International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Antispoofing Methods for Authenticating Live Users in Biometric System

[1]Anita Kori, [2]Swathi S. Wali, [3]Sanjeev Kumar M. Hatture, [4]Dr. Suvarna Nandyal

[1, 2, 3]Department of Computer Science and Engineering, Basaveshwara Engineering College, Bagalkot, Karnataka, India
[4]Department of Computer Science and Engineering, P.D.A College of Engg, Gulburga, Karnataka, India

Abstract: ***In today's e-commerce world the e-business application require a very high level of authentication, as the existing traditional authenticating methods such as username, password, identity card etc can be easily stolen. To alleviate such problems the new authenticating methods using physiological/behavioral biometrics are emerged. Even the biometrics systems are fooled by spoofing techniques with fake biometric traits such as masked face, iris, fake finger print, hand geometry, voice and many more. Spoofing is an attack when a malicious party impersonates another device or a user on a network/system in order to launch attacks against new hosts/system. Hence, the anti-spoofing methods required to challenge the intruders of the biometric system. However, spoofing attack is still a fatal threat for biometric authentication systems. Liveness detection, aims at recognition of human physiological activities as the liveness indicator to prevent spoofing attack. This paper presents an overview of different anti-spoofing methods used with biometric system. It also highlights the issues, challenges and applications of biometric systems with anti-spoofing techniques.***

Keywords: Authentication, spoofing, biometric, anti-spoof, liveness detection.

1. Introduction

Biometric devices, such as fingerprint, face, iris, voice, and handprint recognition, have been suggested for use in applications from access to personal computers, automated teller machines, credit card transactions, electronic transactions to access control for airports, nuclear facilities, and border control. Given this diverse array of potential applications, biometric devices have the potential to provide additional security over traditional security means such as passwords, keys, signatures, picture identification, etc. While biometrics may improve security, biometric systems also have vulnerabilities such as being spoofed by artificial fingers or, in the worst case, dismembered fingers.

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past several years as most of the liveness parameters exist in it. Even though current machine recognition systems have reached a certain level of maturity, their success is limited by the conditions imposed by many real applications. For example, recognition of face images acquired in an outdoor environment with changes in illumination and/or pose remains a largely unsolved problem. In other words, current systems are still far away from the capability of the human perception system.

The spoofing attack is a fatal threat for biometric authentication systems. Liveness detection, which aims at recognition of human physiological activities as the liveness indicator to prevent spoofing attack, is becoming a very active topic in field of fingerprint recognition and iris. There are two different ways to introduce liveness detection into fingerprint recognition systems: at the acquisition stage or at the processing stage. The first method uses extra hardware to acquire life signs. For example, measuring fingertip temperature, pulse, pulse oximetry, blood pressure, electric resistance, odor. These methods introduce difficulties because it is expensive and bulky. Furthermore, it may still be possible to present an artificial fingerprint to the fingerprint sensor and utilize the real fingerprint of the intruder for the hardware to detect liveness. The second method uses the information already captured by the system to detect life signs, for example, skin deformation, pores or perspiration pattern. Skin deformation technique uses the information about how the fingertip's skin deforms when pressed against the scanner surface. However, using a thin artificial fingerprint glued on a live finger may still generate a similar non-linear deformation as a live finger would. The in 2nd section the brief survey of different anti-spoofing methods used with biometric system is discussed followed by the 3rd section which summarizes the issues and challenges and finally the 4th with application of biometric system with anti-spoofing techniques.

2. Review of Literature

Recently liveness Detection with recognition of Face, Eye, Iris are having much attention in the emerging area of Biometrics. Some of the liveness detection methods for anti-spoofing methods are summarized in the following;

A. Introduction to Face Recognition Technology. A Framework is made on face recognition system, and the variants that are frequently encountered by the face recognizer. Several famous face recognition algorithms, such as Eigen faces and neural networks, will also be explained. Among the various biometric ID methods, the physiological methods (fingerprint, face, DNA) are more stable than methods in behavioral category (keystroke, voice print) [1]. The reason is that physiological features are often non-alterable except by severe injury. The behavioral patterns, on the other hand, may fluctuate due to stress, fatigue, or illness. However, behavioral IDs have the advantage of being no intrusiveness. People are more comfortable signing their names or speaking to a microphone than placing their eyes before a scanner or

giving a drop of blood for DNA sequencing. Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness. It has the accuracy of a physiological approach without being intrusive. Face recognition has drawn the attention of researchers in fields from security, psychology, and image processing, to computer vision. Below figure describes about the working of face recognition System.

B. Image Based Face Recognition Issues and Methods. A general statement of face recognition problem can be formulated as follows. Given still or video images of a scene identify or verify one or more persons in the scene using a stored database of faces Available collateral information such as race age gender facial expression and speech may be used in narrowing the search enhancing recognition [2]. The solution of the problem involves segmentation of faces, face detection from cluttered scenes, feature extraction from the face region recognition or verification. Some issues are addressed Among those issues the following two are prominent for most systems the illumination problem and pose problem. Solutions to these problems are discussed in terms of methods as:

Solving the Illumination Problem

They are classified into four types:

- Heuristic Methods: Including discarding the leading principal components.
- Image Comparison Methods: where various image representations and distance measures are applied.
- Class Based Methods: where multiple images of one face under a fixed pose but different lighting conditions are available
- Model Based: Approaches where 3D models are employed.

Solving the Pose Problem

Some of the methods have been proposed to handle the rotation problem. Basically they can be divided into three classes:

- Multiple Images Based Methods: when multiple images per person are available.
- Hybrid Methods: when multiple training images are available during training but only one database image per person is available during recognition.
- Image Shape Based methods when no training is carried out.

3D Model Enhanced Face Recognition

- The subspace LDA systems. It was proposed with the motivation of trying to solve the generalization over fitting problem when performing face recognition on a large face dataset but with very few training face images available per class.
- A varying albedo illumination model for face.
- The Self ratio image rI.

The concept of self ratio image was initially introduced in to address the additional parameter. The idea of using two aligned images to construct a ratio has been explored by many researchers But it was extended to a single image in fig. Based on this concept new shape from shading SFS scheme has been developed.

- Using a generic 3D face shape.

C. Access control: Adaptation and Real Time Implantation of a Face Recognition Method. Here we present the adaptations needed for public use of this kind of control, and the performance evaluation of the modified method [3]. Some of the methods have been introduced. Face verification software have been implemented, used for PC or building access control, improving the feature computation and separability of the learning sets in the feature space. In terms of performance, it has been shown that each person can be easily recognized and that the software can be used in a real environment. Measurement of the recognition rate and the adjustment of the classification method must be adapted to the acquisition protocol to be significant.

D. A Survey of 3D Face Recognition Methods. The main purpose of this overview is to describe the recent 3D face recognition algorithms. The last few years more and more 2D face recognition algorithms are improved and tested on less than perfect images [4]. However, 3D models hold more information of the face, like surface information, that can be used for face recognition or subject discrimination. Another major advantage is that 3D face recognition is pose invariant.

3D Supported 2D Models

Zhao and Chellappa proposed a shape-from-shading (SFS) method for preprocessing of 2D images. This SFS-based method used a depth map for generating synthetic frontal images.

Local Methods

Suikerbuik proposed to use Gaussian curvatures to find 5 landmarks in a 3D model. He could find the correct landmark point with a maximal error. Gordon proposed to use the Gaussian and cean curvature combined with depth maps to extract the regions of the eyes and the nose. He matched these regions to each other and reached a recognition rate of 97% on a dataset Subjects.

Global Methods

One global method on curvature was lately presented by Wong et al. The surface of a facial model was represented by an Extended Gaussian Image (EGI) to reduce the 3D face recognition problem to a 2D histogram comparison.

Template Matching Approaches

Blanz, Vetter and Romdhani proposed to use a 3D morphable model for face recognition on 2D images.One can see that the 3D face recognition approaches are still

tested on very small datasets. However, the datasets are increasing during the years since better acquisition materials become available. By increasing a dataset, however, the recognition rate will decrease. So the algorithms must be adjusted and improved before they will be able to handle large datasets with the same recognition performance.

E. Automatic Dry Eye Detection. Here a new method for the automated detection of dry areas in videos taken after instilling uorescein in the tear film. The method consists of a multi-step algorithm to first locate the iris in each image, then align the images and finally analyze the aligned sequence in order to find the regions of interest [5]. Since the uorescein spreads on the ocular surface of the eye the edges of the iris are fuzzy making the detection of the iris challenging. RANSAC is used to detect the upper and lower eyelids and then the iris. Then align the images by finding differences in intensities at different scales and using a least squares optimization method (Levenberg-Marquardt), to overcome the movement of the iris and the shaking of the camera. The method has been tested on videos taken from different patients. It is demonstrated to find the dry areas accurately and to provide a measure of the extent a new method for automatic detection of the tear film breakup area was developed. Method is demonstrated that can find the relevant area and size and build a confidence map.

F. Face Spoofing Detection From Single Images Using Micro-Texture Analysis. Here a new idea is explored on the detection of Spoofing. Spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access [6]. Inspired by image quality assessment, characterization of printing artifacts, and differences in light reflection, we propose to approach the problem of spoofing detection from texture analysis point of view. Indeed, face prints usually contain printing quality defects that can be well detected using texture features. Hence novel approach is presented based on analyzing facial image textures for detecting whether there is a live person in front of the camera or a face print. The proposed approach analyzes the texture of the facial images using multi-scale local binary patterns (LBP). Compared to many previous works, the proposed approach is robust, computationally fast and does not require user-cooperation. In addition, the texture features that are used for spoofing detection can also be used for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition. Extensive experimental analysis on a publicly available database showed excellent results compared to existing works.

- Spoofing Detection using Micro-Texture Analysis

The method aims at learning the fine differences between the images of real face and those of face prints, and then designing a feature space which emphasizes those differences. Method adopts the local binary patterns, a powerful texture operator, for describing not only the micro textures but also their spatial information.

G. Decomposed Eigenface Method along with Image Correction for Robust Face Recognition. [7] Introduces the decomposed eigenface method by introducing a projection-based image correction. The image correction technique is principally authorized when the object shape is fixed and a sufficient number of images are taken beforehand. However, the proposed technique can also be applied to a canonical eigenspace, which is constructed from several faces taken under various lighting conditions. Reflective noises, shadows and occlusions are detected and corrected by the projection of a facial image onto the canonical eigenface. Based on the newly proposed image correction, we develop herein a refined decomposed eigenface method. The experimental results indicate that the refinement works well for face recognition under various lighting conditions, as compared to the original decomposed eigenface method.

H. Probabilistic recognition of human faces from video. Recognition of human faces using a gallery of still or video images and a probe set of video is systematically investigated using a probabilistic framework. In still-to-video recognition, where the gallery consists of still images, a time series state space model is proposed to fuse temporal information in a probe video, which simultaneously characterizes the kinematics and identity using a motion vector and an identity variable, respectively [8]. The joint posterior distribution of the motion vector and the identity variable is estimated at each time instant and then propagated to the next time instant. Marginalization over the motion vector yields a robust estimate of the posterior distribution of the identity variable. A computationally efficient sequential importance sampling (SIS) algorithm is developed to estimate the posterior distribution. Empirical results demonstrate that, due to the propagation of the identity variable overtime, degeneracy in posterior probability of the identity variable is achieved to give improved recognition. The gallery is generalized to videos in order to realize video-to-video recognition. An exemplar-based learning strategy is adopted to automatically select video representative from the gallery, serving as mixture centers in an updated likelihood measure. The SIS algorithm is applied to approximate the posterior distribution of the motion vector, the identity variable, and the exemplar index, whose marginal distribution of the identity variable produces the recognition result. The model formulation is very general and it allows a variety of image representations and transformation.

1. Face modeling and recognition: In statistical approach, the two-dimensional appearance of face image is treated as a vector by scanning the image in lexicographical order, with the vector dimension being the number of pixels in the image.
2. Video-based tracking and recognition: Nearly all video-based recognition systems apply still-image-based recognition to selected good frames. The face images are warped into frontal views whenever pose and depth information about the faces is available.
3. A model for recognition in video: The details on the propagation model are presented for recognition and discuss its impact on the posterior distribution of identity variable.

3.1. A time series state space model for recognition
3.1.1. Motion equation

4. Sequential importance sampling algorithm

Consider a general time series state space model fully determined by;

(i) The overall state transition probability.
(ii) The observation likelihood
(iii) Prior probability and statistical independence among all noise variables.

5. Still-to-video based face recognition

Still-to-video scenarios used in experiments an their practical model choices, followed by a discussion of experiments. Three databases are used in the still-to-video experiments.

6. Video-to-video based face recognition Video-to-video based face recognition approach has been proposed. It enhances the still-to-video approach by taking an entire video, instead of a single image, to represent the face of an individual.

I. Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection. To improve the performance of biometric systems it is of great importance to study its vulnerabilities to external attacks. In the recent years several works have reported experimental results regarding the robustness of automatic recognition systems to direct and indirect attacks. In the present paper a state-of-the-art review of the attacks to fingerprint- and iris-based security systems has been reviewed [9]. Some of the countermeasures based on physiological properties (i.e. liveness detection methods) proposed in the literature to improve the robustness of the systems, are also summarized.

J. Liveness detection using fingerprints

Several methods to discriminate between real and fake fingerprints have been proposed over the last few years. One of the liveness detection is presented where the periodicity of sweat and the sweat diffusion pattern were used to detect fake fingerprints applying a ridge signal algorithm. The same technique but using a wavelet-based algorithm was described. These two works were extended where a new intensity-based perspiration liveness detection technique is described.

K Liveness detection using iris

The experiments reported in and have shown the necessity of incorporating liveness detection techniques in the commercial iris verification applications in order to prevent eventual direct attacks carried out against the system. In the last few years several efforts have been made in this direction, leading to different iris liveness detection methods.

A second group of possible anti spoofing mechanisms highlighted in is those based on behavioral eye features. One of these liveness detection methods is based in the detection of the eye hippos, which is the permanent oscillation that the eye pupil presents even under uniform lighting conditions.

3. Issues and Challenges

- Complexity of the biometric system increases due to increase in additional liveness detection device [10].
- It is often difficult to enforce ideal human-machine interactions. Continuous close supervision is costly and defeats the purpose of automatic authentication, whereas instruction manuals are often neglected by users. Poor human-machine interactions may unnecessarily affect both Failures to Enrol (FTE) as well as Failure to Acquire (FTA) rates.
- Poor human-machine interactions may unnecessarily affect both Failures to Enrol (FTE) as well as Failure to Acquire (FTA) rates.
- Palmprint and palm-vein biometrics system suffer with many messy lines and infrared ray pass through user body.
- In biometric systems, users can be challenged to repeat a particular face, blink their eyes, not head or present specific fingers to the sensors.
- Voice may corrupt due to variation in cold condition [11].

4. Applications

Apart from the different issues and challenges in biometric system there are many different fields in which the method provides more robustness to the system on usage, some of them are listed below:

1) Virtual reality —Interactive virtual world, Games, Virtual studio, Character animation, Teleconferencing (e.g., film, advertising, home-use)
2) "Smart" surveillance systems —Access control, Parking lots, Supermarkets, department stores Vending machines, ATMs Traffic
3) Advanced user interfaces —Social interfaces, Sign-language translation, Gesture driven control Signaling in high-noise environments,(airports, factories),Motion analysis —Content-based, indexing of sports video, footage, Clinical studies of orthopedic patients.
4) Model-based coding —Very low bit-rate video compression [11].
5) Entertainment-Human-robot-interaction, human-computer-interaction, Drivers'licenses, entitlement programs.
6) Smart cards Immigration, national ID, passports, voter registration, Welfare fraud, TV Parental control, personal device logon, desktop logon, Information security.
7) Security, database security, file encryption, Intranet security, internet access, medical records secure trading terminals.

8) Law enforcement Advanced video surveillance, CCTV control and surveillance Portal control, post event analysis.
9) Shoplifting, suspect tracking and investigation

5. Summary

Biometrics is a means of verifying personal identity by measuring and analyzing unique characteristics like fingerprints. Fingerprint is the most popular biometric system that is widely used in various authentication applications, PC logon, gate access control systems, and so on. The reason can be considered that fingerprint can achieve the best balance among authentication performance, cost, size of device, and ease of use. Although biometric authentication devices can be susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks. Multimodal biometric systems have consistently presented better recognition rates.

Unimodal systems are explained. A common claim is that they also provide higher security when compared to unimodal systems since an intruder would have to successfully break into more than one biometrical system. A multimodal system composed of face and fingerprint traits in different spoofing scenarios have been evaluated. The multimodal systems have a very high probability of being spoofed when only one of its modes is spoofed, contrarily to the common belief that several modes must be spoofed to break the whole multimodal system. The implications of these results are worrying: a multimodal system may be easier to spoof than some of the unimodal systems that compose it.

6. Future Work

This paper presents a holistic view on current technical issues and challenges of biometric systems as physical and logical access control tools in information security. Each topic is discussed in terms of various biometric system performances which are deliberated across individual sub-components of biometric system architecture. Amongst the identified issues include (1) The effects of biometric menagerie (2) robustness of the system to actual operating environment (3) security of biometric data within the system (4) concerns over biometric system testing and reporting and (5) assurance of interoperability. These issues can be used as guidelines by the industries with regard to information security policy and decision making. In the future, as the target access control user population increases, we foresee the need for scalable biometric authentication. In addition, biometric-based access control applications may necessitate for ambient intelligence whereby authentication can be carried out without the need for active user participation. In short, both aspects remain as these technical issues to be studied in our future work.

Author Profiles

Mrs. Anita G. Kori currently perceiving PG degree in Computer science and Engineering at Basaveshwar Engineering College Bagalkot-587102, Karnataka, India.

Miss. Swathi S. Wali currently perceiving PG degree in Computer science and Engineering at Basaveshwar Engineering College Bagalkot-587102, Karnataka, India.

Sanjeevakumar. M. Hatture received the Bachelor's Degree in Electronics and Communication Engineering from Karnataka University, Dharwad, Karnataka State, India, and the Master Degree in Computer Science and Engineering from the Visvesvaraya Technological University, Belgaum, Karnataka, India, and currently pursuing PhD Degree in the Research Centre, Department of Computer Science and Engineering at Basaveshwar Engineering College, Bagalkot under Visvesvaraya Technological University, Belgaum, Karnataka, India. His research interests include biometrics, image processing, pattern recognition, Soft computing and network security. He is life member of professional bodies like IEI and ISTE.

Dr. Suvarna Nandyal currently working as Professor Computer science and Engineering at P.D.A College of Engineering, Gulbarga.

References

[1] Shang-Hung Lin, "An Introduction to Face Recognition Technology," IC Media Corporation, Information Science Special Issues on Multimedia Informing Technlogies,Part-2,Vol 3,No1, 2000.
[2] WenYi Zhao, Rama Chellappa, Image Based Face Recognition Issues and Methods, Sarno Corporation Center for Automation Research, Princeton, Washington Road University of Maryland, 2000
[3] J. Mitéran, J.P. Zimmer, F. Yang, M. Paindavoine Access control: Adaptation and Real Time Implantation of a Face Recognition Method, Laboratory Le2i, University of Burgundy, Aile des Sciences de l'Ingénieur, BP 400, 21011 Dijon, France,2000
[4] Alize Scheenstra, Arnout Ruifrok, and Remco C. Veltkamp, A Survey of 3D Face Recognition Methods, Utrecht University, Institute of Information and Computing Sciences, Padualaan, Netherlands, Netherlands Forensic Institute, Laan van Ypenburg 6, 2497 GB Den Haag, The Netherlands, 2001
[5] Tamir Yedidya, Richard Hartley, Jean-Pierre Guillon, and YogesaKanagasingam, Automatic Dry Eye Detection, 2002
[6] Jukka Matta, Abdenour Hadid, MattiPietikainen, Face Spoofing Detection from Single Images Using Micro-Texture Analysis, 2002
[7] Kazuma Shigenari Fumihiko Sakaue Takeshi Shakunaga, Decomposed Eigenface Method along with Image Correction for Robust Face Recognition,

Department of Information Technology, Okayama University, Nara, Japan.

[8] Shaohua Zhou, Volker Krueger, and Rama Chellappa, Probabilistic recognition of human faces from video, Center for Automation Research (CfAR), Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA, February, 2003

[9] Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia, Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection, Biometrics Recognition Group ATVS, Escuela Politecnica Superior Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente, 11Campus de Cantoblanco - 28049 Madrid, Spain 2004.

[10] Sujan T. V. Parthasaradhi, Reza Derakhshani Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices, IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 35, no. 3, august 2005.

[11] Sravya. V, Radha Krishna Murthy, Ravindra Babu Kallam, Srujana B, A Survey on Fingerprint Biometric System, 2012