to decide whether the given information is live or fake. To make decision classifier is needed.

(i) (ii)

Fig 4: Optical flow extracted by Farneback algorithm: i) live frame, ii) fake frame.

Here the classification algorithm called the Support Vector Machine is used as classifier to differentiate fake and live images. SVM classifier is trained with the sequences of bitmaps which represents motion of real faces and the movements of photos (fake data) and the third kind of data called ambiguous frames(**D***ij*= **L***i* – **F***i* falls below a threshold). **L***i*- frame from the "live" training set .**F***j* - *frames* from the "fake" dataset.

Each observation from the training set is treated as a point in *N*-dimensional space and the SVM classifier tries to find the hyper plane separating samples of opposite classes that

guarantees the widest possible margin separating the samples. Actually SVM is a binary classifier. But in this algorithm the three categories of motion frames are defined (live, fake, ambiguous) so the multi class version of the SVM is applied here.

After liveness test the trained SVM classifier assigns each bitmap from the sequence to one of the classes.

NL, the number of "live" frames,
NF, the number of "fake" frames,
NA, the number of "ambiguous" frames

The false rejection rate of this method is 8.9% and False Acceptance rate is = 0%. Even though they showed high success rate, they decided to add the *temporal* information in their next version in the decision process to improve the robustness of the algorithm. Currently they classified only the individual "motion frames" determined with the optical flow. In next version they planned to analyze the whole sequence of motion changes to improve the performance and make it as robust algorithm to introduce it in real time biometric systems.

The problems faced by this system are
1) When a person rotated the head too fast, many frames were dropped.
2)In poor illumination conditions the useful information gets close to the noise level and the measurements become unstable.
3) It is difficult to cheat the system by rotating the conventional flat photograph, but the results are much more worrying (liveness close to 50%) when the intruder crops the face precisely and uses it as a kind of a simple 3D mask attached to the head.

In March 2013 Dr.Chander Kant and NitinSharma[4] developed non-intrusive and real time method to address spoofing problem based on fusion of thermal imaging(hardware based) and skin elasticity(software based) of human face. Skin elasticity is normal visible face recognition while thermal imaging is a thermal technique that capture image using heat property of the image. That is the thermal IR sensor measures only the heat energy radiation, not the reflectance, from the object. So it is less sensitive to the face appearance variations caused by illumination changes.

Thermal imaging is capable of identifying fake face and images captured from photo or video. Skin elasticity is capable of distinguishing fake faces that uses gelatin, rubber, clay etc. So by combining these two techniques, best performance is achieved in liveness detection.

In this system, face image is captured using camera sensor and thermal sensor at the same time. Before capturing, user is requested to perform some live activities (smile, forehead movement) to get full movement of face skin. Skin elasticity is a visible face detection method. Here a number of face images are captured at a particular interval and those images are compared with each other to detect whether the image captured are real image or fake images.

Then thermal image and one image from set of image sequence taken by camera sensor are taken for processing. These images are converted into gray scale and then to binary image. The superimpose matching score is calculated for those images. If the score is greater than threshold value then the image is real else fake image. Thus the results of these two liveness detection techniques are combined to identify real face from fake faces.

In May 2013 Annu and Dr. Chander Kant [5] developed a Face Recognition system in which Euclidean distance test (EDT) is used for checking a person's aliveness which ensures the detection of fake/dummy images.

A biometric camera is used to capture the user's face images and it produces a sample. Then Euclidean distance is applied to ensure that an input image is actually from a valid user instead of face photos or any other artificial sources. Here the same person's face images are captured under the three different profiles 1. Left, 2.Right and 3.Front in a random order(it may be LFR, LRF, FLR, RLF, RFL, FRL whereas L denotes the left profile and R denotes the right profile and F denotes the front profile of a person) and the Euclidean distance is measured from the captured face images. If these values are dissimilar then the image is actually a real user, else artificial sources are used.

To calculate the difference between the Euclidean distances of the two different images of the same person they used $D(x,y)=\{(x_i-y_i)^2\}^{1/2}$

Then *td* value is calculated by

$$Td=d(x_i,y_i)-d(x_{i+1},y_{i+1})$$

Td is the difference between the Euclidean distances of the two images. If it is not equal to zero then the image is real one and responding to Euclidean distance test else it is coming from a fake biometric system or any other artificial sources.

The main advantage of this system is that if the image is detected as fake one in the Euclidean distance test, then it reports it as fake image and the further computations are not done on that image. If the image is found real, only then the further calculations ie face normalization, feature extraction and matching process are performed for face recognition. The future enhancement of this system is reported as to identify a person at a few meters distance.

In May 2013 Dr.Chander Kant and Nitinsharma[6] developed a non-intrusive and real time method to address spoofing problem based on skin elasticity of human face. This is a software based liveness detection method. Here the users are asked to do some simple mouth movement activities, forehead movement etc to get full movement of face skin. At that time a sequence of face images are captured within a gap. Then after pre-processing, feature extraction is done using correlation coefficient and image extension feature. Using discriminant analysis method, images are discriminated and skin elasticity is calculated. The result is then compared with the database value. If the output is less than the threshold value then the image is a detected as fake image else it is a real image. Thus face skin is discriminated from other artificial sources. Here threshold value is decided based on age because it plays an important role in skin elasticity. If image is identified as real one then Face recognition process is performed.

5. CONCLUSION

Face recognition system gives secure identification and authentication. But these systems are also vulnerable to spoofing attacks. There are many proposed methodologies that are used to overcome spoofing attacks. Here some of the methods are discussed along with their future enhancement.

The future enhancement can be focused on Liveness detection to overcome the drawbacks of those existing systems. Research should be made to find more number of effective and feasible liveness detection techniques and will continue working in this area and come out with commercially accepted liveness detection schemes for face recognition systems in near future.

6. REFERENCES

[1] Gang Pan, Lin Sun, zhaohuiwuand yuemingwang - Monocular camera-based face liveness detection by combining eyeblink and scene context, TelecommunSyst (2011), Published online on 4 August 2010.

[2] Younghwan Kim, Jang-HeeYoo - A Motion and Similarity-Based Fake Detection Method for Biometric Face Recognition Systems, IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.

[3] Maciejsmiatacz- Liveness measurement using optical flow for Biometric person Authentication, Metrology and Measurement systems, Vol. XIX (2012), No. 2, pp. 257-268.

[4] Chander Kant, Nitin Sharma, -Fake Face Recognition using Fusion of Thermal Imaging and Skin Elasticity, IJCSC vol4 , No. 1 March 2013 pp. 65-72.

[5] Annu and Chander Kant - Liveness Detection in Face Recognition Using Euclidean Distances,international journal for advance research in engineering and technology Vol. 1, Issue IV, May 2013.

[6] Chanderkant & Nitinsharma –Fake FaceFace Detection Based on Skin Elasticity, international journal of advanced research in computer science and software engineering, Vol. 3, Issue 5, May 2013.

[7] Mohmad Kashif Qureshi – Liveness Detection of Biometric Traits, International journal of information Technology and knowledge Management, Vol 4, No.1 , pp. 293-295,January - june 2011.

[8] Sanjeevakumar M. Hatture, Nalinakshi B.G , Rashmi P. Karchi –Prevention of spoof attack in Biometric system using Liveness Detection, International Journal of Latest Trends in Engineering and Technology (IJLTET), Special Issue - IDEAS-2013, ISSN: 2278-621X

[9] Debnath,B, Rahul Ranjan, Farkhod Alisherov A and Minkyu Choi. Biometric Authentication: A Review - International Journal of u- and e- Service, Science and Technology. Vol. 2, No. 3, September, 2009.

[10] K. Kollreider, H. Fronthaler and J. Bigun, Halmstad University, SE-30118, Sweden -Evaluating Liveness by Face Images and the Structure Tensor, Published in: "Automatic Identification Advanced Technologies, 2005", Fourth IEEE Workshop on 17-18 OCT 2005, pg.no: 75-80,

[11] Gahyun Kim, Sungmin Eurn, Dong Ik Kim, Jaihie Kim, Jae KyuSuhr- Face Liveness Detection Based on Texture and Frequency Analyses, published in Biometrics(ICB), 2012 5th IAPR International Conference on biometrics, IEEE, on March 29 2012-April 1 2012, pg.no 73-78.

[12] Fargana Abdullayeva, yadigar imamverdiyev, vugar musayev, james wayman- Analysis of security vulnerabilities in Biometric systems,Science Direct 2006.

Manvjeet kaur, sangeev sofat , Deepak saraswat - Template and Database Security in Biometrics Systems: A Challenging Task , International Journal of Computer Applications (0975 – 8887) Vol 4 – No.5, July 2010