Multi Biometric System Against On Spoof Attacks

Abitha Rose P[1], Malghija F[2]

[1] *CSE, Bethlahem Institute Of Engineering,Karungal,Tamilnadu,India*
[2] *II year ME Computer Science & Engineering, Bethlahem Institute Of Engineering, Karungal , Tamilnadu, India*

Abstract- Multibiometric systems are vulnerable to presentation attacks, assuming that their matching score distribution is identical to that of genuine users, without fabricating any fake trait. Recently shown that this assumption is not representative of current fingerprint and face presentation attacks, leading one to overestimate the vulnerability of multibiometric systems, and to design less effective fusion rules. In this project, overcome these limitations by proposing a statistical meta-model of face and fingerprint presentation attacks that characterizes a wider family of fake score distributions, including distributions of known and, potentially, unknown attacks. This allows us to perform a thorough security evaluation of multibiometric systems against presentation attacks, quantifying how their vulnerability may vary also under attacks that are different from those considered during design, through an uncertainty analysis. Empirically show that our approach can reliably predict the performance of multibiometric systems even under never-before-seen face and fingerprint presentation attacks, and that the secure fusion rules designed using our approach can exhibit an improved trade-off between the performance in the absence and in the presence of attack. Finally argue that our method can be extended to other biometrics besides faces and fingerprint.

Key Words **-**statistical meta-analysis, uncertainty analysis, presentation attacks, security evaluation, secure multibiometric fusion.

1.INTRODUCTION

1.1 Overview

Security and access control applications in real-life scenario. Despite their widespread use, these systems still remain vulnerable to various sophisticated attacks that undermine the reliability of the biometric system. Among the different forms of attacks that can be performed on the biometric system, the presentation of biometric artifacts at the sensor level has received much attention from the research community. This attack is termed as a direct attack or presentation attack, in which the unauthorized person will present the biometric artifact of the genuine user to the sensor to gain access to the restricted data, resources or premises. The presentation attack is a serious threat as it can be easily performed without any a priori knowledge about the internal operation of the biometric system.

In my recent work, through an extensiveexperimental analysis, we have shown that the aforementioned assumption is not representative of current face and fingerprint presentation attacks. In fact, their fake score distributions do not only rarely match those of genuine users, but they can also be very different, materials, source images used to fabricate the presentation attack; i.e., presentation attacks can have a different impact on the output of the targeted matcher. For these reasons, the methodology proposed in may not only provide an

overly-pessimistic security evaluation of multibiometric systems to presentation attacks, but also lead one to design secure fusion rules that exhibit a too pessimistic trade-off between the performance in the absence of attack.

1.2 Technologies

Biometric technologies automate the process of using a physiological or behavioral characteristic to prove someone's identity. It is closely connected with problems of information security, including criminology. Since, a physiological biometric characteristic tends to have smaller intra class variations; it is more reliable in terms of identification accuracy. Nowadays, nine different biometric techniques exist. This includes face, fingerprint, hand geometry, hand, vein, iris, and retinal pattern, and signature, voice-print and facial thermo gram. Signature and voice print are behavioral biometrics and all others are physiological biometrics. Other biometric technologies include odor, keystroke dynamics, gait, Deoxyribo Nucleic Acid (DNA).

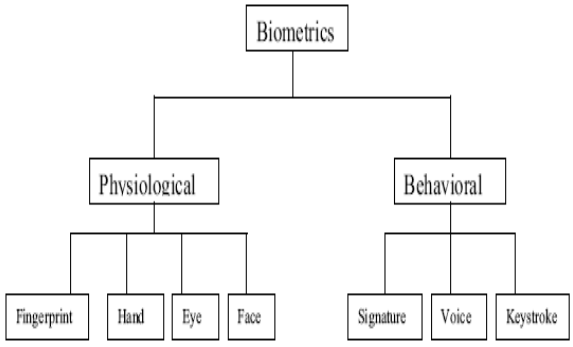

Fig-1Topology of Biometric Identification Methods

1.3 Face Recognition

Facial-scan technology utilizes the distinctive features of the human face to verify or identify individuals. Acquisition for biometric identification purpose requires the individual's face to be proposed to a video camera. An evident deficiency

in some current schemes is the ability to fool or confuse some systems with makeup. Face recognition usually refers to static, controlled full frontal portrait recognition. By 'static', it means that the facial portraits used by the face recognition system are still facial images. One of the very important steps is to determine the best facial features to discriminate one from another. Problem arises when face recognition need to be done under varying poses. Accuracy is affected due to change of hairstyle, lighting and wear of glasses. A face recognition system should not impose any annoying controlled restrictions on how the facial images are acquired.

1.4 IRIS Scan

Iris-scan technology utilizes the distinctive features of the human iris. It has been successfully implemented in ATM's and kiosks for banking and travel applications. Iris scanning is less intrusive than retinal recognition because the iris is easily visible from several feet away. Responses of the iris to changes in light can provide secondary verification that the iris proposeded as a biometric factor is genuine. Though empirical tests with the technology will improve its reliability, it appears quite promising and even practical for many applications, especially two-factor scenarios. While some of the technical issues of iris scanning seem pedestrian, they proposed implementation challenges. A careful balance of light, focus, resolution, and contrast is necessary to extract the attributes or minutiae from the localized image. While the iris seems to be consistent throughout adulthood, it does vary somewhat up to adolescence. It is noted for its accuracy, genetic independence, high processing speed and stability. It also suffers from serious drawbacks which include propensity for false rejection, user discomfort with eye-based technology and high cost with the acquisition device.

Fingerprint

Finger-scan technology utilizes the distinctive features of the fingerprint. It is the most commonly deployed biometric technology. Fingerprint identification techniques fall into two major categories-Automated Fingerprint Identification Systems (AFIS) and fingerprint recognition systems. AFIS is typically restricted to law-enforcement use. Fingerprint recognition derives a unique template from the attributes of the fingerprint without storing the image itself or even allowing for its reconstruction. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical hurdles because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image, so they are less sensitive to dirt and oils. Fingerprint recognition is generally considered reliable enough for commercial use, and some vendors are already actively marketing readers as part of Local Area Network login schemes. It is a mature and proven core technology, capable of high levels of accuracy. It employs ergonomic, easy to use devices. It has the ability to enroll multiple fingers and the sensor cost is also comparatively low. At the same time, some small percentage of user's especially manual workers and elderly people do not have clear fingerprints. Fingerprints are unique to an individual and cannot be easily forged.

Signature Scan

Signature-scan technology utilizes the distinctive aspects of the signature. This technology examines the behavioral components of the signature, such as stroke order, speed and pressure as opposed to comparing the visual images of signatures. Signature is a simple, concrete expression of the unique variations in human hand geometry. Forensic experts have developed criteria over the years for verifying the authenticity of a signature. Automating this process allows computer automation to take the place of an expert in looking for unique identifying attributes.
In addition to the general shape of the signed name, a signature recognition system can also measure both the pressure and velocity of the point of the stylus across the sensor pad. (Keystroke dynamics is a variation on this technique that measures the typing rates and intervals.) Signatures, however, are difficult to model for variation, and users are unaccustomed to signing on tablets. It is resistant to imposters, non-invasive and the users can change the signature.

Hand Geometry

Hand-scan technology utilizes the height and width of the back of the hand and fingers to verify the identity of individuals. The essence of hand geometry is the comparative dimensions of fingers and the locations of joints. Some systems perform simple, two-dimensional measurements of the palm of the hand. Others attempt to construct a simple three-dimensional image from which to extract template characteristics. In one of the most popular descendants of the Identical, a small digital camera captures top and side images of the hand. Reference marks on the platen allow calibration of the image to improve the precision of matching. It is a mature technology and non-intrusive. It is used to maintain attendance record in factories. It is resistive to temperature, humidity and other environmental conditions. Its accuracy is low and the sensor costs high. Also it is difficult to use for some users especially children, arthritis, missing fingers or large hands.

2.PROJECT OVERVIEW

2.1 Project Description

In this work, focus on multibiometric systems exploiting score-level fusion to combine the matching scores coming from K distinct biometric traits. An example for K = 2. During the design phase, authorized clients are enrolled by storing their biometric traits and identities in a database. During the online operation, each user provides the requested biometrics, and claims the identity of an authorized client. The corresponding templates are retrieved from the database and matched against the submitted

traits. The matching scores s = (s1, . . . , sK) ∈ R^K are combined through a fusion rule which outputs an aggregated score f(s) ∈ R. The aggregated score is finally compared with a threshold t to decide whether the identity claim is made by a genuine user (if f(s) ≥ t) or an impostor. Performance is evaluated, as for unimodal systems, by estimating the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) from the genuine and impostor distributions of the aggregated score.

Presentation attacks can target any subset of the K biometrics; e.g., a fake face (e.g., a 3D mask) and/or a fake fingerprint can be submitted to the corresponding sensor. The other impostor's biometrics are submitted to the remaining sensors (if any): such biometrics are said to be subject to a zero-effort attack. In multibiometric systems, the FAR is evaluated when all the biometrics are subject to a zero-effort attack, i.e., against zero-effort impostors].As spoofing attacks affect only the FAR of a given system (and not the FRR), the corresponding performance is evaluated in terms of the so-called Spoof FAR (SFAR) Impostors attempting at least a presentation attack against one of the matchers are referred to as spoof impostors. Different SFAR values can be clearly estimated depending on the combination of attacked matchers, and on the kind of spoofing attacks involved (e.g., one may either use a face mask or a photograph for the purpose of face spoofing). Furthermore, the FAR evaluated against an impostor distribution including both zero-effort and spoof impostors is referred to as Global FAR (GFAR). In the following, to keep the notation uncluttered, we will respectively denote the score distribution of genuine users, zero-effort and spoof impostors at the output of an individual matcher as $p(S_G)$, $p(S_I)$ and $p(S_F)$.

2.2 System Architecture

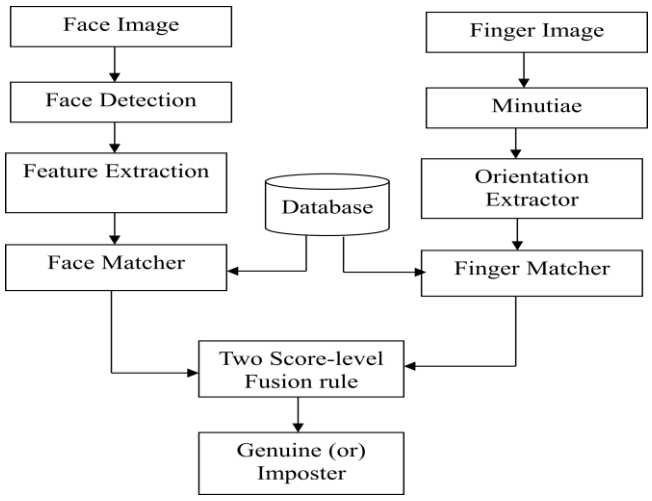

Fig -2 Architecture Diagram

2.3 Modules

The proposed presentation attack detection comprised of four functional units namely.

2.3.1Multibiometric Registration Module

Multimodal biometrics uses information from two or more biometrics. Here, a user registers into the system using face and fingerprint. In design phase, authorized clients are enrolled by storing their biometric traits and identities in a database. In online operation, user provides requested biometrics, and claims the identity of an authorized client.

2.3.2 Face Matcher Module

This module acquires the face biometric data from a user and claims his identity. This module, perform the face detection on each of these images. Thus, given a image is carry out the face detection by employing the Viola-Jones algorithm by considering its robustness and performance in real-life scenarios, the employed face detector is robust enough to detect the face. However, the employed face detector has occasionally resulted in false positives due to the complex backgrounds considered during the data capture. Those false positives that cannot be mitigated using the technique described in are then visually determined and manually rectified to improve the overall performance of the system.

Here, feature extraction module processes the acquired biometric data and extracts a feature set using

PCA. Then the system compares the traits with the templates of the claimed identity provided at enrollment phase.It produces face match score using matching algorithm.

2.3.3 Image Quality Measures

Expected quality differences between real and fake samples may include: sharpness, luminance and artifacts.In this module, a novel parameterization using 5 general image quality features extracted from face image. The 5 features are Edge-based, Spectral distance, Gradient-based, Correlation-based and Corner.Edges and corners are some of the most informative parts of an image.The Fourier transform is a image processing tool applied to the field of image quality assessment.

2.3.4 Fingerprint Matcher Module

This module acquires the finger biometric data from a user and claims his identity. Feature extraction, processes the acquired biometric data and extracts a feature set using Minutiae Extractor and Orientation. Fingerprints can be classified as weakly-order textures exhibiting a dominant ridge orientation at each point. The orientation field provides a rough description of the fingerprint pattern that can be estimated with reasonable accuracy even from noisy input images. Here, characterize the location of each minutia with respect to the input fingerprint pattern based on a descriptor that comprises information about the orientation field in a broad region around the minutia point.

The sampling points assigned to each minutia can be organized in a circular pattern around the minutia

position.Then the system compares the traits with the templates of the claimed identity provided at enrollment phase. It produces finger match score using matching algorithm.

2.3.5 Score-level Fusion Rule

This module combines the matching scores coming from two biometric traits and outputs are aggregated score. Here, spoofing-aware score-level fusion rules are proposed based on LLR rule. This rule includes the probability of attempting a presentation attack against each matcher. It estimate fake score distribution by fitting a Gamma distribution on the corresponding training data. If an attack is attempted, then corresponding score follows a distribution of zero-effort impostors.

2.3.6 Fuzzy Logic Fusion Rule

Here, spoofing-aware score-level fusion rules are proposed based on Fuzzy Logic. In the fuzzification step, each one of the inputs is modelled as a fuzzy variable.A membership function maps each fuzzy variable into a real number on the [0, 1] range. Choosing an appropriate membership function is crucial for keeping the linguistic expression meaningful.For the high quality linguistic expression, we choose a min–max function. Similarity scores with low quality should have low weights in the final output.

2.3.7 Identification Module

First, matching scores is combined by two biometric traits and outputs are aggregated score. The aggregated score is finally compared with a threshold t to decide whether genuine user or impostor.

3.Result

Face Detection

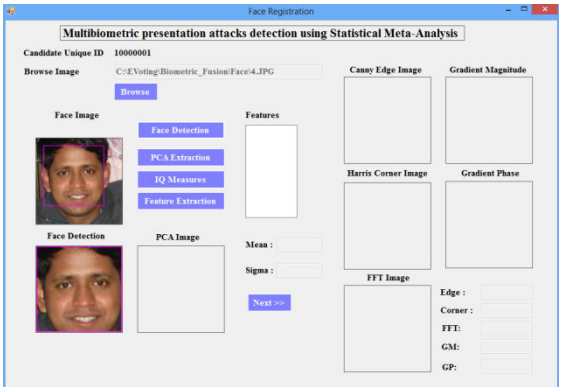

Fig -3 Face detection

Face Feature Extraction

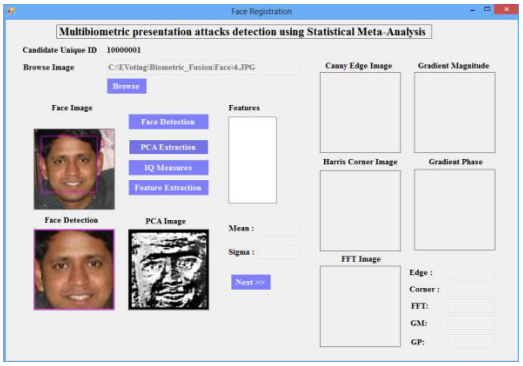

Fig -4 Face feature extraction

Image Quality Measures

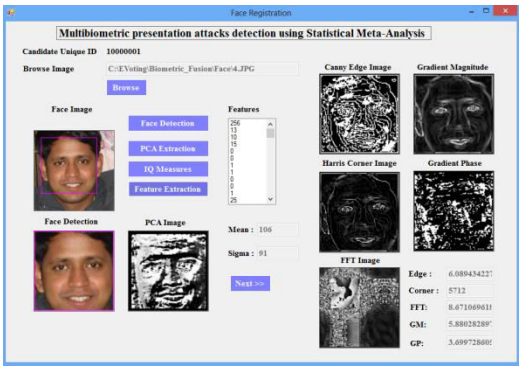

Fig -5 Image quality measures

Finger-Orientation Extractor

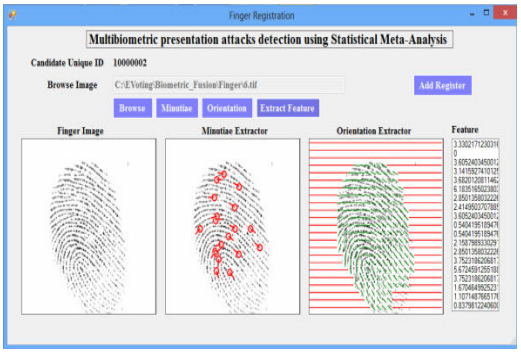

Fig -6 Finger orientation extractor

Election Candidate Registration

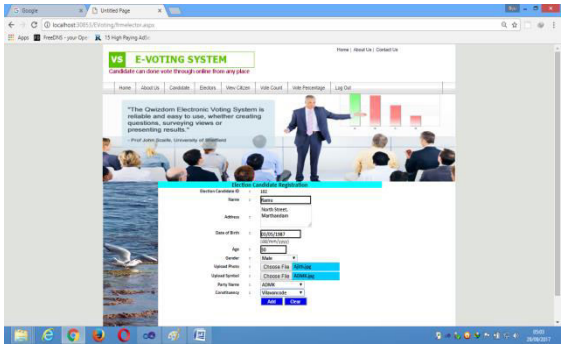

Fig -7 Election Candidate Registration

Vote Registration

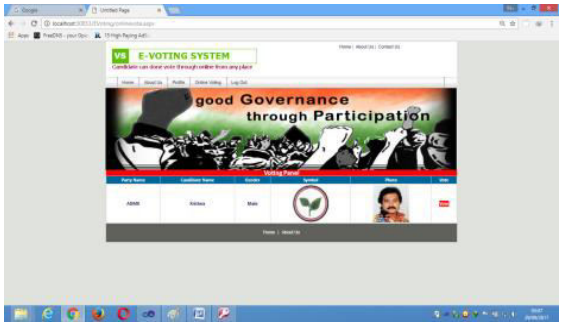

Fig -8 Vote registration

4.CONCLUSION

Proposed an approach to thoroughly assess the security of multibiometric systems against presentation attacks, and to improve their security by design, overcoming the limitations of previous work. Our approach is grounded on a statistical meta-model that incorporates knowledge of state-of-the-art fingerprint and face presentation attacks, by simulating their matching score distributions at the output of the attacked matchers, avoiding the cumbersome task of fabricating a large, representative set of attacks during system design. It also allows us to simulate perturbations of such distributions that may correspond to unknown attacks of different impact, through an uncertainty analysis. This aspect is specifically important, as attackers constantly aim to find novel evasion techniques. In the case of biometric systems, this means that novel, unexpected attacks may be encountered in the near future. For instance, it has been claimed that it is not possible to forecast all potential face spoofing attacks and fake fabrication techniques, as humans can always find very creative ways to cheat a system. Our uncertainty analysis aims thus to overcome this issue. We showed empirically that our approach provides a much more informative security evaluation of multibiometric systems, characterizing the behavior of the system also under never-before-seen attacks, and enabling the design of improved secure fusion rules.

ACKNOWLEDGMENTS

The authors would like to thank all those who have extended their support for successful completion of this work.

REFERENCES

1. A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: a public database and a baseline,” in Biometrics (IJCB), 2011 International Joint Conference on, pp. 1–7, IEEE, 2011.

2. J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live face detection based on the analysis of fourier spectra,” in Defense and Security, pp. 296–303, International Society for Optics and Photonics, 2004.

3. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Li, “A face antispoofing database with diverse attacks,” in 5th IAPR International Conference on Biometrics (ICB), pp. 26–31, March 2012.

4. J. Galbally, S. Marcel, and J. Fierrez, “Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition,” IEEE Transactions on Image Processing, vol. 23, pp. 710– 724, Feb 2014.

5. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” in International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–7, Sept 2012.

6. N. Erdogmus and S. Marcel, “Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect,” in Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on, pp. 1–6, IEEE, 2013.

7. A. Anjos, M. M. Chakka, and S. Marcel, “Motion-based countermeasures to photo attacks in face recognition,” IET Biometrics, 2013.

8. J. M. A. Hadid and J. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” in International Joint Conference on Biometrics (IJCB), pp. 1–7, Oct 2011.

9. J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li, “Face liveness detection by exploring multiple scenic clues,” in Control Automation Robotics & Vision (ICARCV), 2012 12th International Conference on, pp. 188–193, 2012.

10. N. Kose and J. Dugelay, “Classification of captured and recaptured images to detect photograph spoofing,” in Informatics, Electronics Vision (ICIEV), 2012 International Conference on, pp. 1027–1032, May 2012.

11. N. K. Ratha, J. H. Connell, and R. M. Bolle, “An analysis of minutiae matching strength,” in AVBPA, ser. LNCS, J. Bigun¨and F. Smeraldi, Eds., vol. 2091. Springer, 2001, pp. 223–228.

12. A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” EURASIP J. Adv. Signal Process, vol. 2008, pp. 1–17,2008.

13. B. Biggio, G. Fumera, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective," IEEE Sig. Proc. Mag., vol. 32, no. 5, pp. 31–41, Sept2015.

14. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Im- pact of artificial "gummy" fingers on fingerprint systems," Daten- schutz und Datensicherheit, vol. 26, no. 8,2002.

15. B. Geller, J. Almog, P. Margot, and E. Springer, "A chronological review of fingerprint forgery," J. Forensic Sc., vol. 44, no. 5, pp. 963–968, 1999.

16. Y. Kim, J. Na, S. Yoon, and J. Yi, "Masked fake face detection using radiance measurements," J. Opt. Soc. Am. A, vol. 26, no. 4, pp. 760–766,2009.

17. G. Fumera, G. L. Marcialis, B. Biggio, F. Roli, and S. C. Schuckers, "Multimodal anti-spoofing in biometric recognition systems," in Handbook of Biometric Anti-Spoofing, ser. Advances in Computer Vision and Pattern Recognition, S. Marcel, M. Nixon, and S. Z. Li, Eds. Springer, 2014, pp.165–184.