Fusion of Multiple Biometric For Photo-Attack Detection in Face Recognition Systems

Ms. Deveshree R. More
Department of Computer Engineering
YTCEM
Bhivpuri Road, Karjat.
deveshreemore@gmail.com,

Prof. Vanita Mane
Department of Computer Engineering
RAIT
Nerul, Navi Mumbai
vanitamane1@gmail.com

Abstract— A spoofing attack is a situation in which one person successfully masquerades as another by falsifying data and gaining illegitimate access. Spoofing attacks are of several types such as photograph, video or mask. Biometrics are playing the role of a password which cannot be replaced if stolen, so there is the necessity of counter-measures to biometric spoofing attacks. Face biometric systems are vulnerable to spoofing attack. Regardless of the biometric mode, the typical approach of anti-spoofing systems is to classify the biometric evidence which are based on features discriminating between real accesses and spoofing attacks. A number of biometric characteristics are in use in various applications. This system will be based on face recognition and lip movement recognition systems. This system will make use of client-specific information to build client-specific anti-spoofing solution, depending on a generative model. In this system, we will implement the client identity to detect spoofing attack. With this, it increases efficiency of authentication. The image will be captured and registered with its client identity. When user has to be authenticated, the image will be captured with his identity manually entered. Now system will check the image with respect to client identity only. Lip movement recognition will be done at time of authentication to identify whether client is spoof or not. If client is authenticated, then it will check for captured image dimension using Gaussian Mixture Model (GMM). This system also encrypts and decrypts a file by extracting parameter values of a registered face.

Keywords-*Biometric system, Face recognition system, Spoofing, Anti-spoofing*

*****

I. Introduction

Passwords and ID cards are commonly used to restrict access to a variety of systems. However, security can be easily breached when a password is revealed to an unauthorized user or a card is stolen by an impostor. Biometrics is better way than traditional security. Biometrics refers to the automatic identification or verification of an individual or a claimed identity by using certain physiological or behavioral traits associated with the person. Biometrics allows us to establish an identity based on 'who you are', rather than by 'what you possess' (e.g. an ID card) or 'what you know' (e.g. a password). Most of the installed biometric systems make use of fingerprints, hand geometry, iris, and face to establish a person's identity. In addition to enhanced security, biometric systems also introduce an aspect of user convenience. For example, they obviate the need to remember and maintain multiple passwords [1].

Face recognition system is the high possibility of the system being deceived or spoofed by non-real faces such as photograph, video clips or dummy faces. Anti-spoofing is a method used to automatically distinguish between real biometric traits presented to the sensor and forged one. The fact that the biometric traits cannot be kept secret should not be an obstacle for using biometrics. Such reasoning has inspired an ever increasing number of liveness detection and anti-spoofing algorithms for many biometric modes. Non-invasive, user friendly, fast, good performance, low cost is some of the requirement of good anti-spoofing technique. Anti-spoofing techniques are mainly classified into: texture, motion and life sign. Texture analysis techniques take the advantage of detectable texture patterns such as print failures, and overall image blur to detect attacks. Motion analysis differentiates the motion pattern between 3D and 2D faces. Detection of life signs can be of two types. First one assumes some known interaction from the user. The second category focuses on certain movements of certain parts of the face, such as eye blinking and considers those movements as a sign of life and therefore a real face. Some anti-spoofing techniques uses specific hardware device ensuring the presence of a living person in front of the system. Others combine multiple modalities, presuming that this increases the difficulty of spoofing the system .Among systems which depend on additional hardware or require user interaction, software-based solutions which use only the evidence taken by the biometric sensor may be the most favorable due to their inexpensiveness and convenience of use [2].

Face recognition is also useful in human computer interaction, virtual reality, database recovery, multimedia, computer entertainment, information security e.g. operating system, medical records, online banking., Biometric e.g. Personal Identification - Passports, driver licenses, Automated identity verification - border controls , Law enforcement e.g. video surveillances , investigation , Personal Security – driver monitoring system, home video surveillance system[3].

II. Review of Literature

In [4], to resist the main fake approach, i.e., using a photo to spoof the face recognition system, a new technique based on the analysis of 2-D Fourier spectra is proposed. In [5], authors says that when an image is displayed or printed on a medium and captured again, the image obtained is technically an image of the medium only. The main idea is to detect the properties of the medium in question and not what the medium seems to look like. The approach discussed in [6], analyzes the texture of the facial images using multi-scale local binary patterns (LBP) and encodes the micro-texture patterns into an enhanced feature histogram. The results are then fed to a support vector machine (SVM) classifier. In [7], a novel and appealing approach to detect face spoofing using the spatiotemporal (dynamic texture) is introduced which is an extension of the highly popular local binary pattern operator. The key idea of the approach is to learn and detect the structure and the dynamics of the facial micro-textures that characterize real faces but not fake ones. In [8], face part detection and optical flow estimation are combined to determine a liveness score. The purpose of this system is to assist in a biometric authentication framework, by adding liveness awareness in a non-intrusive manner. The degree of difference between the fields generated by movements of 2D planes and 3D objects is used to distinguish between a 3D face and 2D photograph in [9]. The high correlation between the movements of the face region and the background as an indication of a spoofing attack is used in [10]. In [11], a linear fusion combination between static and video analysis is proposed. In [12], fusion of motion and texture based countermeasures under several types of scenic fake face attacks is addressed.

III. PROBLEM STATEMENT

The anti-spoofing systems are designed as binary classifiers whose task is to distinguish between real access and spoofing attack samples, with no regards to the client identity. The face anti-spoofing features proposed in the literature uses several aspects for differentiating between real accesses and spoofing attacks, like texture quality, motion patterns etc., and they show great discrimination capabilities between the two classes of samples. The extracted anti-spoofing features are influenced by the characteristics of the individual clients and may retain some client-specific information. This information may be useful to make better discrimination between the real accesses and spoofing attacks of a particular client. If client specific information is used with face anti-spoofing features, there would be great improvement over client-independent approaches which do not use information about the client identity. So, there is need to implement a face anti-spoofing system based on client identity.

The drawback of existing system is that face detection and client ID verification is done separately and score of both are combined to detect the user is spoofed or real. It takes more time to display the result. This drawback will overcome by proposed work by detecting face and if it is real then only it will go for client ID verification else it will display the user as a fake. The proposed system will upload and download the files by using various parameters of captured image as a key.

IV. PROPOSED WORK

In the proposed system client-specific information is used to build client-specific anti-spoofing solution, depending on a generative model. In proposed system, the client identity will be implemented to detect spoofing attack. With this, it increases efficiency of authentication .The image will be captured and registered with its client identity. When user has to be authenticated, the image will be captured with his identity manually entered. Now system will check the image with respect to client identity only. It will check for captured image dimension using Gaussian Mixture Model (GMM) and if it authenticated then it will go for client identity verification. The client identity spoofing can be detected with the help of lip movement recognition at time of authentication. This system will also encrypt and decrypt a file by extracting parameter values of a registered face of a registered client.

A. Architecture

A biometric system is a pattern recognition system that operates by acquiring biometric data from a user, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Here, three modules of biometric system are designed: 1. Enrollment of user 2.Uploading a file 3. Downloading a file.

Enrollment of users: Fig 1 shows the architecture of enrollment of users. Following are the steps for the enrollment:

1. Give all the details of the client.
2. Register the client identity and face of the client using sensor. This module captures the biometric data of an individual.
3. Define the parameters of the biometric data. This is called as feature extraction. This module gets the biometric data and processes it to extract a set of salient or discriminatory features.
4. Store the extracted features in the database.

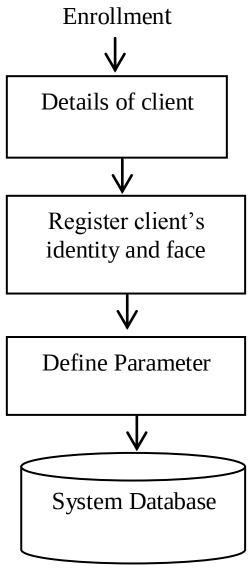

Fig 1: Enrollment Process

File uploading process: Fig 2 shows the architecture of file uploading. Following are the steps for downloading process:

1. The user interested for uploading files has to login first.
2. Check whether the interested user is valid or not. This is done by matcher module, in which the features extracted during recognition are compared against the stored templates to generate matching scores.

3. If match is found, then a file is encrypted using face parameters and total characters of files.

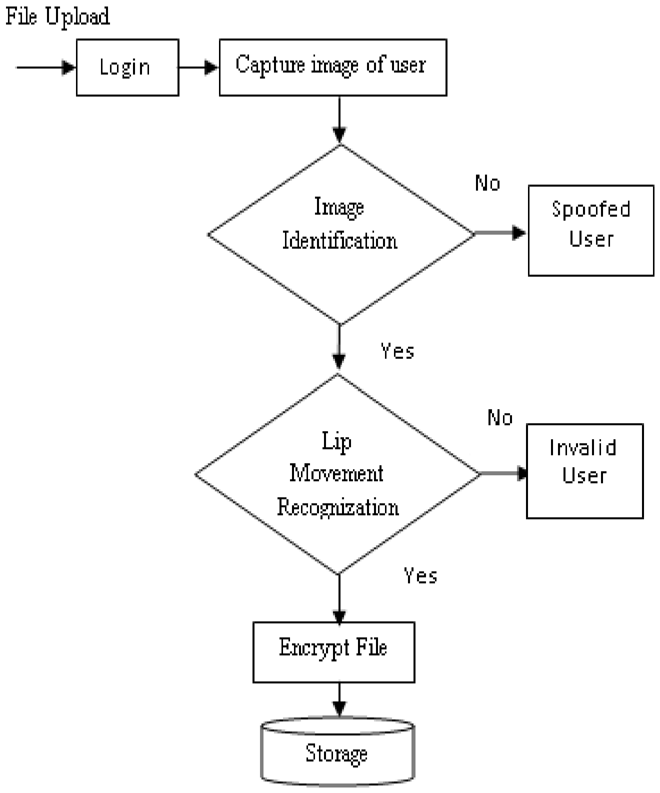

Fig 2: File Uploading Process

4. Take text to be encrypted, fetch parameter value to encrypt the text, store the encrypted values into system with field.

File Downloading: Fig 3 shows the flow of file downloading process. Following are the steps for downloading process:
1. The user interested for uploading files has to login first.
2. Lip movement recognition is done. If is it recognized then move further or considered the user as spoofed user.
3. Image of user is captured and processed for face identification. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to many comparisons to establish an individual's identity.
4. If image is identified as a valid user then he is allowed to select a file for decryption.
5. Fetch parameter value to decrypt selected field. Decrypt the file and get plain text as output.
6. Decrypted file is displayed

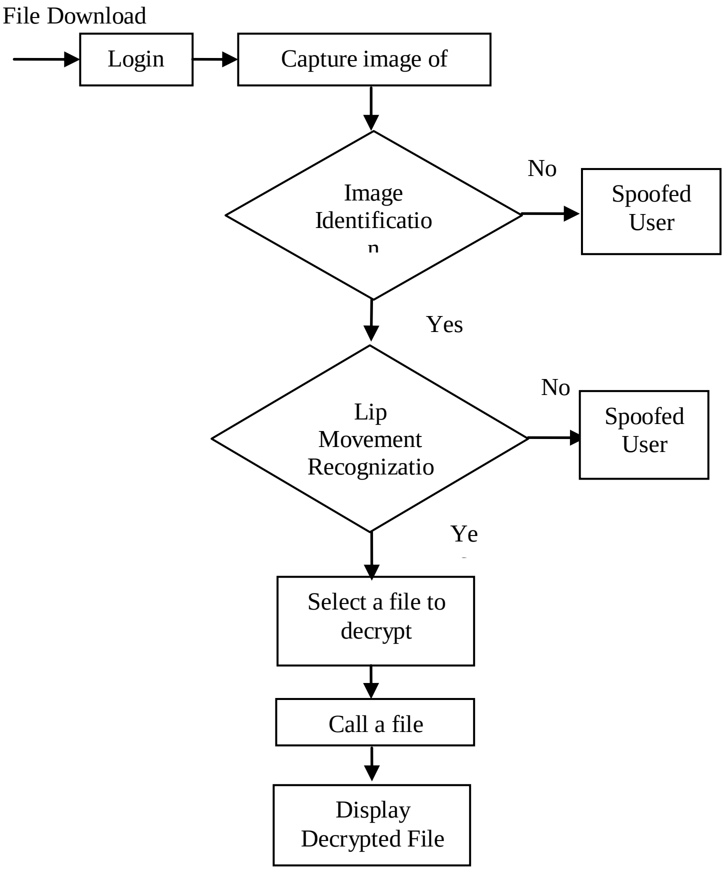

Fig 3: File Downloading Process

A. *Lip Movement Recognition Algorithm*

1. Face Localization: A user's face is detected in every image frame captured by a web camera.
2. Mouth Region Localization: Then, a mouth region is localized and its shift from the reference mouth position is calculated.
3. Detection of lip region and lip shape: A small region (blob) placed on user lip is found in mouth region. This blob is used as a starting condition for an iterative method for lip shape extraction.
4. Gesture Recognition: Lip shape and lip region image features are used by an decision system to classify gestures made by a user [13].

B. *Algorithm of Overall System*

Consider N samples are with us.
1. From each sample we can obtain K parameter.
2. Now we can have two hypotheses H0 and H1.
3. H0 - can be build up using samples registered with the system.
4. H1 - samples which were to be authenticated but failed during authentication.
5. Considering image to be authenticated x.
6. For all samples we will consider image vector of x and will compare with H0 samples.
7. If any image is matched with x then face is detected goto 8 else goto 10.
8. Check for lip position of the authenticated face; if it is same as in registered then image is detected with complete authentication else go to 9.
9. Image is authenticated but may be spoofed.
10. Image is not authenticated. Register into non-authenticated database with time and date if available increase hit counter, else store with hit = 1.
11. If encryption, take text to be encrypted, fetches parameter value to encrypt the text, store the encrypted values into system with field.
12. If decryption fetch parameter value to decrypt selected field. Decrypt the file and get plain text as output.

V. Evaluation Parameters

1. False Positive (FP): Mistaking biometric measurements from two different persons to be from the same person is called false positive.

2. False Negative (FN): Mistaking two biometric measurements from the same person to be from two different persons is called false negative.

3. False Positive Rate (FPR) or False Acceptance Rate (FAR): The False Accept Rate (FAR) describes the proportion of identification or verification transactions in which an impostor subject was incorrectly matched to a genuine user template stored within a biometric system. It corresponds to the ratio between FP and the total number of negative samples.

4. False Negative Rate (FNR) or False Rejection Rate (FRR): The False Reject Rate (FRR) describes the proportion of identification or verification transactions in which a genuine subject is incorrectly rejected from a biometric system. It corresponds to the ratio between FN and the total number of positive samples.
5. Equal Error Rate (EER): The EER is the value where FAR and FRR are equal. The lower the equal error rate value, the higher the accuracy of the biometric system.
6. Total Error Rate (TER): The TER consists of the sum of the False Accept Rate (FAR) and the False Reject Rate (FRR).
7. Half Total Error Rate (HTER): The HTER is an aggregate of FAR and FRR.
8. Decision Threshold (τ): It is computed to serve as a boundary between the output scores of the positive and the negative class. By changing this threshold one can balance between FAR and FRR. Increasing FAR reduces FRR and vice-versa.

VI. Conclusion

Anti-spoofing systems are most frequently designated to secure and work in cooperation with biometric recognition systems. A client-specific anti-spoofing system will be implemented based on generative model which use client identity information to detect spoofing attacks. Using client identity information can be of great help in successfully detecting spoofing attacks. Performance of this anti-spoofing system can be better as compared to the existing anti-spoofing systems which does not use information related to client identity. This system will encrypt and decrypt a file only if there is genuine user.

References

[1] Anil K.Jain And Arun Ross, Department Of Computer Science And Engineering, "Learning User-Specific Parameters In A Multibiometfuc System", Michigan State University, East Lansing, MI 48824.

[2] Ivana Chingovska And André Rabello Dos Anjos, "On The Use Of Client Identity Information For Face Antispoofing", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 4, April 2015.

[3] Divyarajsinh N. Parmar, Brijesh B. Mehta," Face Recognition Methods & Applications", IJCTA , Vol 4(1),84-86 Jan-Feb 2013.

[4] J. Li, Y. Wang, T. Tan, And A. K. Jain, "Live Face Detection Based On The Analysis Of Fourier Spectra," Proc. SPIE, Vol. 5404, Pp. 296–303,Aug. 2004.

[5] J. Bai, T.-T. Ng, X. Gao, And Y.-Q. Shi, "Is Physics-Based Liveness Detection Truly Possible With A Single Image?" In Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), May/Jun. 2010, Pp. 3425–3428.

[6] J. Määttä, A. Hadid, And M. Pietikäinen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis," In Proc. Int. Joint Conf. Biometrics, Oct. 2011, Pp. 1–7.

[7] T. De Freitas Pereira Et Al., "Face Liveness Detection Using Dynamic Texture," EURASIP J. Image Video Process., Vol. 2014, P. 2, Jan. 2014.

[8] K. Kollreider, H. Fronthaler, And J. Bigun, "Non-Intrusive Liveness Detection By Face Images," Image Vis. Comput., Vol. 27, No. 3, Pp. 233–244, 2009.

[9] W. Bao, H. Li, N. Li, And W. Jiang, "A Liveness Detection Method For Face Recognition Based On Optical Flow Field," In Proc. Int. Conf. Imageanal. Signal Process., 2009, Pp. 233–236.

[10] J. Yan, Z. Zhang, Z. Lei, D. Yi, And S. Z. Li, "Face Livenessdetectionby Exploring Multiple Scenic Clues," In Proc. 12th Int. Conf. Controlautom. Robot. Vis., 2012, Pp. 188–193.

[11] R. Tronci Et Al., "Fusion Of Multiple Clues For Photo Attack Detection Inface Recognition Systems," In Proc. IJCB, Oct. 2011, Pp. 1–6.

[12] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, And S. Marcel,"Complementary Countermeasures For Detecting Scenic Face Spoofingattacks," In Proc. Int. Conf. Biometrics (ICB), 2013, Pp. 1–7.

[13] PiotrDalka,AndrzejCzyzewski,"Human-Computer Interface Based On Visual Lip MovementAnd Gesture Recognition",nternational Journal of Computer Science and Applications,Technomathematics Research FoundationVol. 7 No. 3, pp. 124 - 139, 2010.