Multi-biometric Liveness Detection – A New Perspective

Kenneth Okereafor [1], Oliver Osuagwu [2], Clement Onime[3]
3

[1] Nigerian National Health Insurance Scheme (NHIS) , Abuja. nitelken@yahoo.com
[2] Department of Computer Science, Imo State University, Owerri profoliverosuagwu@gmail.com
[3]Department of ICT, Abdul Salem International Centre for Theoretical Physics, Trieste Italy onime@ictp.it

Abstract

The problem of securing valuable data stored in databases has been of great concern to organizations and individuals alike. The more worrisome is the increasing complexity of fraud perpetration by cyber criminals which demands that a more secure method be deployed. Basic Multi-biometric Authentication System was thought to have sealed the vulnerabilities and escape route from cyber criminals, but emerging attack patterns have proved us wrong. In spite of their benefits, multi-biometric systems also have peculiar challenges especially circumvention of security strategy, that is, how susceptible the system or the presented biometric modality is to spoof attacks and identity fraud. Liveness detection has been applied as an anti-spoofing mechanism to checkmate circumvention, however its application approach has thrown up more vulnerabilities. In this paper, we introduce our work and adopt the Structured Systems Analysis and Design Methodology (SSADM) to assist us understand the weaknesses and propose a solution which integrates liveness detection to halt spoofing of legitimate subjects, and propose a different approach for performing liveness detection in multi-biometric systems that significantly minimizes the probability of circumvention and strengthens the overall security strategy of the authentication process. The expected output of the research is a prototype software for multi-modal biometrics that detects, in a randomized sequence, the absence of liveness and blocks access to critical infrastructure by fraudsters.

Keywords: *Authentication, biometrics, liveness detection, spoofing, trait.*

1.0 Introduction

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 in seeking to advance the proper and beneficial use of biometrics [1]. We are motivated by the idea that the proper application of appropriate technology can curtail the rising spate of cyber criminalities around the globe, specifically by refining the existing biometric liveness detection process into a more secure anti-spoofing mechanism. The goal of this research is to design and develop a software prototype for enhanced liveness detection, capable of performing multiple instances of different trait verifications using alternating traits and modalities from the same person for each successive instance. In this work, we adopt multi-mode biometrics using finger, face and voice modalities.

Human traits that are suitable for biometric purposes in line with the generic qualities specified by [2] and [3] are first captured by a sensor to generate an image which later gets processed through feature extraction into a template. Biometric templates exist in the form of electronic data that can be manipulated in similar ways as any other form of digital data element. Once the templates are captured into the appropriate database (DB) or biometric repository, they become useful for pattern recognition in either the identification or the verification (authentication) mode.

Given the criticality of biometric templates for authentication, it becomes necessary to deploy adequate all-round protective mechanisms and systems to secure them in storage, in process and in transit. Although the security of some of the deployed protective systems is questionable when utilized alone, integration with other technologies such as Identity Based Encryption (IBE), Public Key Infrastructure (PKI) or digital signatures results in cryptographically secure applications of biometrics [4], which gives a reasonable guarantee of an encrypted biometric authentication.

2.0 Securing Biometrics With Cryptography

The concept of encrypted biometrics evolved in the quest to mitigate the effects of compromised biometric template. For a system that uses biometric templates for identification and authentication, there is the issue of what to do when a template has been compromised [5]. For a mere password or token-based system, the solution is straightforward; the user performs a password reset or gets a new physical token. However, in a case of iometric template compromise, user cannot renew his iometrics such as grow a new finger or swap to a spare yeball. It appears the solution to a compromised iometric template lies in the application of the revocable eatures of biometric templates.

Revocable templates are biometric templates that have een enhanced through several different cryptographic ethods to allow for the revocation and reissuance of the xisting biometric token without modifying the underlying biometric [5]. Revocable biometric templates are also called cancellable biometrics. They are the resulting code generated when biometric data has been converted into random strings suitable to apply cryptographic techniques for security. The extraction is usually done by fuzzy extractors [6] or secure sketches. Figure 1 below depicts a typical sequence that generates revocable biometric templates

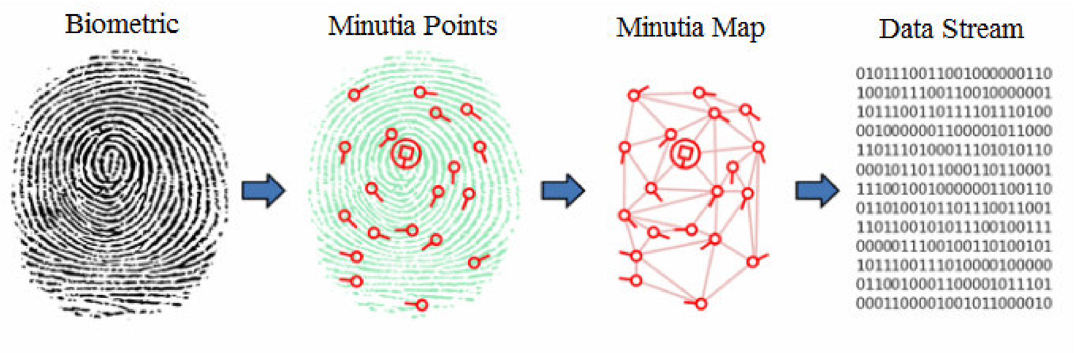


Figure 1: Sequence for the revocable biometric templates process. Adapted from [5]

Two methods commonly used to create cancellable iometric templates are *salting* and *one-way ransformations* [5]. Whereas *salting* inserts a known set f fake data into predetermined locations of the template disguise it and allow compromised biometric template be recovered, *one-way transformations* distort the iometric template in a revocable but irreversible manner ereby increasing privacy and accuracy. Since it becomes mpracticable to reveal information from the cancellable iometrics template, the one-way transformations used to reate them is also known as non-invertible transforms [7]. ancellable biometric templates are essential for biometric uthentication systems (BAS), especially for those perated under unattended and/or over networked nvironments.

.0 The Liveness Detection (LD) Landscape

Despite the superiority of Biometric Authentication ystems (BAS) over passwords and PINs that can be orgotten or physical tokens that can be damaged, isplaced or stolen, they are still not foolproof. Spoofing r copy attack) is a fatal threat for BAS [8], and occurs hen an impostor attempts to mimic the traits orresponding to legitimately enrolled subjects [9]. The bility to detect spoof attempts is a measure of the erformance and security of BAS.

Liveness Detection (LD) is the process of verifying at the biometric modality presented or rendered before a biometric verification system for the purpose of capturing the biometric trait is real and not fake [10]; and that such a presenter is medically alive [11], and physically present at the moment of such capture [12]. LD reads claimant's physiological signs of life [13]. Biometric circumvention describes to what extent a biometric system can be fooled using fraudulent methods [14], and how susceptible the modality is to spoof attacks [3] and identity fraud [2].

The goal of any anti-spoofing approach is to strengthen the security of biometric authentication, and at a basic level, LD is an anti-spoofing mechanism that attempts to answer questions concerning the originality of the trait presented before the BAS scanner. In our analysis though, we identified that the factors that influence the use and effectiveness of any liveness detection techniques include (i) ease of trait acquisition, (ii) nature of trait in view, (iii) tolerable level of intrusiveness, and (iv) duration of processing. The overall LD goals are better security and sustenance of a reasonable balance between False Accept Rate (*FAR*) and False Reject Rate (*FRR*) incidents. A well-applied *LD* technique should guarantee a *FAR* low enough to ward off the possibility of incorrectly authenticating impostors, and a marginal *FRR* low enough not to reject legitimate users.

3.1 Aspects of LD in Focus

Effectively, LD denotes the methods capable of discriminating real human traits (live or non-live) from synthetic counterfeits made by silicon [15], gelatin [16] or play-doh [17], with the help of appropriate spoof mitigation algorithms [18]. Checking for signs of vitality involves the search for, and measurement of, certain intrinsic properties [11] (such as thermal, optical, mechanical and electrical quantities), involuntary properties [8] (such as blood flow, oxygen saturation and pulse rate), and response to external stimuli (such as eye blinking). These elements must be tested for verification. In this section, we critically analyse some measurable quantities (metric) required for running liveness detection checks on selected traits.

Fingerprint LD

The use of fingerprint recognition for access control and other uses is becoming increasingly common due to its security and ease of use [5]. Despite its broad application, the existing fingerprint recognition systems can be easily deceived, for example, by presenting a well-duplicated synthetic finger [19]. A vital question on fingerprint LD is "*how do we verify that the fingerprint image presented before a thumb scanner or fingerprint reader is not an artificial finger or a fake dummy finger fabricated out of gelatine* [16], *play-doh* [17], *silicon* [15] *or any other spoofing tactics* [18]*; or molds made out of latent fingerprints stealthily picked from or left by legitimate users, or from the dismembered thumb* [20] *of the real enrolee?*"

In attempting to answer this question, fingerprint LD tests check for signs of vitality using an analysis of measurement of some or all quantities as shown in Table 1

Table 1: Quantities evaluated in a fingerprint LD test

SN	Quantity	Description
1	Warmth	Test for the presence of normal warmness within acceptable temperature range for a living human body.
2	Pulse	Test for the presence of pulse on the finger as evidence of the presence of a natural heartbeat.
3	Density	Test for the pressure tolerance, elasticity and texture upon contact with the finger.
4	Haemoglobin	Test for the presence of blood flow.
5	Oxymetry	Test for the appropriate saturation of oxygen in the blood inside the finger.
6	Blood pressure [15]	Test for the presence of the force exerted by the heart's action of pumping and circulating blood, in relation to the diameter and elasticity of the arterial walls within normal blood pressure range for each given gender.
6	Spectroscopy	Test for the relative absorption or reflection or radiation (eg Infra Red light) on the submitted finger.
7	Perspiration	Test for the presence of secreted sweat from pores only found in real live human finger traits.

Facial print LD

Primarily facial recognition measures the overall facial structure including distances between eyes, nose, mouth, and jaw edges [21]. Generally speaking, there are three ways (also called replay-attacks [22]) to spoof facial recognition [23] as follows: (i) photograph of a valid user, (ii) video of a valid user, and (iii) 3D model of a valid user. After acquiring the facial image [24], face recognition processing [23] in BAS involves four steps:

- Step 1: The face image is enhanced and segmented.
- Step 2: The face boundary and facial features are extracted.
- Step 3: The extracted features are matched against features in the DB.
- Step 4: The classification or recognition of the user is achieved.

While all four steps are implemented differently by different vendors [25], a significant question in facialprint LD is *"can we determine, with some degree of certainty, that the facial image presented before a biometric facial camera is not a portrait picture of a legitimate user merely presented as a static paper photograph, or disguised in a facial mould or a mask; or a mere screen/video display of the valid user's picture?"* Table 2 highlights typical quantities measured in a facialprint LD

Table 2: Quantities evaluated in a Facialprint LD test

SN	Quantity	Description
1	Nodal geometry	Test for the conformity of the geometry of nodal points on the face including nose, cheek, jaw, eye, socket, forehead, etc.
2	Facial expressio n	Test for conformity of trait to involuntary actions and response to stimuli such as smile, frown, wink, etc.
3	Mouth moveme nt	Test for the presence of the natural pattern of human mouth movement during speech.
4	Eye blinking	Test for the presence of a sequence that indicates the pattern of human eye action.
5	Facial thermogr am	Test for the presence of radiation only emitted by a living human face.

Voiceprint LD

The voice recognition system uses the unique characteristics of the human voice including measurement of audible frequency, tone, pitch, etc to distinguish the subject and used for confirmation of liveness in authentication. Detecting elements of liveness in the human voice asks the relevant question: *"How can we confirm that the voice image presented before a voice recognition system is not a playback of a pre-recorded audio clip, or a synthesized voice clip of the legitimate user; or from a physically-present impostor who is anonymously mimicking the voice of an authentic user?"*

Vein pattern LD

LD in a vein pattern modality essentially checks for palm vein matching quantities whose measurement connote the presence of life in the subject including blood flow, contour synthesis, geometry of fingers, oxymetry, spectroscopy, pulse rate, blood pressure, etc. A pertinent question regarding vein pattern LD is *"to what extent can we verify that the hand modality presented before a vascular pattern reader or hand geometry scanner is from a valid user and also a living hand naturally attached to a living human body and not a standalone dismembered part or from a cadaver?"*

Eye LD for iris and retina patterns

The focus of eye biometrics is basically to identify vitality signs that show proof of the presence of a live human eye whose iris and retina show measurements indicating liveness. The vital question is *”how do we verify that the eye image presented before a retina scanner or iris sensor is not faked with a mimicking contact lens or other eye image enhancing agents?”*

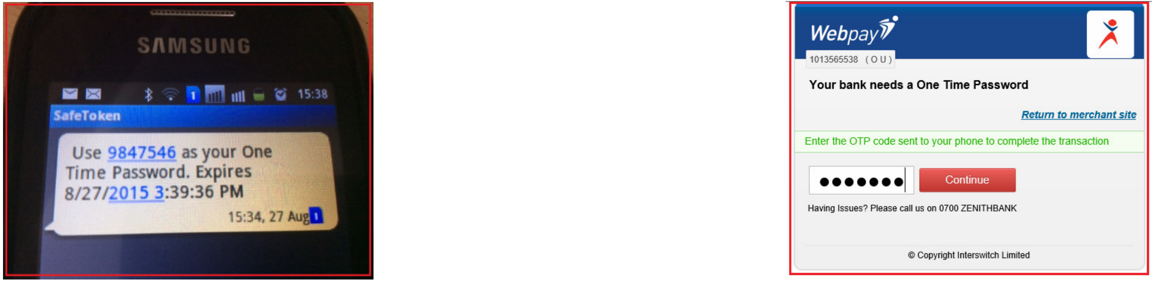
Measurable quantities for detection of real living iris or retina include a combination of physiological characteristics and involuntary actions such hippus movements, eye blinking, coloration, blood flow, temperature checks, etc.

Keystroke pattern LD

Keystroke liveness check tends to ask the question *“How can we truly confirm that the keystroke patterns presented before typing sequence sensor are generated from a real physical keypad and are coming from the typing action of a real physical human being and not from a pattern captured by a key logger attack tool or simulated by other keystroke pattern generators?”*

3.2 One-Time Password (Otp) Security Imperatives

OTP was introduced to provide a pseudo password in form of a one-off access code to deal with one of the major weaknesses of traditional password, reusability. An OTP is a password code used to perform a timed single instance authentication without possibility of reuse in future transactions. OTP is mostly used by online payment systems to provide a one-off password code which is sent to the user’s email address or phone number and must be used within a specified limited timeframe beyond which the OTP expires. An expired OTP becomes unusable and a new code must be generated and used to complete the transaction. Apart from its short-lived lifespan, a significant security benefit of an OTP lies in the added association with the user’s personal telephone number and/or email address. Figure 2 below shows a sample of an OTP sent as a Short Message Service (SMS) safe token message to a user’s phone number for use in the authorization of an online payment transaction



Use 9847546 as your One Time Password. Expires 8/27/2015 3:39:36 PM

15:34, 27 Aug

1013565538 (O U)

Your bank needs a One Time Password

Return to merchant site

Enter the OTP code sent to your phone to complete the transaction

●●●●●●● Continue

Having Issues? Please call us on 0700 ZENITHBANK

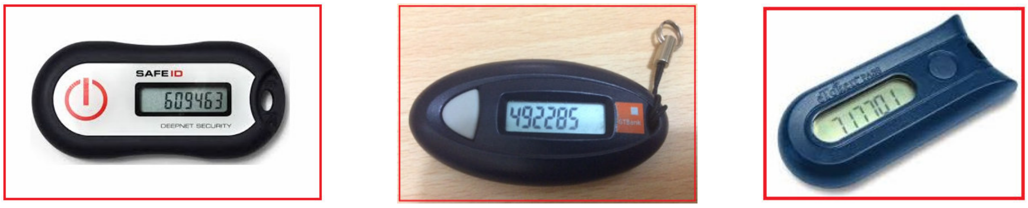
© Copyright Interswitch Limited

(a) *(b)*

Figure 2: One Time Password implementations showing (a) 6-digit token sent via sms, and (b) online payment authorization portal [26] *where the sent token is entered as secure approval code to complete a pending transaction.*

For example the ComBiom ® Safe ID USB stick [27] offers a multi-functional token with integrated biometric authentication that enables physical access control and logical access control in one token. Figure 3 below shows several hardware tokens that randomly generate fixed length, short-lived, unique codes for access control and authorization of online payment transactions

.



(a) (b) (c)

Figure 3: Hardware tokens used to generate random 6-digit OTP security codes for (a) access control [27], and (b), (c) online payment authorization.

To secure the biometric authentication process in a multi-factor environment, we take advantage of the widespread use and reliability of OTPs to introduce an added element of further strength in corroborating identity and forestalling circumvention of the authentication process.

2.3 How Significant Is Multi-Biometric (Mb) Fusion?

No single biometric method to date can guarantee a 100% authentication accuracy and usage by itself. Multi-biometrics evolved in response to the need to build more security into BAS. The combination of multiple biometric sources, modes and more formidable methods of authentication is referred to as multi-biometric fusion, and such a system that operates through any of such combination is often called a multi-biometric system [10]. MB is the concurrent application of more than one biometric source, method or other determining factors as a distinguishing element of authentication.

The uniqueness of the multi-biometric concept lies in its emphasis on multiple application of variables, methods or factors as simplified in Table 3.

Table 3: Description of the multi-biometric fusion concept

	Multi-Biometric Fusion Technique	**Description Of Technique**	**Example**
	Multi-sample	Multiple presentation of a sample in varying fashions.	4R Fingers + 4L Fingers + 2 thumbs (4-4-2)
	Multi-mode OR Multi-identifier	Multiple presentation of a sample from multiple sources.	Thumb + Face + Voice + …
	Multi-system	Multiple application of different biometric hardware from different OEMs assuming vendor interoperability is guaranteed.	System$_1$ + System$_2$ + System$_3$ + … Example, using the Lumidigm ® Mercury M301 fingerprint reader together with the Verifi ® P5100 thumb scanner [28].
	Multi-algorithm	Application of multiple matching algorithms to a single trait in sequence. Using different processing and feature extraction methods on the same biometric data.	PCA$_{a1}$ + ICA$_{a2}$ + LDA$_{a3}$ + … Example, [29] discusses a face recognition system that combines three different global feature extraction schemes (Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminant Analysis (LDA).
	Multi-sensor	Processing of similar samples with multiple sensors. Multi-sensor systems employ multiple sensors to capture a single biometric trait [9] or modality of an individual [10].	(Face)$_{s1}$ + (Face)$_{s2}$ + … Example, a face recognition system may deploy a 2D camera to acquire the face image, and an infrared sensor in conjunction with a visible-light sensor to acquire the subsurface information of a person’s face.
	Multi-instance OR Multi-unit	Application of repeated instances and iterations of sources. Here the same modality or trait is recorded in terms of multiple instances or parts.	Li + Ri + … Example, left iris followed by the right iris of an individual.
	Hybrid model	Concurrent utilization of multiple fusion techniques.	A mix of many techniques and sources in one.

4.0 Identified Problems With Current LD Approach

In general, LD is an embedded function of the biometric scanner and different manufacturers implement it in different ways, generally proprietary to each vendor [25], but the problem lies in the way the liveness detection check is currently run in multi-biometric systems by many vendors as a single instance process.

(1) **Deficient technique:** As far as we know from available literature, there appears not to be much research into a single biometric system that performs multiple simultaneous instances of liveness checks on the same person using different traits at each instance prior to authentication. To the best of our knowledge, no such system has been proposed either. Most biometric authentication systems are either limited in the number of instances checked for liveness or are completely unimodal in nature.

(2) **More Vulnerable:** The gap introduced by the deficiency of multiple simultaneous instances of liveness checks using multiple traits from the same subject has serious security implications. The risk is that after a smart attacker has performed reconnaissance, he can launch a spoof attack targeting only a single liveness detection technique on a single trait, concentrating all efforts at achieving this by taking advantage of the system not having a way of associating each single liveness check of a person's trait to another liveness check on a different trait of the same person for consistency. This security glitch is too grievous to be ignored by the global Cybersecurity community.

(3) **Intrusiveness:** Operationally, the average biometric user becomes uncomfortable if the trait acquisition method tends to be too invasive, restrictive, demanding or time-consuming; for example a theoretical multi-identifier liveness detection process could require a user to recite a pre-written text (*test for voice liveness*), while holding a pulse meter (*test for vein liveness*), and staring at an iris scanner (*test for iris liveness*) either simultaneously or in sequence. In the circumstance, and even where no physical contacts are made with sensors, many users still develop a natural apathy against the entire biometric liveness detection process describing it as grossly intrusive.

(4) **Limited Systems Design:** A good number of existing unimodal biometric systems do not have a built-in liveness detection module and most uninformed users are equally unaware of the implications of this limitations. Economic factors top the list of reasons for the acquisition of low grade systems that are deficient in the liveness detection component. On the part of the Original Equipment Manufacturers (OEM)s and vendors, inadequate Research and Development (R&D) is a major factor militating against the design and development of quality biometric systems with embedded liveness detection component.

4.1 Proposed Mitigation Approaches

The way and manner, hence the approach, in which LD is applied in a biometric authentication system is significant to determining the level of security expected and achieved. Using the Structured Systems Analysis and Design Methodology, we have thoroughly reviewed existing liveness detection techniques focusing on their performance, user acceptance, intrusiveness and security effectiveness against spoof attacks. We also examined the comments of various classes of biometric system end-users and their expectations from future developments.

Based on our analysis of the current liveness detection landscape, and having identified its inherent technical and operational weaknesses, we have developed a new model of trait vitality checks that is capable of enhancing the effective security of the biometric authentication strategy while remaining non-intrusive and user-friendly. We present an introductory part of our iterative (recursive) trait liveness verification model as a series of three approaches, namely:

- **Combination approach**

Apply one LD method on a particular biometric trait followed by another dissimilar LD method on a different trait, from the same enrolee. The rationale of our approach is based on the fact that physically uncorrelated modalities or traits (E.g. retina and fingerprint) usually yield stronger security and improved performance than correlated modalities or traits (E.g. lip movement and voice) [9].

First assumption (consistency)

In our model, we assume that at any time during the authentication process,

$$\mathbf{LD_{count}} = \mathbf{T_{count}}$$

where $\mathbf{LD_{count}}$ = Number of liveness detection instances, and

$\mathbf{T_{count}}$ = Number of traits prompted for.

The rationale is that, applying *n* separate LD methods (supposing an *n*-factor multi-biometric authentication) on *n* separate traits but from the same subject, defeats the attack purpose since an attacker would naturally be xpected to perform *n* separate spoofs, one for each of the iveness detection techniques applicable to the particular rait used or prompted for.

econd assumption (paranoia)

Ve further assume that the attacker has cleverly produced ll possible spoofs applicable to a particular trait in eadiness to any liveness detection check applicable to his arget trait only.

herefore prompting for a second, a third, and possibly an th different instance of liveness detection using a different trait for each instance makes it more difficult for the attacker to successfully circumvent all the options.

The near-intractability of (the attacker) having to spoof each known liveness detection method for each trait used in the biometric authentication system, up to the count of liveness detection instances permissible in the system, decreases the probability of spoofing, discourages the attacker and greatly improves the overall system security. Our approach is illustrated with some tables below .

Table 4: Our LD approach, instance 1 on fingerprint trait

LD Instance 1	Modality	Human thumb/finger
	Trait 1:	Fingerprint
	LD checks applied	Test of warmth (temperature test).
		Test of oxygen saturation in blood (oxymetry test).
		Test of sweat secretion from pores (perspiration test)
	Probability score	**P1**

Table 5: Our LD approach, instance 2 on facialprint trait

LD Instance 2	Modality	Human face
	Trait 2:	Facial print
	LD checks applied	Test for instantaneous radiation (facial thermograph).
		Test for effect of background illumination.
		Test of light absorption (spectroscopy) on skin.
		Test for effect of variable focus.
		Test of eye blinking sequence.
		Test for natural facial expressions (smile, frown, etc.)
	Probability score	**P2**

Table 6: Our LD approach, instance 3 on iris pattern trait

LD Instance 3	Modality	Human eye
	Trait 3:	Iris pattern
	LD checks applied	Test of pupil pulsation (Hippus test).
		Test of infra-red scattering
		Aqua reflection density test.
	Probability score	**P3**

Table 7: Our LD approach, instance 4 on voiceprint trait

LD Instance 4	Modality	Human voice
	Trait 3:	Voiceprint
	LD checks applied	Test for frequency within the audible range.
		Test for concurrency with lip movement.
		Other ancillary tests
	Probability score	**P4**

Probability

Overall probability of liveness is the mean of **P** expressed as a percentage.

$$P_t = \underline{P_1 + P_2 + P_3 + P_4 \ldots + P_n} \qquad (1)$$

$$\sum \qquad f(p)n/ \qquad n$$

(2)

The probability module built into the LD algorithm computes the mean matching score based on a predefined rule-set determined partly by the count of instances and the security criticality required from the system in its area of application, which is the basis for the manual calibration of the system. The system calibration determines its sensitivity in controlling error rates.

System tolerance

To reduce the probability of high False Accept Rates, our system is built to tolerate a low score from not more than one LD instance per subject.

Randomization approach

By randomizing the choice and sequence of the possible liveness detection instances through appropriate algorithm, the attacker faces the unpredictability of guessing which next trait to expect and this situation further reduces his chances of beating the False Accept Rate (FAR) – False Reject Rate (FRR) balance. Randomization is automated as a built-in programme module into the BAS to increase overall security.

By prompting the user for a random set of traits at the point of acquisition [9], our model shows that the multi-biometric activates a challenge-response mechanism, ensuring that the system is interacting with a live user. Furthermore, to maintain the FAR - FRR balance (and sustain a zero tolerance for type-2 errors), the sensitivity of the BAS can be tuned to such a less-sensitive range that False Accept (FA) possibilities are significantly reduced without considerably impacting on False Reject (FR).

Innovativeness of the Proposed Approach

A lot of innovations can be built around this concept of iterative (recursive) Liveness Detection.

Simultaneity

Firstly, the fusion of the combination and randomization approaches constitutes a unique iteration, a sequencing we term recursive liveness detection. Our approach allows for simultaneous liveness checks on multiple traits, thereby minimizing delays and reducing possibility of fatigue-induced user apathy.

Synchronized processing

Secondly, the BAS can run the matching algorithm in synch with the trait supply thereby minimizing delays and overbearing processing time.

5.0 Further Research

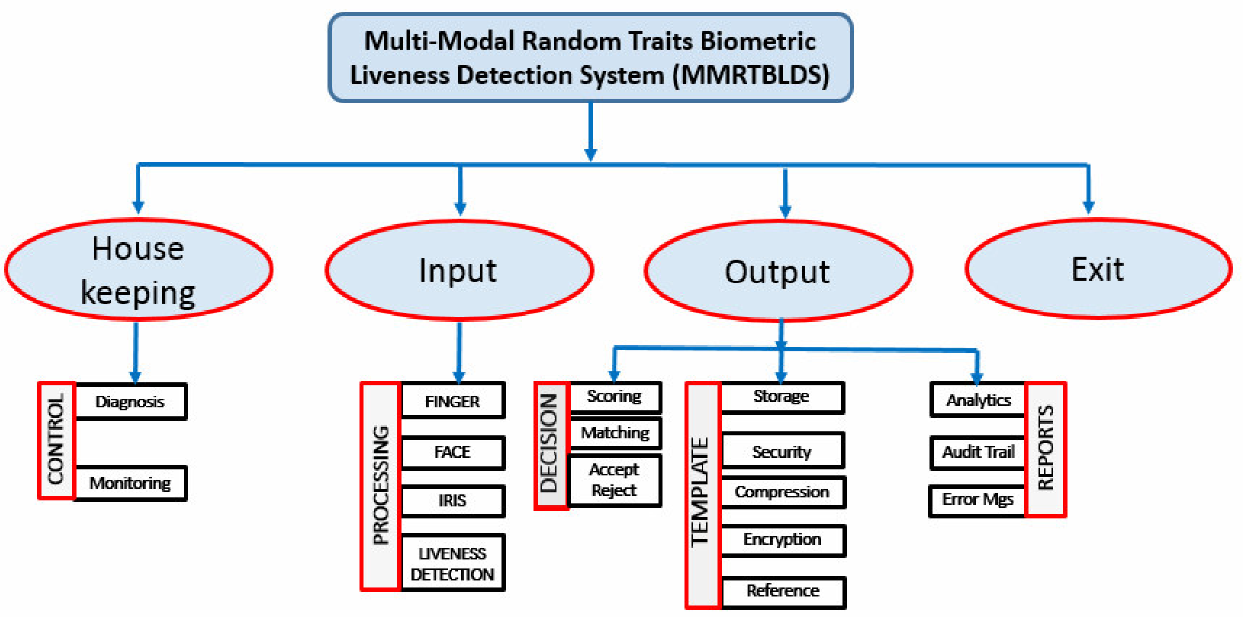
Untapped areas exist in MB and LD, including the need to focus research on developing a comprehensive taxonomy of LD necessary to advance further knowledge in the field of biometric securit

6.0 Conclusion

Biometric technology and Biometric Authentication Systems (BAS) have come to stay, at least going by the rate of advancing research and development including innovations in LD techniques. Every LD technique tends to ask "*does the biometric sample being captured represent an actual measurement from an authorized, live person?*" A negative answer connotes circumvention, and all known biometric modalities and traits can be circumvented with varying degrees of ease irrespective of whether physiological or behavioural. Although each trait possesses measurable characteristics that can be used to verify liveness and checkmate spoofing, it is the application of these characteristics that makes all the difference. The way and manner, hence the approach, in which the LD technique itself is applied within the BAS is significant to determining the level of security expected and achieved.

In this paper our biometric liveness detection approach which is based on the appropriate combination of traits from different uncorrelated modalities of the same person in a recursive manner has been presented. The outcome of our study will hopefully assist future development of anti-spoofing countermeasures not only to detect and prevent but also to mitigate effects of successful spoof attacks. The expected Liveness Detection prototype runs on Oracle Relational Database Management System (RDBMS) as the backend engine, the Open Database Connector (ODBC) as Application Programme Interface (API) and in Java as the front engine development language. The High Level Model illustrated in Fig 4 consists of a control centre with the following automation boundaries: housekeeping, biometric inputs, analytics module, metric computation module, report \module

.



Module. etc.

Fig **3.4: High Level Model of the Multi-Moda l Random Trait Biometric Liveness Detection System**

References

[1] S. Marcel and A. Nouak, "European Association for Biometrics (EAB) establishes new pan European research collaboration," European Association for Biometrics, Naarden, The Netherlands, 2015.

[2] A. K. Jain, "Some Challenges In Bometrics: Facial Sketch, Altered Fingerprints & SMT," Idiap Speaker series: Swiss Centre for Biomerics Research and Testing, Martigny

Switzerland., 2013.

[3] "Biometrics Metrics Report v3.0," US Military Academy, 2012.

[4] N. D. Sarıer, "Biometric Cryptosystems Authentication, Encryption and Signature for biometric identities," Istambul, Turkey, 2011.

[5] Dev Technology, "Emerging Biometric Technology: Revocable Biometric Features," Dev Technology Group, 7 Nov 2013. [Online]. Available: http://devtechnology.com/emerging-biometric-technology-revocable-biometric-features/. [Accessed 27 April 2016].

[6] J. Bringer, H. Chabanne and B. Kindarji, "Identification with Encrypted Biometric Data," in *Communication on Information Systems Security Symposium, International Conference on Communications (ICC) 2009*, Dresden, Germany, 2009.

[7] K.-H. Cheung, A. Kong, J. You and D. Zhang, "An Analysis on Invertibility of Cancelable Biometrics based on BioHashing," Biometrics Research Centre, Department of Computing, The Hong Kong Polytechnic University, Hung Hom,, Kowloon, Hong Kong..

[8] S. A. C. Schuckers, "Spoofing and Anti-Spoofing Measures," Elsevier, New York, 2002.

[9] A. Ross, "AN INTRODUCTION TO MULTIBIOMETRICS," in *15th European Signal Processing Conference (EUSIPCO 2007)*, Poznan, Poland, 2007.

[10] H. Li, K.-A. Toh and L. Li, Advanced Topics in Biometrics, World Scientific Publishers, 2103.

[11] G. S. Sawhney, Fundamentals of Biomedical Engineering, New Delhi: New Age International (P) Ltd., Publishers, 2007.

[12] "Biometrics - Presentation Attack Detection - Part 3: Testing, Reporting and Classification of Attacks.," ISO/IEC Standard JTC 1/SC 37 30107-3, 2014.

[13] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: A tool for information security," *IEEE Transactions on Information Forensics and Security,* vol. 1, no. 2, pp. 125 - 143, 2006.

[14] "The impact of biometrics: Technologies of Control," 2015. [Online]. Available: https://www.le.ac.uk/oerresources/criminology/msc/unit8/page_19.htm. [Accessed April 2016].

[15] 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.

[16] 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.

[17] 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.

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

[19] E. Marasco and C. Sansone, "Combining perspiration- and morphology-based static features for fingerprint liveness detection," *Journal of Pattern Recognition Letters,* vol. 33, no. 9, p. 1148 –1156, 2012.

[20] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," Elsevier Ltd., New York, 2007.

[21] O. S. Adeoye, "Multi-mode Biometric Solution for Examination Malpractices in Nigerian Schools," *International Journal of Computer Application (0975 - 8887),* vol. 4, no. 7, pp. 20 - 26, 2010.

[22] I. Chingovska, A. Anjos and S. Marcel, "On the Effectiveness of Local Binary Patterns in

Face Anti-spoofing," *IEEE In Proceedings, International Conference of the Biometrics Special Interest Group (BIOSIG) 2012,* September 2012.

[23] G. Pan, Z. Wu and L. Sun, "Liveness Detection for Face Recognition," Department of Computer Science, Zhejiang University , China, [Online]. Available: http://cdn.intechopen.com/pdfs-wm/5896.pdf..

[24] B. G. Nalinakshi and S. M. Hatture, "Liveness Detection Technique for Prevention of Spoof Attack In Face Recognition System," *International Journal of Emerging Technology and Advanced Engineering,* vol. 3, no. 12, 2013.

[25] D. Simon, "On liveness algorithm fusion.," Secure Planet, Washington DC. , 2015.

[26] "Online payment engine," Webpay, [Online]. Available: http://www.interswitchng.com/#WEBPAY. [Accessed 2015].

[27] "ID All-in-One through USB Token," Biometric Swiss Identity Security Solutions, 2014.

[28] "Fingerprint Scanner Reviews (Top 10 Reviews)," reviews & comparisons, 2016. [Online]. Available: http://www.toptenreviews.com/computers/scanners/best-fingerprint-scanners/. [Accessed April 2016 2016].

[29] X. Lu, Y. Wang and A. K. Jain, "Combining Classifiers for Face Recognition," *IEEE International Conference on Multimedia and Expo (ICME),* vol. 3, pp. 13 - 16, 2003.