Enhancing Biometric Liveness Detection Using Trait Randomization Technique

Kenneth Okereafor
Department of Information Systems,
University of Azteca,
Mexico
nitelken@yahoo.com

Clement Onime
Information and Communications Technology Section,
International Centre for Theoretical Physics
Trieste, Italy
onime@ictp.it

Oliver Osuagwu
Department of Computer Science,
Imo State University, Owerri, Nigeria
profoliverosuagwu@gmail.com

***Abstract*—Biometric Authentication Systems (BAS) have several security benefits over traditional password and token authentication including an inherent difficulty to copy, clone and share or distribute authentication credentials (biometric traits). Spoofing or presentation attack remains a major weakness of biometric systems and tackling it at the trait level is still challenging with several different approaches and methods applied in existing systems. In this paper, we focus on the well-known approach of Suspicious Presentation Detection (SPD) and present the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) that further mitigates spoofing or presentations attacks using randomization and combination of several different SPD detection techniques across three different modalities during trait capture. We discuss the detection of life using five distinct properties each from finger, face and eye modalities and present results from a simulation that highlights the improved security based on an impostor's inability to accurately predict the combination of trait liveness properties the system might prompt and test for during capture.**

Keywords-component; Biometric trait; Liveness Detection; Suspicious presentation

I. INTRODUCTION

Although biometric recognition is fundamentally superior and more resistant to social engineering attacks [1], it is susceptible to spoofing. Spoofing consists of presenting stolen, copied or synthetically replicated biometric traits in order to defeat the security of a biometric system and gain unauthorized access [2], [3]. It also refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting to the sensor a synthetic forged version of the original biometric trait [4]. Since spoofing basically involves persons presenting as others in order to bypass security controls and gain unauthorized access, it is also referred to as presentation attack. During a spoofing or presentation attack, the biometric trait presented before a sensor can either be a real trait or one faked by a real impostor. The term artefact also refers to an experimental (faked) trait used to simulate a presentation attack.

The feasibility of a spoof attack is much higher than other types of attacks against biometric systems, as it does not require any internal knowledge of the system, such as the feature extraction and/or matching algorithm used [2]. With the rising deployment of biometric systems in various applications, there are increasing concerns about the potentially catastrophic impact of spoofing or presentation attacks especially for mission critical applications. The growing sophistication of cyber-attacks by cyber criminals is a global threat that requires a re-definition and strengthening of the biometric authentication process [5].

In examples from [7] and [6], intruders used some type of synthetically produced artefact (e.g. face mask, gummy finger or printed iris image) or tried to mimic the behaviour of genuine users (e.g. gait, signature), to fraudulently access the biometric system. This and other reported incidences of successful attacks on facial recognition cameras and fingerprint scanners through the submission of fake traits have led to the classification of spoofing as a major threat that can curtail the security of biometric authentication systems [7], [8], reduce their reliability [9], and deepen biometric apathy.

The rest of the paper is structured as follows: the next section discusses the mitigation of spoofing or presentation attacks focusing on Suspicious Presentation Detection (SPD) and is followed by a presentation of the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) and the results, and discussion of a simulation of MMRTBLDS.

II. BACKGROUND

Biometric traits are not secrets and spoofing attacks based on synthetic replication rely on this well-known drawback that our fingerprints, face, iris, voice or even our DNA, may be publicly available data [10], [11], [12]. Since biometric systems are vulnerable to manipulation [13], the ability of the Biometric Authentication System (BAS) to detect elements of real liveness in the presented trait in order

978-1-5386-2735-8/17 $31.00 © 2017 IEEE
DOI 10.1109/UKSim.2017.44

to minimize the incidence of False Accept Rate (FAR) provides a measure of the system's security. Several anti-spoofing countermeasures exist and can be applied independently or in some combined format to increase their efficacy including cancellable biometrics or biometric revocation, multi-biometric fusion, multi-factor authentication, challenge response, and Suspicious Presentation Detection (SPD). This paper focuses on the mitigation of spoofing attacks using liveness detection as in SPD.

Majority of spoofing attacks involving suspicious presentation of traits functionally target the biometric sensor. They are also called direct attacks [14] since they come in the form of supplying the sensor with a fake biometric trait in any form in order to deceive the data capture sub-system into acquiring a false image from such forged traits. Table 1 presents a non-exhaustive list of direct attacks against five different modalities along with some information on how circumvention occurs, although we shall subsequently focus on the finger, face and eye modalities.

TABLE I. DIRECT ATTACK METHODS

SN	Modality / Trait	Attack Method
1	Finger print	Placing a fabricated gummy finger on a fingerprint sensor
2	Finger print	Presenting a photographed 2D image of the finger before a fingerprint scanner.
3	Finger print	Placing a dismembered human thumb from a cadaver or a living victim on a fingerprint sensor.
4	Facial print	Wearing a face mask mimicking the impersonated user before a facial recognition camera.
5	Facial print	Presenting a photograph or 2D portrait of a valid user's facial image in front of a facial camera.
6	Facial print	Presenting an isometric view of a 3D mold of a legitimate user's face before a High Definition (HD) facial camera.
7	Facial print	Replaying before a facial recognition system, a recorded video clip of the face of the mimicked person using a cell phone, or other handheld device.
8	Facial print	Compelling a victim, through brute force or social engineering, to display facial impression before a facial recognition system.
9	Iris pattern	Placing a lifeless mold of the human eyeball made from silicon, PVC, mud, gelatine or other synthetic materials before an iris recognition system.
10	Iris pattern	Presenting a photographed portrait of a legitimate user before an iris recognition camera.
11	Iris pattern	Wearing a contact lens or image printout of the eye in front of an iris scanner.
12	Voice print	Playing back a recorded audio clip before a voice recognition system.
13	Signature pattern	Reproducing a user's signature pattern on a hand-writing reader.

With the exception of items 8 and 11, the attacks documented in Table 1 may be reasonably mitigated using techniques that involve the detection of life. In most Biometric systems, Liveness Detection (LD) or SPD is applied in the traditional manner simply to test for the presence of elements of liveness otherwise called vitality signs, which include human pulse, temperature, oxymetry, spectroscopy, etc. However application of LD to mitigate Suspicious Presentation attacks in the traditional approach is faced with a major flaw, it is predictable and may be easily circumvented whenever attackers are able to develop specific spoofing artefacts to circumvent biometric authentication such as item 11 of Table 1. In the next section, we present the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS): that further improves the mitigation of suspicious presentation attacks through randomization and combination of several different SPD techniques.

III. MULTI-MODAL RANDOM TRAIT BIOMETRIC LIVENESS DECTECTION SYSTEM (MMRTBLDS)

The Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) is a framework that can significantly improve accuracy in preventing suspicious presentation attack patterns by reducing the impostor's ability to predict the pattern and series of liveness tests through a complex trait randomization technique.

As stated in the preceding section, most biometric systems implement SPD using a single well-defined technique that is limited only to a single modality. Figure 1 shows the logical implementation of the MMRTBLDS decision sub-system using digital logic circuits. The output (decision) will only be positive when two or more inputs are positive.

Table 2 presents our analysis of 15 different liveness parameters that are commonly used for the detection of live (SPD techniques) during the capture of biometric traits. The choice of parameters listed in Table 2 was governed by the

ease of obtaining suitable measurements during enrolment or verification. Consideration is limited to five (5) biomedical properties of human liveness from each of the three (3) modalities adopted for the study: finger, face and iris. In the framework, a minimum of three parameters are randomly selected during capture. The underlying condition on the randomization process is that each parameter must belong to a different modality (finger, face or eye). The measurements obtained from the selected parameters are then logically combined to provide a single output that is used for the SPD process.

TABLE II. DESCRIPTIVE SUMMARY OF MEASURABLE LIVENESS PARAMETERS

SN	Trait property[a]	Description, measurements, units and notation as applied in simulation
1	Finger pespiration	Probability of proportion of presence of real sweat on human finger. Perspiration evaluated as a proportion of real fluid secreted as human sweat at any instance.
2	Finger oxymetry	Proportion of oxygen in blood (Sp02) at sea level. (Sp02) reading evaluated in 3 decimal notations and measured as a percentage (%).
3	Finger spectroscopy	Measurement of the rate of reflectivity and absorptivity of radiation on a living human finger. Measured as a 1 – 0 probability for the sake of liveness verification simulation.
4	Pulse	Measurement of pulse to confirm beat rate (per minute) of a living human heart.
5	Temperature	Indication of body warmth within acceptable temperature values of about 36.8°C with a tolerance of ± 0.4°C. Measured as beats per minute (bpm). Measured in degrees Celsius (°C).
6	Facial Thermograph	Evidence of the presence of graphical image representation of heat measured around a living human face. Real values measured using radiations in the infrared range of the electromagnetic spectrum in nanometers (μm) (roughly 9,000–14,000 nanometers or 9 - 14 μm).
7	2D facial map	Probability of the presence of two dimensional pictorial impression of the human face.
8	3D facial geometry	Probability of the presence of a normalized three dimensional graphical representation of the human face as an indication of biometric liveness. Real 3D values are mathematically represented as a unique character string
9	Eye blinking	Evidence of natural eye blinking within acceptable human range of about 8 blinks per minute with a tolerance of ±8 for a healthy human adult indicating possible biometric liveness of the face. Measured as blinks per minute (bpm) totaling up to 4.2 million blinks a year.
10	Lip movement	Probability of the presence of natural lip motion in a healthy living human mouth suggesting biometric liveness.
11	Hippus	Involuntary vibration or pulsation of the pupil in a living human eye signifying biometric liveness. Measured as a frequency quantity in Hertz (Hz).
12	Iris Spectroscopy	Measurement of the rate of reflectivity and absorptivity of radiation on the iris of a living human eye as indicative of biometric liveness.
13	Ocular fluid density	The fluid contained in the sclera portion of the human eyeball is called the aqueous humour. Its density is the Ocular fluid density measured as a ratio of mass per unit volume (kg/m3). Unit of measurement is ρ which is the Greek small letter Rho. For all liquids, water is a reference standard fluid with density ρ = 1000kg/m^3, while for gases air or O2 is a standard fluid with density ρ = 1.293 kg/m^3. The aqueous humour is made of 98% water and its density is often quoted as 1.0 x10^3 = 1000kg/m^3 [15].
14	Eye blinking	Evidence of natural eye blinking within acceptable human range of about 8 blinks per minute with a tolerance of ±8 for a healthy human adult indicating biometric liveness of the eye. Measured as blinks per minute (bpm) up to 4.2 million times a year
15	Pupil auto adjusment	Evidence of natural adjustment of the pupil diameter in response to illumination level and light intensity as a proof of biometric liveness. Real 3D values are mathematically represented as a unique character string

Figure 1 shows the logical implementation of the MMRTBLDS decision sub-system using digital logic circuits. The final decision is based on the combination of the results of three liveness detection tests and the output (decision) will only be positive when two or more inputs are positive.

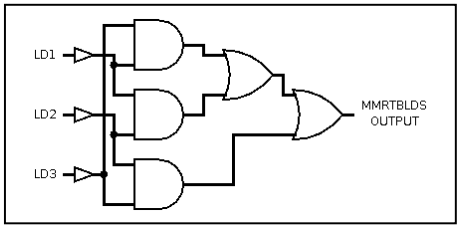

Figure 1. MMRTBLDS Decision Logic sub-system.

In general, the MMRTBLDS framework requires the ability to measure "x" different liveness detection parameters each from "y" different modalities. During biometric capture, SPD decision is based on obtaining positive results from at least "y-1" randomly selected parameters with a constraint that the randomization maximizes the selection spread over "y" different modalities.

IV. METHODOLOGY

A software/simulation implementation of the MMRTBLDS framework was developed. The simulation focused on the randomized trait selection algorithm that selects and checks distinct liveness detection methods from dissimilar traits of the same enrolee. Table 3 shows the measurement ranges that were adopted for each parameter during implementation along-side their individual or traditional thresholds.

TABLE III. MMRTBLDS LIVENESS DETECTION TRESHOLDS

Trait property	Regular limits	MMRTBLDS limits
Finger pespiration	$0 \le y \le 1$	$0.005 \le x \le 1$
Finger Oxymetry	$80 \le y \le 100$	$88 \le x \le 100$
Finger spectroscopy	$0 \le y \le 1$	$0.005 \le x \le 1$
Finger Pulse	$60 \le y \le 100$	$60 \le x \le 100$
Finger Temperature	$36.4 \le y \le 37.2$	$35 \le x \le 38$
Facial Thermograph	$0 \le y \le 1$	$0.005 \le x \le 1$
2D-facial maps	$0 \le y \le 1$	$0.005 \le x \le 1$
3D-facial geometry	$0 \le y \le 1$	$0.005 \le x \le 1$
Eye blinking	$0 \le y \le 16$	$1 \le x \le 16$
Lip movement	$0 \le y \le 1$	$0.005 \le x \le 1$
Hippus	$0.5 \le y \le 1.4$	$0.5 \le x \le 1.4$
Iris Spectroscopy	$0 \le y \le 1$	$0.005 \le x \le 1$
Ocular fluid density	$980 \le y \le 1000$	$950 \le x \le 1000$
Eye blinking	$0 \le y \le 16$	$1 \le x \le 16$
Pupil auto-adjustment	$0 \le y \le 1$	$0.005 \le x \le 1$

For ocular Fluid density measurements, we assume a traditional range of 980 - 1000, and simulation threshold of 950 – 1000 (lower than assumed traditional) as the aqueous humour is 98% water in composition. The simulation software also implemented the decision process in line with Figure 1 where the overall or resulting output is based on the combined aggregation of three dissimilar LD tests.

V. RESULTS

Table 4 shows the results from the simulation software discussed in the previous section. The simulation software is developed for 3 different modalities (finger, face and eye), each with 5 LD parameters. The final MMRTBLDS decision is based on obtaining a positive output from 2 out of 3 randomly selected tests. Table 4 presents the results from 5 different iterations (instances), where successive iteration is based on a freshly-randomized set of traits satisfying the randomization conditions.

TABLE IV. MMRTBLDS SIMULATION RESULTS FOR 5 RUNS

No	Random parameter	Input value	LD result	MMRTBLDS result
1st	Finger pespiration	0.04	0=Fail	**FAIL**. Suspected fake trait detected.
	Facial Thermograph	1.21	0=Fail	
	Hippus	0.9	1=Pass	
2nd	Eye blinking	9	1=Pass	**PASS.** Real live trait detected
	Finger Spectroscopy	0.7	1=Pass	
	Iris Spectroscopy	0..001	0=Fail	
3rd	Ocular fluid density	981	1=Pass	**PASS.** Real live trait detected
	Lip movement	1	1=Pass	
	Finger Oxymetry	92	1=Pass	
4th	Pulse	77	1=Pass	**PASS-** Real live trait detected
	Pupil auto Adjusment	0.5	1=Pass	
	3D-facial geometry	1	1=Pass	
5th	2D-facial map	0.003	0=Fail	**FAIL**. Suspected fake trait detected
	Hippus	0	0=Fail	
	Temperature	21	0=Fail	

As shown in Table 4: During the 1st instance, the MMRTBLDS framework returned a failure to detect live despite a positive measurement by the hippus parameter (from the eye modality). The 2nd instance shows the situation where the MMRTBLDS framework returned a positive detection of live despite the failure to detect live by the eye modality (iris spectroscopy). The 3rd and 4th instances show the situation where all randomly selected parameters agree on the detection of life. While during the 5th instance, failure was based on a combined failure from all tested parameters as all their values fall outside the threshold range.

VI. LIMITATIONS AND FUTURE WORK

The design of the MMRTBLDS framework's decision sub-system presented in Figure 1 could become increasingly complex to implement when using more than three liveness detection parameters as inputs. This could be addressed by

switching to a micro-controller based design to automate the randomization pattern and selection of biomedical signals for processing of liveness instead of the simple logic gates as in Figure 1. Along the lines of successful experiments and research in micro-controller based biometric systems already applied in Biometric Attendance [16], [17], Fingerprint based Automated Teller Machine (ATM) [18] and embedded authentication systems [19].

Incorporating the MMRTBLDS framework into existing biometric systems may be difficult, limited or impossible especially for unimodal systems. Future work will involve investigating ways of integrating an MMRTBLDS framework unit into existing biometric systems especially in a vendor neutral manner.

The purposely developed simulation software described in this paper is quite basic in functionality supporting well-defined input parameters. A possible future version will allow the use of randomization also on input values as this will allow flexibility and better simulation of measurements suitably influenced by other external factors.

A comprehensive mathematical representation of the randomization trait algorithm is a work in progress as this will enable performance evaluations and comparison with other similar algorithms.

Biometric performance can be measured in terms of error rates (ER) [20], which is the rate at which these errors occur. The two types of error rates are False Reject Rate (FRR) and False Accept Rate (FAR), and their computation is very important to isolate conflicting performance requirements [21] in biometric system.

Table 5 shows the ranges of FAR threshold values commonly used to evaluate the strength of a biometric mechanism. Since performance matrix is relative and biometric systems merely perform matching and do not necessarily provide perfect (unique) identification; the matching process is only probabilistic and is subject to statistical error [22] whereby the performance measure equals the percentage of queries in which the correct answer is the top match [23], example a commercial fingerprint-based authentication system requires a very low FRR for a given FAR [24]. Of all the seven fundamental characteristics of biometrics, uniqueness and permanence are most integral to biometric performance evaluations.

TABLE V. FAR TRESHOLDS FOR BIOMETRIC STRENGTH EVALUATION[20]

FAR Threshold	Index	Strength	Security classification
1 in 100	10^2	Basic	Weak and unusable
1 in 10000	10^4	Medium	Moderate and marginal
1 in 1000000	10^6	High	Strong and desirable

VII. CONCLUSIONS

Spoofing or presentation attacks have been described as a major weakness of Biometric Authentication Systems as false acceptance is a severe problem that requires urgent attention, especially in mission critical applications.

This paper presented the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS): a framework for mitigating direct spoofing or presentation attacks on Biometric Authentication Systems based on a logical combination of randomly selected liveness detection parameters. Also described, is a simulation of the MMRTBLDS framework along with some preliminary results that highlight some of the strengths of the MMRTBLDS framework in significantly improving security of biometric authentication.

ACKNOWLEDGMENT

Kenneth Okereafor thanks the Information and Communications Technology Section of the Abdus Salam International Centre for Theoretical Physics (ICTP), Trieste, Italy; and the Swiss Center for Biometrics Research and Testing, Martigny, Switzerland for their support and contributions towards this research.

REFERENCES

[1] S. S. Mudholkar, P. M. Shende and M. V. Sarode, "BIOMETRICS AUTHENTICATION TECHNIQUE FOR INTRUSION DETECTION SYSTEMS USING FINGERPRINT RECOGNITION," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol. 2, no. 1, pp. 57 - 65, 2012.

[2] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis and F. Roli, "Security Evaluation of Biometric Authentication Systems Under Real Spoofing Attacks," Department of Electrical and Electronic Engineering, University of Cagliari, Italy, Cagliari, 2014.

[3] B. Geller, J. Almog, P. Margot and E. Springer, "A chronological review of fingerprint forgery," Journal of Forensic Science, vol. 44, no. 5, p. 963 – 968, 1999.

[4] J. GALBALLY, S. MARCEL and J. FIERREZ, "Biometric Anti-spoofing Methods: A Survey in Face Recognition," IEEE Access Journal, vol. 2, no. 2014, p. 1530 – 1552, 2014.

[5] K. U. Okereafor, C. Onime and O. E. Osuagwu, "Multi-biometric Liveness Detection - A New Perspective," West African Journal of Industrial and Academic Reseearch, vol. 16, no. 1, pp. 26 - 37, 2016.

[6] J.-W. LI, "EYE BLINK DETECTION BASED ON MULTIPLE GABOR RESPONSE WAVES," in IEEE Proceedings of the Seventh International Conference on Machine Learning and Cybernetics., Kunming, China., 2008.

[7] S. Gaur, V. A. Shah and M. Thakker, "Biometric Recognition Techniques: A Review," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 1, no. 4, pp. 282 - 290, 2012.

[8] M. K. Qureshi, "Liveness detection of biometric traits," International Journal of Information Technology and Knowledge Management, vol. 4, no. 1, pp. 293 - 295, 2011.

[9] B. G. Nalinakshi, S. M. Hatture, M. S. Gabasavalgi and R. P. Karchi, "Liveness Detection Technique for Prevention of Spoof Attack in Face Recognition System," International Journal of Emerging Technology and Advanced Engineering (IJETAE), vol. 3, no. 12, pp. 627 - 633, December 2013.

[10] Get Your German Interior Minister's Fingerprint Here," The Register, 2008. [Online]. Available: http://www.theregister.co.uk/2008/03/30/german_interior_minister_fingerprint_appropriated/. [Accessed May 2016].

[11] B. Schneier, "Biometrics: Truths and fictions," In Proc. Crypto-Gram Newsletter, 1998.

[12] B. Schneier, "Inside risks: The uses and abuses of biometrics," Communications of the ACM: ACM Digital Library, vol. 48, no. 8, p. 1136, 1999.

[13] A. Hadid, N. Evans, S. Marcel and J. Fierrez, "Biometrics systems under spoofing attack: an evaluation methodology and lessons learnt," Technical report, Idap Research Centre. Idiap Report Series, Martigny, Switzerland, 2015.

[14] P. Tome and S. Marcel, "On the Vulnerability of Palm Vein Recognition to Spoofing Attacks," Idiap Research Institute, Swiss Centre for Biometrics Research and Testing, Martigny, Switzerland., 2015.

[15] A. D. Fitt and G. Gonzalez, "Fluid Mechanics of the Human Eye: Aqueous Humour Flow in the Anterior Chamber," in Bulletin of Mathematical Biology (Society for Mathematical Biology - 2006), Southampton, UK, 2006.

[16] S. Kumar, D. Rasaily, M. Mukhia and A. Ashraf, "Biometric Attendance System using Microcontroller," International Journal of Engineering Trends and Technology (IJETT), vol. 32, no. 6, pp. 306 - 308, 2016.

[17] D. K. Yadav, S. Singh, S. Pujari and P. Mishra, "Fingerprint Based Attendance System Using Microcontroller and LabView," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering., vol. 4, no. 6, pp. 5111 - 5121, 2015.

[18] D. Sunehra, "Fingerprint Based Biometric ATM Authentication System," International Journal of Engineering Inventions: e-ISSN: 2278-7461, p-ISSN: 2319-6491., vol. 3, no. 11, pp. 22 - 28, 2014.

[19] C.-H. Chen and J.-H. Dai, "An embedded fingerprint authentication system with reduced hardware resources requirement.," IEEE: Proceedings of the Ninth International Symposium on Consumer Electronics, 2005. (ISCE 2005)., pp. 145 - 150, 2005.

[20] The National Technical Authority of Information Assurance, Biometric Policy Guidance Document, "Biometric security issues," UK Government Communications-Electronics Security Group (CESG), 2010.

[21] M. Imran , A. Rao and H. G. Kumar, "A New Hybrid Approach for Information Fusion in Multi-biometric Systems," in IEEE Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics, India, 2011.

[22] UK Government Biometrics Working Group (BWG), "Biometric Security Concerns v1.0," UK, 2003.

[23] P. C. Cattin, "Biometric Authentication System Using Human Gait," Doctoral Dissertation submitted to the Swiss Federal Institute of Technology, Zurich, Switzerland, 2002.

[24] M. N. Uddin, S. Sharmin and A. H. Ahmed, "A Survey of Biometrics Security System," International Journal of Computer Science and Network Security (IJCSNS), vol. 11, no. 10, pp. 16 - 23, 2011.

[25] Y. Li, K. Xu, Q. Yan and R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems," in in Proc. 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2014), Kyoto Japan, 2014.