International Journal in IT & Engineering (IJITE)
Volume 8 Issue 10, October 2020 ISSN: 2321-1776 Impact Factor: 6.493
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

RANDOMIZED MULTI-BIOMETRIC LIVENESS DETECTION: PROSPECTS AND APPLICATIONS FOR SECURE AUTHENTICATION

Kenneth Okereafor, PhD, PhD
Department of Information and Communications Technology,
National Health Insurance Scheme Abuja, NIGERIA.
nitelken@yahoo.com

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

Sani Felix Ayegba, PhD, PhD
Department of Computer Science,
Federal Polytechnic Idah, NIGERIA
felixsani@yahoo.com

Oluwasegun Adelaiye
Department of Computer Science,
Bingham University Karu, NIGERIA
oluwasegun.adelaiye@binghamuni.edu.ng

ABSTRACT

Biometric systems verify humans using their unique physiological or behavioural patterns to offer more secure authentication over passwords and tokens. Despite their benefits, Biometric Authentication Systems remain vulnerable to spoofing, wherein an impostor presents a forged biometric trait and bypasses security checks. Impacts of successful spoofing can be potentially fatal such as in healthcare and crime investigation systems where insecure authentication can result in patient misdiagnosis and criminal misidentification, respectively. Existing anti-spoofing techniques are mostly uni-modal and predictable, and therefore incapable of coping with the sophistication of modern-day biometric cyberattacks. This paper presents the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework which employs a complex trait randomization algorithm to mitigate predictability. Fifteen liveness attributes derived from finger, face and iris traits are used to simulate various authentication scenarios, resulting in 99.2% efficiency over uni-modal biometric systems. The paper also proposes areas of useful application of the framework based on its capacity to neutralize an impostor's ability to accurately predict biometric trait combinations at the sensor verification stage.

Keywords: Biometric, impostor, liveness detection, multi-modal, randomization, spoofing, trait.

1.0 INTRODUCTION

1.1 Overview of Access Control

Effective access control is the bedrock of a secure information system with full complements of the *authentication*, *authorization,* and *accounting* functions. While authentication ensures verification of subjects, authorization assigns system privileges. The accounting function tracks system transactions, logs operations in chronological order and facilitates reliable audit. All three functions complement each other to guarantee data confidentiality, integrity, availability, authenticity, and non-repudiation. As the first in the access control process, authentication requires careful selection for high-risk environments and mission-critical applications. Beyond the traditional password-based and token-based authentication schemes, biometric authentication systems are increasingly attractive for their superior advantages especially as biometric traits can neither be reused, replaced, swapped, nor forgotten. This paper is an extension of work on *"Enhancing Biometric Liveness Detection Using Trait Randomization Technique"* originally presented at the 2017 IEEE UKSim-AMSS 19th International Conference on Computer Modelling & Simulation [1] at the University of Cambridge UK, and later published as an extended research paper as *"Biometric Anti-spoofing Technique Using Randomized 3D Multi-Modal Traits"* [2].

1.2 Biometric Authentication Background

Biometric systems have found ubiquitous use wherever human verification is required in a secure manner for access control and identity recognition. As a result, they have continued to attract patronage for mobile authentication schemes, patient identification systems, physical and logical access control systems, time and attendance systems, digital forensics and crime investigation, border patrol and immigration control [3], [4], [5], [6], etc. In the medical domain for example, biometric technologies are utilized to ensure accurate patient identification and forestall incidences of misdiagnosis and fatal misidentifications [7], [8]. In National civic identity schemes, biometric systems form the crux of National Identity repositories for gathering citizens' digital identities [9], [10], [11], [12], [13] for the purposes of population demographics, disease surveillance, electoral operations, birth and death statistics management, financial industry regulations, etc. with India currently deploying the world's largest biometric identity database [14]. Biometric systems are also useful in law enforcement and crime control particularly in criminal suspects' forensic cross-matching and the use of Artificial Intelligence (AI) in addressing the rising global cybercrime challenges [15], [16], [17]. Recent digital health trends include the innovative use of AI [18] within decision support systems, accurate predictive analytics in healthcare delivery, disease surveillance, pattern, and tele-medical diagnostics, among many other health sector applications.

1.3 Biometric Spoofing and its Impacts

Despite their benefits for secure authentication [19] including the difficulty to copy, steal, misplace, or forget biometric credentials, Biometric Authentication Systems (BAS) still exhibit a fundamental flaw – they can be spoofed, which 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 [20], [21], [22]. Since the trait supplied by the impostor involves fake presentation and is of deceitful intent to bypass security controls and gain unauthorized access, biometric spoofing is also known as Suspicious Presentation (SP). It is also possible to develop an experimental trait for research purposes; such an intentionally-faked trait is called an artefact. Both physiological and behavioural biometric traits can be spoofed. 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-equipped imposter, although behaviour-based spoofing requires more sophistication to create suitable replica or experimental artefacts such as producing identical signatures and audio samples respectively. The overall intent of every spoof attempt is to bypass security controls and gain unmerited access through the presentation of fake or counterfeit traits. Table 1 shows several attack methods used by an impostor to present fake traits (for five selected modalities) before a biometric scanner along with explanation of how the attacks occur.

Table 1: Direct attack methods on selected biometric modalities [2]

SN	Modality	Spoofing Method	Spoofed Trait
1	Finger	Attacker places a fake finger fabricated from the impersonated person's fingerprint impression made from gelatin [22], [23] 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/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 [9], [24], [25] before an iris recognition system.	Iris pattern
6		Attacker presents legitimate user's photographed portrait 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 means 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

As shown in Table 1, in the finger modality an attacker may present a fake finger fabricated using gelatine 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, gelatine, 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 [26], [27], [28]. Attacks against the voice modality may involve play-back of pre-recorded audio or mimicking voice using special modulators. The 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 with the potential to impact the security of biometric authentication systems [27], [29], reduce their reliability [30], and deepen biometric apathy.

Successful spoofs have huge impacts on information systems, and justify the need to evolve countermeasures to protect biometric systems and infrastructure against spoofing [31]. The growing sophistication of cyberattacks is a global threat that requires a re-definition and strengthening of the biometric authentication process [32]. 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.

This paper which is an extension of the originally-published work in an optimized biometric anti-spoofing framework [1], [2], [32] discusses several useful areas of application of the multi-modal biometric liveness detection framework using a randomized fusion of fingerprint, facial print and iris patterns as adopted traits for the research. The paper is organized as a bottom-up compendium by first presenting anti-spoofing background using Suspicious Presentation Detection (SPD), followed by a presentation of the modus operandi of the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework together with its parameter thresholds, simulation results and application areas.

1.4 Mitigating Biometric Spoofing

Biometric traits are not immune to cyberattacks [33], [34], [35], as their versatility makes them susceptible to manipulation [36] and spoofing. The security of a Biometric Authentication System (BAS) lies in its ability to detect attributes of real liveness in the presented trait. Presentation attacks manifest as spoofing based on synthetic replication of traits, cloning of artefacts or copying of biometric credentials. Several anti-spoofing countermeasures exist, Table 2 illustrates some known anti-spoofing techniques.

Table 2: Some known biometric anti-spoofing techniques

SN	Anti-spoofing technique	Mode of operation
1	Biometric cryptography	The hashing and systematic revocation of biometric templates to strengthen against their cloning. This is also known as cancellable biometrics or biometric revocation.
2	Multi-biometric fusion	The concurrent application of more than one biometric source, method or other classifying factors to boost authentication security. Examples: Multi-sample, Multi-mode, Multi-algorithm, Multi-sensor, Multi-instance and Hybrid model.
3	Multi-factor authentication	The simultaneous application of different authentication modes to protect against spoofing and other authentication security breaches. Example: Combination of *biometrics + password + token.*
4	Challenge response	The use of interactive sequence of actions to verify identity and authenticity. Examples: reciting a pre-written speech, responding to eye blinking request, or supplying a facial expression prompt.
5	Liveness Detection (LD)	LD is an embedded technique used to determine if the biometric sample presented at the point of verification is an actual authentic measurement from an authorized, live person physically present at the time of capture. LD is also called Suspicious Presentation Detection (SPD).

As shown in Table 2, of all described techniques, only LD deals with the detection of fake/counterfeit trait in biometric authentication. Mitigating spoofing attacks using LD is also called Suspicious Presentation Detection (SPD) as it involves the detection of fake traits presented in a dubious or suspicious manner.

Typically, biometric spoofing attack occurs at the biometric scanner/sensor attack node (vulnerable point) through the presentation of fake traits. There are multiple attack nodes and channels in a biometric system, but the scanner is mostly vulnerable to direct attacks [37] which come in the form of supplying the scanner with a fake biometric trait in order to circumvent it. Figure 1 shows twelve attack nodes (numbered 1 through 12) with a typical biometric system and clearly 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/fake trait to the scanner. Other attack 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. The focus of this paper is on direct attacks on sensors. All the direct attack methods and patterns illustrated earlier in Table 1 are based on exploitation of Node 1 vulnerabilities.

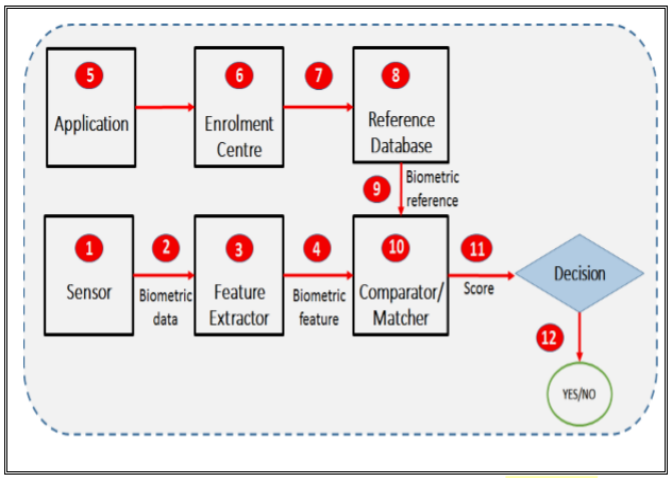


Figure 1: Attack nodes in a biometric authenication system [1]

Spoof attacks on sensors can be mitigated through the detection of life such as detecting real human gait (walking pattern) or genuine living human palm. On existing biometric systems, LD is performed by checking for the presence of a single element of liveness or other vitality signs, such as pulse, temperature, or oximetry, etc. Regrettably this uni-modal approach to LD makes it highly predictable, insecure, and easily circumvented as a well-equipped attacker is able to easily develop specific spoofing artefacts against the known single modality in advance to bypass the LD process. Enhanced LD systems are similarly limited to the use of additional (one or two) traits, which does not impose any burden of predictability on the part of the impostor.

2.0 THE NEW MULTI-BIOMETRIC RANDOMIZATION FRAMEWORK

The Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) is a framework that addresses the identified gaps of traditional LD methods and improves mitigation of suspicious presentation attacks through randomization and combination of several different SPD techniques in a multi-modal manner [1]. The design of the MMRTBLDS framework significantly improves accuracy in preventing biometric spoofing. A series of trait parameters derived from multiple biometric modalities of the same subject are subjected to random liveness tests. Randomizing the selection of liveness parameters for testing minimizes the impostor's ability of accurately predicting the pattern while the multimodal approach optimizes authentication security. The multi-modal structure of the MMRTBLDS framework compensates for the weak single modality design of contemporary liveness detection implementations. Figure 2 illustrates the digital logic circuit of its decision sub-system, where the output (decision) only produces a positive when two or more liveness parameter input values are positive.

Table 3 presents the analysis of fifteen (15) different liveness parameters used for the simulation of the detection of live during the capture of biometric traits. The choice of parameters listed in Table 3 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 emanate from a different modality (finger, face, or eye) governed by a random number generator logic. The measurements obtained from the selected parameters are then logically combined to provide a single output that is used for the SPD/LD process.

Table 3: Description of measurable liveness parameters [2]

SN	Trait property	Simulation measurement descriptions (units and notations)
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, 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.

SN	Trait property	Simulation measurement descriptions (units and notations)
		Measured as blinks per minute (bpm) totaling up to 4.2 million blinks per 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/m^3). 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 O_2 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 $1.0 \times 10^3 = 1000kg/m^3$ [38].
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 is an illustration of the logic of the MMRTBLDS decision sub-system using digital gates. The final decision is a function of the combination of the states of three liveness detection tests and the output (decision) only returns positive when two or more inputs are of positive values.

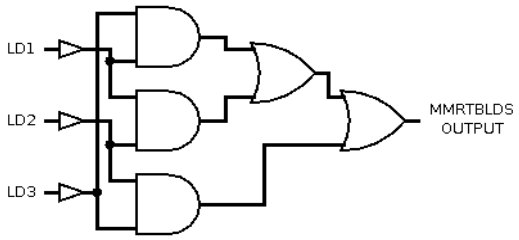


Figure 2: MMRTBLDS Decision Logic sub-system [2], [32].

The MMRTBLDS framework functionally implements 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. These constraints stipulate that two traits cannot be selected from the same modality at any instance of randomization, thereby further strengthening its security.

2.1 Simulation of the MMRTBLDS Framework

A Graphical User Interface (GUI) software written in Visual Basic (VB) was developed for simulation of the MMRTBLDS framework. The core of the application is on simulation of the randomized trait selection algorithm which selects and checks distinct liveness detection trait combinations from dissimilar traits of the same enrolee's modalities. Table 4 shows the input measurement ranges adopted for each parameter during implementation, along with their traditional thresholds.

Table 4: MMRTBLDS liveness detection thresholds [2]

SN	Trait property	Regular limits	MMRTBLDS limits
1	Finger pespiration	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
2	Finger Oxymetry	$80 \leq y \leq 100$	$88 \leq x \leq 100$
3	Finger spectroscopy	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
4	Finger Pulse	$60 \leq y \leq 100$	$60 \leq x \leq 100$
5	Finger Temperature	$36.4 \leq y \leq 37.2$	$35 \leq x \leq 38$
6	Facial Thermograph	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
7	2D-facial maps	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
8	3D-facial geometry	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
9	Eye blinking	$0 \leq y \leq 16$	$1 \leq x \leq 16$
10	Lip movement	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
11	Hippus	$0.5 \leq y \leq 1.4$	$0.5 \leq x \leq 1.4$
12	Iris Spectroscopy	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$
13	Ocular fluid density	$980 \leq y \leq 1000$	$950 \leq x \leq 1000$

SN	Trait property	Regular limits	MMRTBLDS limits
14	Eye blinking	$0 \leq y \leq 16$	$1 \leq x \leq 16$
15	Pupil auto- adjustment	$0 \leq y \leq 1$	$0.005 \leq x \leq 1$

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 2 where the resulting output is based on the combined aggregation of three dissimilar LD tests.

2.2 Result Analysis

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

Table 5: MMRTBLDS simulation results for 5 instances [2]

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	

As shown in Table 5, 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 show screenshots from simulations corresponding to the 1st, 3rd, and 5th instances, respectively.

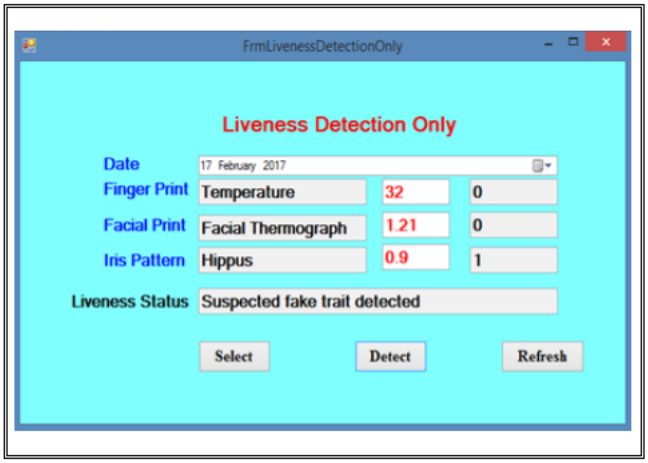


Figure 3: Screenshot of 1st instance of Liveness Detection simulation showing detection of suspected fake trait [2].

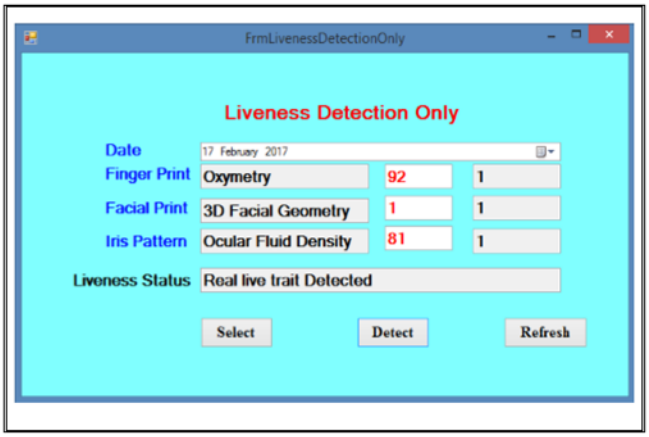


Figure 4: Screenshot of 3rd instance of Liveness Detection simulation showing detection of real live trait [2].

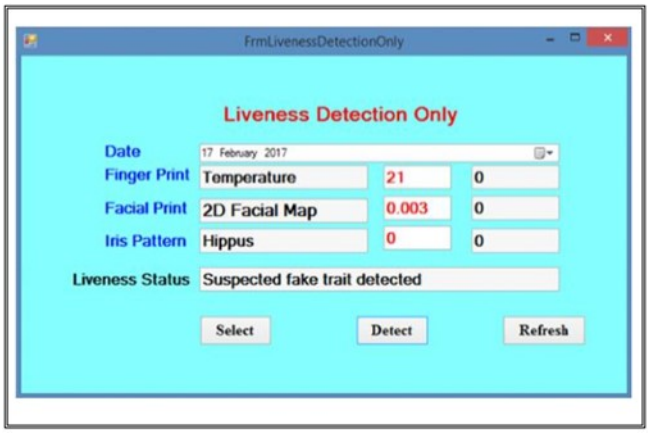


Figure 5: Screenshot of 5th instance of Liveness Detection simulation showing detection of suspected fake trait [2].

2.3 Efficiency of the MMRTBLDS Framework

The efficiency of the MMRTBLDS framework is computed from the security accuracy results obtained from the simulation instances. With three (3) modalities of five (5) liveness parameters each, totalling fifteen (15) liveness quantities, and without repeated traits in successive iterations, the system generates a total of 125 distinct combinations of randomized parameter options based on the randomization decision logic earlier illustrated in Figure 2; hence a system cardinality of 125. Table 6 summarizes the simulation parameter counts.

Table 6: Simulation parameter counts

Property	**Count**
No. of adopted biometric modalities (**m**)	3
No. of trait parameters per modality (**n**)	5
No. of trait parameters in total	15
No. of allowable randomization instances – cardinality (**A**). Computed using an algorithm that implements the logic of Figure 2.	125

The cardinality indicates how many unique sets of combinations in total (each with three randomly-selected traits) can be obtained from fifteen liveness quantities without any parameter repeated per instance. Therefore, the probability that an intruder is able to accurately predict the precise set of trait combinations contained in any instance is computed as follows:

Given **A** = cardinality = 125
Let **p** = probability of accurate prediction of a single set of trait combinations by an impostor,

$\therefore$ $\mathbf{p} = \mathbf{A}^{-1} = (125)^{-1} = 0.008$,

⇒ impostor success probability expressed in percentage = 0.8%,
⇒ impostor failure probability expressed in percentage = 100% – 0.8% = 99.2%.

Let **E** = system efficiency
E ≡ the probability of the impostor's failure, derived as follows:

E = 1 – **p**
E = 1 – 0.008 = 0.992 = 99.2%.

So, the expected maximum or theoretical efficiency of the MMRTBLDS framework is 99.2%. Since the framework's computed efficiency is equivalent to security accuracy and dependability measured in terms of its spoof-prevention ability, this result suggests that the introduction of multi-trait parameter randomization into the liveness detection method can significantly reduce the impostor's ability to accurately predict the precise set of liveness parameters prompted. Table 7 summarizes system efficiency statistics and further portrays the framework's capacity to improve the overall authentication security of Biometric Authentication Systems. The system only shows a 0.008 probability of failure.

Table 7: System efficiency summary

	Probability		**Rate**	
	Accurate	Wrong	Success	Failure
Impostor effort	0.008	0.992	0.8%	99.2%
System efficiency	0.992	0.008	99.2%	0.8%

3.0 APPLICATIONS OF THE MMRTBLDS FRAMEWORK

Given its potentials to nullify impostor attempts to spoof and circumvent, the MMRTBLDS is capable of significantly improving the security and performance of Biometric Authentication Systems in the following application areas:

3.1 Crime Control, Law Enforcement and Forensics

The improved system efficiency would ensure fewer cases of mis-identification in digital profiling often encountered by crime fighters and law enforcement agents. The framework's trait randomization and multi-modal features are capable of optimizing biometric authentication accuracy leading to reduced False Accept Rate (FAR) statistics during forensic investigations.

3.2 Medical Science and Healthcare

This work could potentially improve the capacity of medical personnel to react to medical emergencies. With an optimized fingerprint scan based on the MMRTBLDS framework, patients who are unconscious or unable to talk can still be quickly identified digitally, through liveness verifications of

their specific biometric liveness attribute such as pulse, oximetry, temperature and perspiration, along with other pertinent medical history like drug allergies and current medications. Optimizing liveness detection by the application of this framework greatly improves the integrity of information generated by the Health Information Exchange (HIE) for use by major stakeholders within the healthcare industry.

3.3 Identity and Access Management (IAM) Systems

The application of the MMRTBLDS framework improves the accuracy level, trustworthiness, security and reliability of biometric queries for Identity and Access Management (IAM) systems used by consulates and diplomatic missions, the military, healthcare sectors, telecoms providers, population and statistics agencies, and government identity schemes. Achieving improved security and accuracy of IAM systems through detection of multi-biometric liveness is one of the cardinal requirements for building trust, confidence, and integrity into national biometric databases without which demographic statistics would remain speculative at best. “Speculative figures” impede national planning and is always to the detriment of the economically-disadvantaged. This work favours the advocacy for the effective use of the right technology in producing accurate national identity statistics.

3.4 Immigration and Border Control

Applying the MMRTBLDS framework to the design and development of immigration and customs access control systems could aid officials in carrying out real-time secure biometric template comparisons across remote databases and facilities where the possibility of criminal migration and criminal presentation of counterfeit traits before weak biometric systems is high. This could potentially eliminate the challenges hitherto experienced with biometric-based border control systems including high rates of False Accept Rate (FAR), trait spoofing, fraud, identity theft, impersonation, and piggybacking.

3.5 Language Translation Systems

Although a Language Translator (LT) is generally meant to enhance information exchange by ensuring that both speech and text are automatically translated and easily interpreted where language is a barrier [39], there are instances where translated output requires protected exchange between LT and the target recipient. Any unlawful modification, unauthorized access, or delayed delivery of such machine-translated [40] output due to spoof-related misidentification can have severe consequences including privacy and confidentiality breaches. Application of the MMRTBLDS framework in such scenarios, guarantees the safe identification of the intended recipient(s) and preserves the confidentiality and integrity of the translated output. This finds ready usefulness in embassy classified diplomatic discussions, consulate interviews, legal proceedings, forensic examinations, chain of custody, parliamentary sessions, etc. Such other environments where certain categories of language/information translation demand the highest level of confidentiality or the preservation of data integrity, would readily embrace the application of the MMRTBLDS framework to ensure effective access control.

3.6 Nuclear Facilities and Highly Sensitive Production Factories

Application of the framework in nuclear facilities and other environments requiring fool proof identification and certification (including pharmaceutical laboratories, food processing plants, identity

repositories, and aviation control systems) could potentially assist in maintaining non-repudiation of transactions and digital operations, thereby averting severe consequences, loss of data and fatalities. In such mission-critical applications, the MMRTBLDS facilitates all-round detection of spoof attempts.

4.0 LIMITATIONS AND FUTURE RESEARCH

4.1 Cost Considerations

The presented simulation of the MMRTBLDS framework shows that it is capable of improving the efficiency and performance of LD as applied in multi-biometric authentication systems. The framework achieves this through randomly selecting unique combinations of liveness detection tests over three different modalities in a manner that is totally unpredictable by the impostor. It is clear that implementing the MMRTBLDS framework would significantly escalate the cost of development and implementation of the Biometric Authentication System due to the need to carry out 15 different liveness tests on 15 traits across 3 different modalities on the sensor module, as well as, additional logic and circuitry required for the decision module.

4.2 Uni-modal Compatibility

Section 4 presented the maximum theoretical efficiency of 99.2%, however, more work is required to determine the robustness against a possible spoof attack of a single trait and/or a single modality (5 liveness attributes). The MMRTBLDS framework does not address spoof attacks against single liveness detection so a successful spoof attack can only occur if the attacker is able to attack all 15 liveness attributes at once, which is currently extremely difficult for the impostor to perform.

4.3 Development of Multi-sensing Biometric Scanners

With the evolution of Body Area Networks, sensor capabilities are expanding [41]. The MMRTBLDS offers the intellectual research foundation into the possibility of developing sensors with multiple capabilities, projected to be tagged *"Multi-sensing Biometric Scanners" (MBS)*. MBS shall be a new generation of biometric scanners capable of performing simultaneous sensing of multiple trait properties from a single scanner, for both biometric identification and authentication purposes. In future, multi-sensing scanners are predicted to replace standalone fingerprint scanners, iris scanners and voice recognition sensors. Multi-sensing Biometric Scanners propelled by the MMRTBLDS framework will introduce a heterogeneous sensor interface capable of simultaneously sensing temperature, pulse rate, oximetry, spectroscopy, vibration frequency and related biomedical attributes and liveness parameters from a single human modality presented to it. MBS shall build more interactivity into the capabilities of Internet of Things (IoTs) and mobile computing, allowing cell phones to securely authenticate voice, face, finger, and gesture through a single contact or contactless electronic sensing interface in a prompt style. The scalability of the MMRTBLDS framework is the bedrock of the Multi-sensing Biometric Scanner concept which will revolutionize electronic sensor technologies, promote digital miniaturization, and improve biometric security and efficiency.

4.4 Automated Randomization

When using more than three liveness detection parameters as inputs, there is a likelihood that the design of the MMRTBLDS framework's decision sub-system presented in Figure 2 could become increasingly complex to implement. 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 2. Our projection is strengthened by recent successful experiments and research in micro-controller based biometric systems already applied in Biometric Attendance [42], [43], Fingerprint based Automated Teller Machine (ATM) [44] and embedded authentication systems [45].

4.5 Vendor-neutral Implementation [2]

There is an identified challenge of incorporating the MMRTBLDS framework into existing uni-modal biometric systems. Fixing this challenge will be a major priority in future work, and such vendor neutrality will ensure interoperability and enable versatility of the framework's application.

4.6 Scalable Operation

The rigid basic functionalities of the framework support well-defined input parameters. These can be made more scalable to widen its scope and flexibility. A future version will allow the use of randomization also on input values as this will allow resilience, adaptability, and better simulation of measurements suitably-influenced by other external factors.

4.7 Performance Improvement and Error Correction

There is a potential operational challenge to the limited design of the framework's computation logic. Since biometric performance can be measured in terms of error rates (ER) [46], including the rate at which spoof-related errors occur, misapplication of the system could escalate inherent errors and cause performance issues. Future refinements of the MMRTBLDS framework will include a robust error correction module to provide a balance between False Reject Rate (FRR) and False Accept Rate (FAR). This is hoped to assist in isolating conflicting performance issues [47], [48] and statistical errors [49]. This will be achieved by applying standard FAR threshold values shown in Table 8 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 would satisfy the requirement of very low FRR for a given FAR [50], [51] in commercial fingerprint-based authentication system.

Table 8: FAR thresholds for biometric strength evaluation [1], [2]

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

5.0 CONCLUSIONS

Operationally, biometric spoofing, or presentation attacks, have severe consequences especially on mission critical applications such as crime investigation, healthcare, border control, and civic digital identity systems. Liveness detection (LD) as a commonly-implemented anti-spoofing technique is now becoming predictable, and inadequate in addressing the growing sophistication of biometric spoofing attacks.

This work presents the Multi-Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework that mitigates biometric spoofing and addresses the limitations of traditional anti-spoofing countermeasures based on a logical combination of randomly selected liveness detection parameters from disparate modalities. The presented results and analysis obtained from a simulation of the MMRTBLDS framework suggests a theoretical maximum system efficiency of 99.2% against predictable direct attacks. The unique strengths of the MMRTBLDS framework in significantly-improving security of Biometric Authentication Systems have been discussed along with practical areas of applications.

The outcome of the research is very useful to the security design of biometric systems deployed in environments where a high degree of access control is required to validate authentic subjects with a potential to improve the performance and efficiency of global biometric and identity-based schemes.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The support and goodwill of the following organizations are greatly appreciated:

- UNESCO International Centre for Theoretical Physics (ICTP), Trieste, Italy.
- Swiss Centre for Biometrics Research and Testing, Martigny, Switzerland.

- Azteca University, Mexico.
- Central University of Nicaragua, Nicaragua.
- National Health Insurance Scheme, Abuja, Nigeria.
- Imo State University, Owerri, Nigeria.
- Idah Polytechnic, Idah, Nigeria.
- Bingham University Karu, Nigeria.

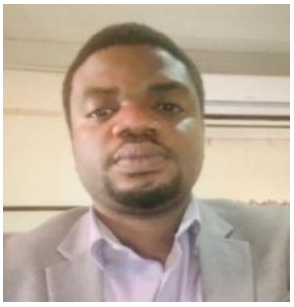
ABOUT THE AUTHORS

Kenneth Okereafor is a United Nations–trained biometric expert with two and half decades of global expertise in cyber threat mitigation technologies across industry, government, and academia. He holds a PhD in Biometrics & Cybersecurity from Azteca University Mexico and is a former employee of the US Department of State. He is currently a Deputy General Manager at Nigeria's National Health Insurance Scheme (NHIS), where he coordinates database security and health informatics. He has been involved with country-level professional service for the International Organization for Standardization (ISO) and currently chairs ISO's Technical Committee & National Mirror Committee (TC & NMC) on ISO/TC-215 Health Informatics Standards Working Group 4 - "Security and Privacy" in Nigeria, developing cybersecurity standards for Nigeria's eHealth ecosystem. With a second PhD in Information and Communications Technology (ICT) Administration and Governance, Kenneth is an alumnus scientist of the UNESCO International Centre for Theoretical Physics, Italy, and has published several papers on Biometrics, Cybersecurity, eHealth, Telemedicine, and Digital Forensics.

Oliver E. Osuagwu is a Professor of Computer Science at the Imo State University Nigeria. He has over 30 years of enriched experience in the teaching and practice of computing and IT and has made tremendous contributions to the Nigerian University system. He holds a Doctor of Science degree in Computer Science from Azteca University, Mexico, PhD in Information Technology from the Central University of Nicaragua, and PhD in Computer forensics from American Heritage University of Southern California. Prof Osuagwu has mastery over Software Engineering, Computer Networks, Cybersecurity and Computer Forensics as well as Programming (structured and OOP). He is the first Chartered Fellow of the renowned British Computer Society (BCS) in South Eastern Nigeria, and also a Chartered Fellow of

the Nigeria Computer Society (NCS) and Computer Professionals Registration Council of Nigeria (CPN). He has graduated over 25 PhD and 250 MSc candidates in Computing and IT. Prof Osuagwu has published several academic books in use in Nigerian Universities, and over 150 published articles in competent journals and international conferences.

Sani Felix Ayegba is a Principal Lecturer in the Department of Computer Science at Federal Polytechnic Idah, Nigeria. He holds dual PhD in Computer Science and Information Technology from Universidad Azteca, Mexico, and Universidad Central De Nicaragua, respectively. His research interests include Human Language Engineering, Machine Learning and Cybersecurity. Sani is very passionate about Computer Science education and has contributed to several curriculum assessment and development programmes within the academia.



Oluwasegun Ishaya Adelaiye is a lecturer in the Department of Computer Science at Bingham University, Karu, and a PhD candidate at the University of Abuja, Nigeria. He has published over ten academic articles and has supervised over a dozen undergraduate students. He has a BSc in Computer Science from University of Abuja and an MSc in Information and Network Security from Robert Gordon University, UK. Adelaiye's research interests include cybersecurity, network security, anomaly detection and machine learning.

References

[1] 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. "IEEE Xplore Digital Library", 17 May 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8359039/. [Accessed 2018].

[2] K. U. Okereafor, O. E. Osuagwu and C. Onime, "Biometric Anti-spoofing Technique Using Randomized 3D Multi-Modal Traits," International Journal of Simulation, Systems, Science & Technology (IJSSST), vol. 19, no. 5, pp. 5.1-5.8, 2018. https://ijssst.info/Vol-19/No-5/paper5.pdf

[3] O. E. Osuagwu, Software Engineering: A pragmatic approach, Owerri: Spring, 2010.

[4] 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.

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

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

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

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

[9] 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.

[10] Q. Gao, "A Preliminary Study of Fake Fingerprints," International Journal of Computer Network and Information Security (IJCNIS), vol. 12, no. 1, p. 7 21, 2014.

[11] H. İnaç and F. Ünal, "The Construction of National Identity in Modern Times: Theoretical Perspective," International Journal of Humanities and Social Science, vol. 3, no. 11, pp. 223 - 232, 2013.

[12] I. A. Ibrahim and Y. Abubakar, "The Importance of Identity Management Systems in Developing Countries," International Journal of Innovative Research in Engineering & Management (IJIREM), vol. 3, no. 1, pp. 1 - 12, 2016.

[13] Y. ALKHURAYYIF, "National ID Cards," International Journal of Computing Science and Information Technology, vol. 1, no. 2, pp. 44 - 48, 2013.

[14] D. STACEY, "India leads the way in biometrics with huge database," WALL STREET JOURNAL, New York, 2017.

[15] 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.

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

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[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] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

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

[30] 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.

[31] 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.

[32] 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. https://www.ajol.info/index.php/wajiar/article/view/145878/135395

[33] "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].

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

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

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

[37] 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.

[38] 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.

[39] İ. Erton and Y. Tanbi, "Significance of Linguistics in Translation Education at the University Level," JOURNAL OF LANGUAGE AND LINGUISTIC STUDIES, vol. 12, no. 2, pp. 38 - 53, 2016.

[40] R. Fiederer and S. O'Brien, "Quality and Machine Translation: A realistic objective?," The Journal of Specialized Translation, vol. 11, pp. 52 - 74, 2009.

[41] S. Memon, M. Sepasian and W. Balachandran , "Review of fingerprint sensing technologies," in IEEE International Multitopic Conference (INMIC), 2008.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

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

[47] 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.

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

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

[50] 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.

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