Biometric Anti-spoofing Technique Using Randomized 3D Multi-Modal Traits

Kenneth Okereafor

Department of Information and Communications Technology,
National Health Insurance Scheme,
Abuja, Nigeria
nitelken@yahoo.com

Oliver Osuagwu

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

Clement Onime

Information and Communications Technology Section,
The Abdus Salam International Centre for Theoretical Physics
Trieste, Italy
onime@ictp.it

***Abstract* - Despite their advantages over password-based and token-based authentication, Biometric Authentication Systems (BAS) are not perfect. They are particularly vulnerable to spoofing, also called Suspicious Presentation (SP) attacks whereby an impostor presents a fake trait to the biometric scanner during verification. Spoofing has a critical impact on system security leading to a trust deficit on biometric systems with weak anti-spoofing mechanisms. Mitigating biometric spoofing is a possibility, hence several techniques have evolved in recent times including multi-biometrics, biometric cryptography and Liveness Detection (LD) - also called Suspicious Presentation Detection (SPD). Unfortunately, nearly all known LD techniques exhibit a fundamental set of flaws – they are mostly uni-modal, easily predictable by a well-equipped impostor, and can be circumvented by well-crafted SP attacks. This paper presents the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework, as an alternative approach that implements LD using multiple traits each acquired from separate modalities of the same subject combined in a randomized manner. The strength of the framework lays in the impostor's inability to accurately predict the exact set of randomized trait parameter combinations in advance of LD. The framework employs a 3D simulation of fifteen liveness parameters, composed of three each from finger, face and iris traits, based on random number generation. Simulation results obtained using 125 distinct randomized combinations show significant improvements in biometric authentication security with a system efficiency of 99.2%.**

Keywords – Biometrics; Liveness detection; MMRTBLDS; Randomization; Spoofing; Traits

I. INTRODUCTION

Biometric systems enjoy huge usefulness in a variety of areas including logical access control, physical access control, time and attendance, law enforcement and surveillance [1], [2] [3]. The unique security benefits of Biometric Authentication Systems (BAS) account for their popularity and growing application for identification and verification purposes in commerce, healthcare, academia, research and industry. Recent digital health trends reveal the integration of Artificial Intelligence (AI) [4] into emerging biometric innovations for decision support systems. While addressing the rising global cybercrime challenges [5], [6], [7], biometrics in AI specifically aid accurate predictive analytics in healthcare delivery, disease surveillance, pattern and tele-medical diagnostics, among many other health sector applications [8], [9].

Despite biometric advantages [10] especially the difficulty to copy or steal attributes, and the infeasibility to misplace own biological trait credentials (eye swapping, finger trading or hand misplacement); Biometric Authentication Systems (BAS) remain vulnerable to spoofing. Spoofing results when an impostor maliciously presents a suspected fake or counterfeit trait to the biometric system with the intention to bypass its security controls and gain unmerited access. Since the trait supplied to the system by the impostor is of deceitful intent and involves using fake presentation in order to bypass security controls and gain unauthorized access, biometric spoofing is also known as Suspicious Presentation (SP). In a laboratory scenario however, it is also possible to experimentally present a forged trait to a prototype biometric scanner for purely research purposes; such a well-intentioned fake trait is called an artefact. Spoofing is the ability to deceive a biometric system to the point of recognizing an unauthorized user as a genuine one by means of presenting a stolen, copied, forged or synthetically replicated version of the original biometric trait to the biometric sensor [11], [12], [13]. Biometric spoofing has several consequences on the system and can occur on any biometric type irrespective of whether it is physiological or behavioural in nature. For example: fingerprints and iris patterns can be forged in much the same way that hand writing patterns and voice prints can be faked by a well-equiped imposter, except that behaviour-based spoofing would require more sophistication to create replica artefacts such as producing identical signatures and audio samples respectively. The reality of huge impacts and high risks justify the need to deploy systems to safe-guard information and its supporting processes, systems and infrastructures against spoofing [14].

Table I illustrates that the impostor's attack patterns using fake traits can take a number of various forms. For example, with the finger modality, an attacker may present a fake finger fabricated using gelatin or other materials with a

fingerprint impression, or a photographic image of a finger and/or a dismembered finger. While for the eye modality, molds of the eye may be fabricated using silicon, gelatin, latex or similar substances, or a photographic portrait, or a contact lens imprinted with the mimicked retina image for scanning. Attacks against the face modality could be performed using a face mask, photographic image, isometric view of a 3D mold or a pre-recorded video clip of the face [15], [16], [17]. Attacks against the voice modality may involve play-back of pre-recorded audio or mimicking voice using special modulators. 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 capable of curtailing the security of biometric authentication systems [16], [18], reduce their reliability [19], and deepen biometric apathy.

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 the matching algorithm used [11]. 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 [20]. This paper presents a simulation of a secure anti-spoofing multi-biometric liveness detection [21], [20] framework using a randomized fusion of fingerprint, facial print and iris pattern as adopted traits for the research.

The remainder of the paper is organized to first discuss the background of anti-spoofing using Suspicious Presentation Detection (SPD), followed by a presentation of the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework together with its parameter thresholds and simulation results. Subsequent sections present improved authentication security resulting from the framework as well its applications and future scalability.

II. BACKGROUND

Biometric systems are vulnerable to manipulation [22] of the presented trait. The ability of the Biometric Authentication System (BAS) to detect elements of real liveness in the presented trait in order to minimize the incidence of False Accept Rate (FAR) provides a measure of the system's security. Spoofing attacks based on synthetic replication, cloning or copying of traits rely on the well-known drawback that our fingerprints, face, iris, voice or even our DNA, may be publicly available data [23], [24], [25], hence biometric traits are not total secrets. There are several anti-spoofing countermeasures for improving the authentication performance and effectiveness of biometric systems either applied independently or in some combined format, including: biometric cryptography (also referred to as cancellable biometrics or biometric revocation), multi-biometric fusion (combination of different biometric modes), multi-factor authentication (concurrent application of different authentication modes such as biometrics + password + token), challenge response (use of interactive sequence of actions to verify identity), and Suspicious Presentation Detection (SPD) – which is the detection of fake or counterfeit trait as a biometric authentication sample. Mitigating spoofing attacks using SPD is also called Liveness Detection (LD). This paper reviews the traditional application of LD, exposes its weaknesses and introduces a new anti-spoofing technique that extends the application of LD.

Functionally, every biometric spoofing attack involves presentation of fake traits to the biometric scanner, occurring at an attack node - those vulnerable points in a biometric system where attacks are usually targeted at. Although there are multiple attack nodes, the scanner is mostly vulnerable to direct attacks. Direct attacks [26] on the scanner come in the form of supplying the scanner with a fake biometric trait in order to circumvent it. Figure 1 gives a pictorial view of twelve attack nodes (numbered 1 through 12) and indicates that attack Node 1 on the sensor is the first direct attack, outside the digital limits of the biometric system using the impostor's presentation of an artefact (a fake trait) to the scanner. Other nodes in Figure 1 are indirect attacks against the system's digital limits using sophisticated techniques to bypass the feature extractor, the comparator (matcher), or the communications channels connecting them. This paper focuses on direct attacks on Node 1.

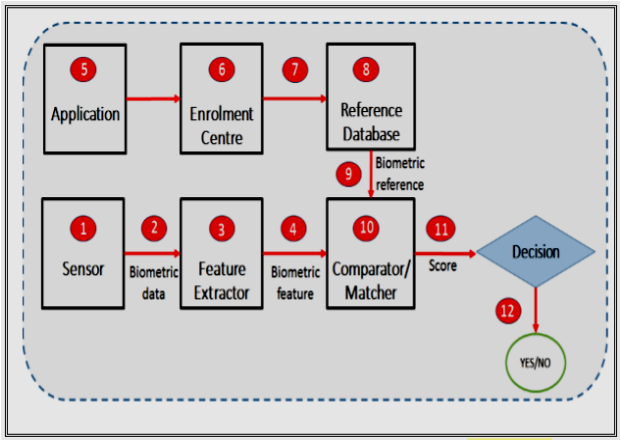

Figure 1: Attack nodes in a biometric authenication system.

Table I below presents an expanded list of Node 1 direct attacks against five different biometric modalities together with some information on how such attacks occur. Subsequently the simulation shall focus on the finger, face and eye modalities.

TABLE I. DIRECT ATTACK METHODS

SN	Modality	Spoofing Method	Spoofed Trait
1	Finger	Attacker places a fake finger fabricated from the impersonated person's fingerprint impression made from gelatin [27], [28] or other materials on a fingerprint scanner.	Fingerprint
2		Attacker presents a photographed 2D image of the legitimate person's finger before a fingerprint scanner.	Fingerprint
3		Attacker places a dismembered thumb or finger severed from a real living victim to a fingerprint scanner with the hope of acquring a genuine fingerprint impression .	Fingerprint
4		Attacker presents a dismembered thumb or finger from the cadaver (dead body) of the victim before a fingerprint scanner targeting to obtain a legitimate fingerprint sample match.	Fingerprint
5	Eye	Impostor places a lifeless mold of the legitimate person's eyeball made from silicon, PVC, mud, gelatine, EcoFlex, latex, silgum, wood glue or other synthetic materials [29], [30], [31] before an iris recognition system.	Iris pattern
6		Attacker presents a photographed portrait of the legitimate user before an iris recognition camera.	Iris pattern
7		Attacker wears a contact lens or an image printout of the authentic enrolee's eye in front of an iris scanner.	Iris pattern
8		Impostor wears and displays a crafted contact lens or fabricated eyeball of the real user in front of a retina scanner.	Retina pattern
9	Face	Attacker wears and presents a face mask modelled after the impersonated person's geometry before a facial recognition system.	Facialprint
10		Attacker presents a photograph or 2D portrait of a valid enrolee's facial image in front of a facial recognition system's camera.	Facialprint
11		Attacker presents an isometric view of a 3D mold of a legitimate user's face before a High Definition (HD) facial camera.	Facialprint
12		Attacker replays a recorded video clip showing the face of the mimicked person captured with the help of a cell phone, video recorder or other handheld device before a facial recognition system.	Facialprint
13		Attacker compels a victim, through brute force, social engineering, or any other compelling manner to display own facial image before a facial recognition system.	Facialprint
14	Voice	Impersonator plays back a recorded audio clip mimicking the authentic enrollee's spoofed voice before a voice recognition system.	Voice print
15	Hand writing	Attacker reproduces a user's signature pattern on a hand-writing reader.	Signature pattern

III. WEAKNESSES OF EXISTING LIVENESS DETECTION TECHNIQUES

Almost all the Node 1 attacks documented in Table I above may be reasonably mitigated using techniques that involve the detection of life such as detecting real human voice or genuine living human finger. 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 and other vitality signs, including pulse, temperature, oxymetry, spectroscopy, etc. Unfortunately contemporary applications of LD to mitigate Suspicious Presentation attacks in the traditional manner are faced with some major drawbacks: they are often implemented in a unimodal manner using predefined tests. This makes them highly predictable and easily circumvented as attackers are able to easily develop specific spoofing artefacts against the known single modality in advance to bypass the biometric LD process.

In the next section therefore, we present the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS): a framework that addresses the weaknesses of traditional LD methods and improves mitigation of suspicious presentation attacks through randomization and combination of several different SPD techniques in a multimodal fashion.

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

The Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework is designed to significantly improve accuracy in preventing biometric spoofing. The framework functions by subjecting a series of trait parameters derived from multiple biometric modalities of the same subject to random liveness tests. The application of randomness in the selection of liveness parameters for testing minimizes the impostor's ability to predict the pattern while the multimodal approach optimizes authentication security.

Contrary to the single modality design of most liveness detection implementations, the MMRTBLDS executes in a well-defined multi-modal structure illustrated in Figure 2 showing digital logic circuits of the framework's decision sub-system. The output (decision) only produces a positive when two or more inputs are positive.

Table II presents our analysis of fifteen (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 II was governed by ease of obtaining suitable measurements during enrolment or verification. We limit our considerations 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	Description, measurements, units and notations as applied in the 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 (SpO_2) at sea level. (SpO_2) 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. Measured as beats per minute (bpm).
5	Temperature	Indication of body warmth within acceptable temperature values of about 36.8°C with a tolerance of ± 0.4°C. 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 (for face)	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 and physical presence.
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 $\rho = 1000 kg/m^3$, while for gases air or O_2 is a standard fluid with density $\rho = 1.293\ kg/m^3$. The aqueous humour is made of 98% water and its density is often quoted as $1.0 \times 10^3 = 1000 kg/m^3$ [32].
14	Eye blinking (for eye)	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 2 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) is only positive when two or more inputs are of positive value.

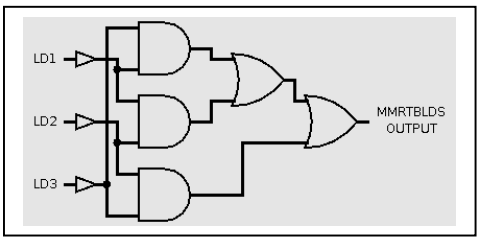

Figure 2. MMRTBLDS Decision Logic sub-system.

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 result from at least ***y-1*** randomly selected parameters with a constraint that the randomization maximizes the selection spread over the ***y*** different modalities.

V. 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 enrollee. Table III shows the measurement ranges that were adopted for each parameter during implementation along-side their individual or traditional thresholds.

For ocular Fluid density measurements, we assume a traditional range of 980 – $1000 kg/m^3$, and simulation threshold of 950 – $1000 kg/m^3$ (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.

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	$0 \le y \le 1$	$0.005 \le x \le 1$

VI. RESULTS

Table IV shows the results from the simulation software discussed in the previous section. The simulation software is developed for three (3) different modalities (finger, face and eye), each with five (5) LD parameters. The final MMRTBLDS decision is based on obtaining a positive output from two (2) out of three (3) randomly selected tests.

TABLE IV. MMRTBLDS SIMULATION RESULTS FOR 5 INSTANCES

Instance	Random parameter	Input value	LD result	MMRTBLDS result
1st	Finger Temperature	32	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	Finger Oxymetry	92	1=Pass	**PASS.** Real live trait detected
	3D-facial geometry	1	1=Pass	
	Ocular fluid density	81	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	Finger Temperature	21	0=Fail	**FAIL**. Suspected fake trait detected
	2D-facial map	0.003	0=Fail	
	Hippus	0	0=Fail	

Table IV presents the results from five (5) different iterations (instances), where each successive iteration is based on a freshly-obtained randomized set of traits satisfying the randomization conditions.

As shown in Table IV above, 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 iris spectroscopy parameter from the eye modality. The 3rd and 4th instances show the situation where all randomly selected parameters agree on the detection of life, falling within threshold limits. While during the 5th instance, LD failure was based on a combined failure from all tested parameters as all their values fell outside the threshold range. Figure 3, Figure 4 and Figure 5 below show screenshots from simulations corresponding to the 1st, 3rd and 5th instances respectively.

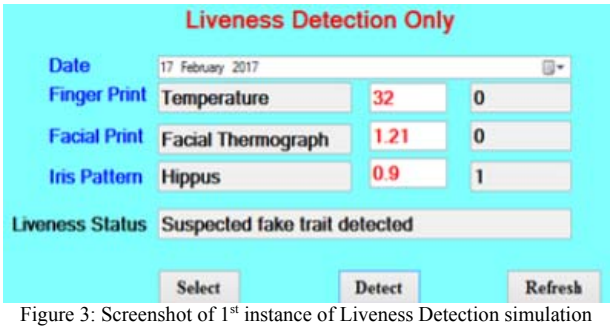

Figure 3: Screenshot of 1st instance of Liveness Detection simulation showing detection of suspected fake trait.

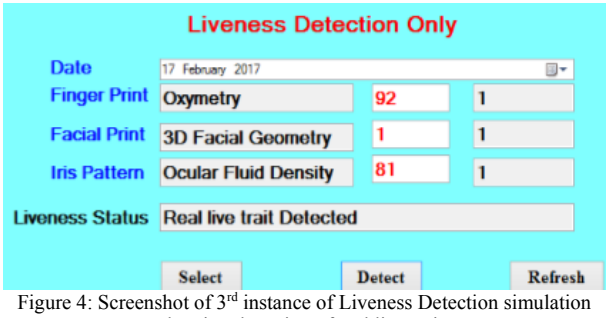

Figure 4: Screenshot of 3rd instance of Liveness Detection simulation showing detection of real live trait.

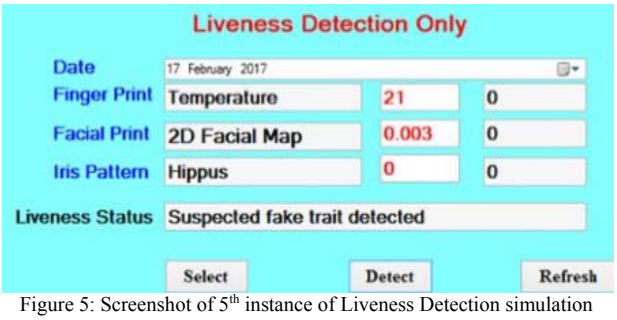

Figure 5: Screenshot of 5th instance of Liveness Detection simulation showing detection of suspected fake trait.

VII. APPLICATIONS

The MMRTBLDS framework presented in this work is highly beneficial to many industrial usages especially where a high degree of access control is required to validate authentic subjects into a facility. Such industrial applications require a well-designed implementation mechanism to ensure that the uniqueness of the framework is utilized in practical terms.

A. Healthcare Access: It is desirous for hospital encounter management information systems to exhibit a secure patient authentication mechanism. Application of the MMRTBLDS guarantees the highest level of biometric-based validation checks that ensure that only legitimate patients are properly identified, fully authenticated and correctly diagnosed.

B. Immigration and Border Control: The MMRTBLDS is ideal for border environments and facilities where the possibility of criminal migration is high. It is uniquely suited for border checks as an integral part of criminal database look up to prevent false accept consequences of granting access to criminal suspects on the wanted list. By optimizing the process of detecting fake biometric samples, the framework helps border and access control systems to prevent spoofing associated with criminal presentation of counterfeit traits before weak biometric systems.

C. Highly-Sensitive Production Factories: Environments requiring strict identification and certification of users such as pharmaceutical laboratories, nuclear facilities, food processing factories, identity repositories, and aviation systems often experience spoof attacks resulting in severe consequences, loss of data and occasional fatalities. Sensitive environments require a foolproof mechanism to maintain non-repudiation of transactions and digital operations. The MMRTBLDS comes to the rescue as a secure mechanism that guarantees all-round detection of spoof attempts. Application of the framework in such environments complements other access control measures and eliminates the attacker's chances of success.

VIII. LIMITATIONS AND FUTURE WORK

A. Automated Randomization: There is a likelihood that 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. We hope to address this 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. Our projection is strengthened by recent successful experiments and research in micro-controller based biometric systems already applied in Biometric Attendance [33], [34], Fingerprint based Automated Teller Machine (ATM) [35] and embedded authentication systems [36].

B. Vendor-Neutral Implementation: Incorporating the MMRTBLDS framework into existing biometric systems may be difficult, limited or impossible especially for unimodal systems. Our future work will involve investigating ways to integrate the MMRTBLDS framework into existing biometric systems especially in a vendor neutral manner to ensure interoperability.

C. Scalable Operation: It is very clear that the purposely developed simulation software described in this paper is quite basic in functionality supporting well-defined input parameters. To introduce scalability, 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. This also widens the scope of the framework's application.

D. Performance Improvement and Error Corrector: The limited design of the framework's computation logic is potentially challenging to its operations. Since biometric performance can be measured in terms of error rates (ER) [37], including the rate at which spoof-related errors occur, misapplication of the system could escalate inherent errors and cause performance issues. As a remedy, we will introduce an error correction module into future refinements of the MMRTBLDS framework to provide a balance between False Reject Rate (FRR) and False Accept Rate (FAR) and isolate conflicting performance issues [38], [39] and statistical errors [40]. To implement the proposed error correction module, we will apply standard FAR threshold values shown in Table V to evaluate the error-handling strength of the framework. Since biometric performance matrix is relative and the matching process is only probabilistic, the introduction of an error corrector satisfy the requirement of very low FRR for a given FAR [41] in commercial fingerprint-based authentication system.

TABLE V. FAR TRESHOLDS FOR BIOMETRIC STRENGTH EVALUATION

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

IX. CONCLUSIONS

Spoofing/presentation attacks have been presented as major weakness of Biometric Authentication Systems as false acceptance is a severe problem with huge consequences, especially in mission critical applications such as healthcare, civic digital identity systems, border control, and crime investigation.

This paper presented the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS): a

framework for mitigating biometric spoofing based on a logical combination of randomly selected liveness detection parameters. By integrating a mix of randomization and the use of multiple traits from disparate modalities, the framework applies security by obscurity to increase the attacker's difficulty of accurately predicting the exact trait parameters to be prompted for liveness testing. The scalability of the framework's randomization strategy completely redefines the concept of spoof mitigating by addressing the limitations of traditional anti-spoofing countermeasures.

A simulation of the MMRTBLDS framework has also been described along with some preliminary results that highlight its strengths in significantly improving security of Biometric Authentication Systems.

ACKNOWLEDGMENT

The authors extend special thanks to the National Health Insurance Scheme, Nigeria; Information and Communications Technology Section of the Abdus Salam International Centre for Theoretical Physics (ICTP) Trieste, Italy; Centre for Cyberspace Studies (CCS) of the Nasarawa State University, Nigeria; and the Swiss Center for Biometrics Research and Testing Martigny, Switzerland for their support and goodwill on this research.

REFERENCES

[1] S. Asha and C. Chellappan, "Biometrics: An Overview of the Technology, Issues and Applications," International Journal of Computer Applications (IJCA), vol. 39, no. 10, pp. 35 - 52, 2012.

[2] S. Shrivastava, "Biometric: Types and its Applications," International Journal of Science and Research (IJSR), pp. 204 - 207, 2015.

[3] Ravi Das, "The Application of Biometric Technologies," 2016. [Online]. Available: https://resources.infosecinstitute.com/the-application-of-biometric-technologies/#gref. [Accessed 9 August 2018].

[4] S. Chabbra and N. Singh, "Applications of Swarm Intelligence in Biometrics systems," International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), vol. 2, no. 2, pp. 3089 - 3094, 2014.

[5] J. Phiri, T.-J. Zhao, C. H. Zhu and J. Mbale, "Using Artificial Intelligence Techniques to Implement a Multifactor Authentication System," International Journal of Computational Intelligence Systems (IJCIS), vol. 4, no. 4, pp. 420 - 430, 2011.

[6] N. Singla and S. Sharma, "Biometric Fingerprint Indentification Using Artificial Neural Network," International Journal of Advanced Research in Computer Science & Technology (IJARCST), vol. 2, no. 1, pp. 28 - 31, 2014.

[7] S. S. Mudholkar, P. M. Shende and M. V. Sarode, "Biometrics Authentication Technique for Intrusion Detection System Using Fingerprint Recognition," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol. 2, no. 1, pp. 57 - 65, 2012.

[8] 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.

[9] 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.

[10] 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.

[11] S. S. Ahmad, B. M. Ali and W. A. Adnan, "TECHNICAL ISSUES AND CHALLENGES OF BIOMETRIC APPLICATIONS AS ACCESS CONTROL TOOLS OF INFORMATION SECURITY," International Journal of Innovative Computing, Information and Control, vol. 8, no. 11, pp. 7983 - 7999, 2012.

[12] 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.

[13] 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.

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

[15] 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.

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

[17] K. U. Okereafor, O. E. Osuagwu and C. Onime, "Enhancing Biometric Liveness Detection Using Trait Randomization Technique," in 2017 IEEE UKSim-AMSS 19th International Conference on Modelling & Simulation, Cambridge, 2017.

[18] 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.

[19] "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].

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

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

[22] 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.

[23] "Spoof Mitigation and liveness detection solutions for the biometric authentication industry," 2013. [Online]. Available: http://nexidbiometrics.com/technology/spoof-lab/. [Accessed April 2016].

[24] K. M. Valsamma, "Aadhaar, Function Creep and The Emerging Symbiotic Relationship between Society and Technology," PARIPEX - Indian Journal Of Research (ISSN - 2250-1991), vol. 3, no. 8, pp. 184 - 185, 2014.

[25] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli and S. Schuckers, "LivDet 2011 - fingerprint liveness detection competition," in The 5th IAPR International Conference on Biometrics, 2012.

[26] D. Gragnaniello, G. Poggi, C. Sansone and L. Verdoliva, "An Investigation of Local Descriptors for Biometric Spoofing Detection," IEEE Transactions in Information Forensics and Security, vol. 10, no. 4, pp. 849 - 863, 2015.

[27] D. Menotti, G. Chiachia and A. Pinto, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," IEEE Transactions on InformationForensics and Security, vol. 10, no. 4, pp. 864 - 879, 2015.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

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

[34] 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.

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

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

[37] 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.

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

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

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

[41] 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.