International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(4): 498-507
The Society of Digital Information and Wireless Communications, 2015 (ISSN: 2305-0012)

A Framework for Integrating Multimodal Biometrics with Digital Forensics

[1]Victor R. Kebande † and [2]Nickson M. Karie*

[1]Department of Computer Science,
Egerton University, Njoro
Box 536, Egerton, Kenya
[2]Department of Computer Science, Kabarak University,
Private Bag - 20157, Kabarak, Kenya
vickkebande@gmail.com†, nkarie@kabarak.ac.ke*,

ABSTRACT

Multimodal biometrics represents various categories of morphological and intrinsic aspects with two or more computerized biological characteristics such as facial structure, retina, keystrokes dynamics, voice print, retinal scans, and patterns for iris, facial recognition, vein structure, scent, hand geometry, and signature recognition. The objectives of Digital Forensics (DF), on the other hand, is to inspect digital media in a forensically sound manner with the essence of identifying, discovering, recovering, analysing the artifacts and presenting facts and suggestions about the discovered information to any court of law or civil proceedings. Because the accuracy of biometric indicators may rarely be investigated during a digital forensic investigation processes, integrating digital forensics with multimodal biometrics can enable effective digital forensic investigations on multiple captured physiological and behavioural characteristics.

This paper, therefore, presents a self-adaptive approach for integrating digital forensics with multimodal biometrics. This is motivated by the fact that, as of the time of writing this paper, there is lack of effective and standardised methods for performing digital investigation across multimodal biometric indicators. In addition, there are also no proper digital forensic biometric management strategies in place. For this reason, to enable effective digital investigations on multiple captured physiological and behavioural characteristics, this paper aims at proposing a framework that is meant to facilitate the integration of DF and multimodal biometrics. The framework is also meant to enhance the analysis of potential digital evidence during investigations. Integrating multimodal biometrics and digital forensics using the proposed framework gives a promising approach to add value especially in enforcing security measures in different systems as well as a restricting factor to unauthorized access key discoveries. The integration of digital forensics with multimodal biometrics is the main focus of this paper.

KEYWORDS

Digital forensics; framework; multimodal biometrics; biometric indicators; security; digital evidence

1. INTRODUCTION

In detecting the identity of a human, it is evident that every individual demands to know exactly whether the party is who is being claimed to be. Vijay and Jadhav [21] describe biometrics as the morphological, physiological or behavioural characteristics of a person used to authenticate the identity. Multimodal biometrics usually combines more than one way of recognition. Therefore, different features that come from behavioural aspects can be linked with different aspects of digital forensics for proper matching. Based on these methods Kant and Nath [5] extrapolates that features of different fingerprints may exhibit different characteristics.

For example, trying a face match with a face that has scars can yield different result, given that, the hierarchy of multimodal biometrics have strong features that require evidence regarding the original match and the procedure followed hence the need for different computerized forensics structures to be highlighted [11]. Besides, each intrinsic approach used needs to have a pattern towards digital forensics process. Yasinsac, Erbacher, Marks and Pollit [17] suggested the use of either two models a top down or bottom up model through which every classified multimodal model must be digitized towards digital forensics for open matching and recognition.

Multimodal biometric systems are gaining more attentions lately because they are able to overcome limitations in unimodal biometric systems. In this paper, therefore, a new approach for integrating multimodal biometrics with digital forensics has been proposed to enhance the digital forensic investigation of multimodal biometric systems. The experimental results show that the proposed framework can be used for applications that use multimodal biometrics security for identification purposes.

As for the remaining part of this paper, section 2 presents background and motivation concepts while section 3 elaborates on some previous related work. A detailed explanation of the proposed framework is handled in section 4 followed by a hypothetical scenario in section 5. Section 6 discusses the evaluation of the proposed concept. Finally, conclusion and future work is given in section 7.

2. BACKGROUND AND MOTIVATION

According to Besbes, Trichili and Solaiman [20] biometrics is unique and unchanged, or acceptably changed, over an individual's life time and is deemed to be one of the best access control solutions. By authenticating individual's behavioural or biological characteristics instead of tokens and passwords or Personal Identification Number (PIN), biometrics recognition can offer high levels of identity authentication than knowledge and token based counterparts [16].

The PIN is a numeric password shared between a user and a system, which can be used to authenticate the user to the system. The user is sometimes required to provide a non-confidential user identifier (ID) or token and a confidential PIN to gain access to the system. The system then looks up the PIN based on the user ID and compares the available PINs with the received PIN. The user is granted access only when the number entered matches with the number stored in the system. However, despite the name, a PIN does not at times personally identify the user.

According to Revett, [19] biometrics can be classified into three different categories as follows:

a) Physical biometrics
b) Biological biometrics
c) Soft biometrics.

Physical biometrics is static and hence it does not change. It includes fingerprint, face, iris, retina among others. Biological biometrics on the other hand is dynamic and can change. It includes signature, keystroke, handwriting and gait. Soft biometrics refers to human characteristics and may include height, weight and colour of hair.

Biometrics system based on single source of information is called Unimodal biometrics system. Multimodal biometrics, on the other hand, integrates two or more biometric features. This integration of two biometric features can enhance security as well as meets user satisfaction as portrayed by Akilan, Gunasekaran and Saravanan [1].

According to a research by Waheeda [22] Multimodal biometric system can operate in three different modes. These Modes are briefly explained as follows:

- **Serial Mode** – This mode checks each modality before the next modality is investigated. It is also known as cascade mode.
- **Parallel Mode** – This mode combines all the information modalities that are processed together to perform recognition.
- **Hierarchical Mode** – This mode forms a tree like structure for the combination of individual classifiers.

It is also important to note that according to Akilan, Ginasekaran and Saravanan [1] multimodal biometrics is designed to operate in the following scenarios:

- **Multiple Sensors** – This scenario combines different biometric information of a single user from different sensors.
- **Multiple Biometric**– This scenario is used where different biometric characteristics of a single user obtained from different sensors can be combined.
- **Multiple Units of the Same Biometric** – This scenario is used where, for example, the Iris from left and right side of the eyes of a single person may be combined.
- **Multiple Snapshots of the Same Biometric** – This scenario is used where multiple snapshots of the same instance collected are combined for recognition and enrolment.
- **Multiple Representations and Matching Algorithms for the Same Biometrics** - This scenario combines various approaches to feature extraction and matching of the multi biometrics.

The next section discusses the related work in this research paper.

3. RELATED WORK

Generally, biometrics relies on a single source of evidence to proof that a particular task has been accomplished. Besides, a normal generic biometric system should have data, sensors, matching template, data transmission and a decision [12][13][15]. A series of well documented research has shown that multimodal biometric and digital forensics is still far apart. However, Ross & Jain have described fusion scenarios that depend on traits, sensors and feature sets in a multimodal biometric system [12]. The levels of fusion in this study highlight multiple matchers of face and fingerprints, snapshots, optical and capacitance sensors, right fingers and middle fingers. In their study, the authors were able to come up with a conclusion that multimodal biometrics increases as well as improves matching performance, deters spoofing and facilitates indexing.

Different Digital Forensic (DF) process models have been proposed by a number of researchers that can help in investigative processes although they have not been fully standardized. Pollit proposed a model with the following components policies and practices, examination and procedures [18]. Nevertheless Kohn, Eloff and Olivier [9] proposed a framework for digital investigation that had preparation, investigation and presentation phases. Notwithstanding that, Beebe and Clark [2] in there paper also proposed a hierarchical, objective-based on forensic investigation process model.

Discounting that, a number of relevant works on digital forensic readiness have also been proposed as related works. Valjarevic and Venter proposed a Harmonized Digital Forensic Investigation Process Model (HDFIPM) which had incident detection, planning, first response phase, preparation and evidence collection phase [14]. Another research by Kebande and Venter has proposed a cloud forensic readiness model that had the following phases, collection, hashing and preservation and finally a framework for enhancing potential digital evidence presentation that will determine if evidence is admissible with less efforts through evidence capturing and source identification was proposed by Karie and Venter [6-7].

Lastly, a multimodal biometric system that uses fingerprint, face and speech has been proposed by Jain, Hong and Kulkarni [4]. In their work, the authors have designed a multimodal system that is able to integrate face, fingerprint and speech to perform personal identification. Further, the choice of the above indicators was motivated by their routine use by the law enforcement community. Additionally, this study was done through verification of the aforementioned biometric indicators. In spite of this Kenneth [8] has proposed different subdivisions of behavioural biometrics with different characteristics that are focused on deployability, user acceptance, ease of use, and quality of identification. This author presented the subdivision as voice recognition, signature verification, keystroke dynamics, graphical authentication system. However, digital forensics was hardly mentioned in this study.

The section highlighted other researchers work that is somewhat represented as related work in our research, in the next section, we discuss the proposed framework.

4. PROPOSED FRAMEWORK

In this section, we present the self-adaptive framework as a contribution to integrating digital forensics with multimodal biometrics and how the framework works. The goal of the framework is to enhance a high level of security through integrating proactive and reactive processes through multimodal biometrics. The framework consists of subdivisions that are used to portray various methods of integrating multimodal biometrics and digital forensics.

The framework is organized into two structures. Figure 1 represents the high-level view of the framework while figure 2 represents the detailed framework; figure 3 represents the respective sequence flows of events for the framework. Figure 4 on the other hand represents a hypothetical scenario.

4.1 High-level view of the framework

The high level view of the framework is organized into four layers as shown in figure 1. The layers include: Biometric input and acquisition, biometric extraction, Digital Forensic Readiness (DFR) and Digital Forensic Investigation (DFI). Each of the highlighted components has been explained in brief below.

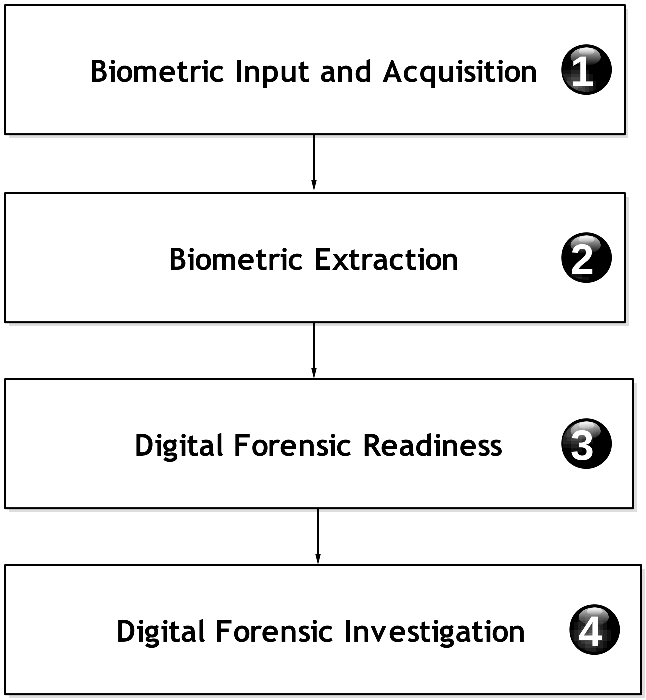

Biometric Input and Acquisition
1
Biometric Extraction
2
Digital Forensic Readiness
3
Digital Forensic Investigation
4

Figure1. High-level view of the framework

A high-level view of the framework is shown in Figure 4. Multiple biometrics ranging from multiple sources are acquired to help establish identity in layer l as input. Pieces of evidence are generated from this section. These inputs are represented as user specific parameters. Next is biometric extraction in layer 2 which allows matching and making decisions whether the acquired pieces of digital data correlates with the original biometric. Digital forensic readiness in layer 3 allows the environment to be forensically ready through the digital content stored in the databases. Finally, digital forensic investigation follows in layer 4 which employs the actual scientific methods of investigations. More details shown in Figure 1 are explained in the detailed framework represented as Figure 2 however, Figure 3 gives procedural flows for the high-level framework.

4.2 Detailed Framework

This section gives a discussion about the detailed framework, which is divided into four distinct parts as shown in Figure 2. The biometric extraction and acquisition part which comprises of biometric multimodal indicators. The framework has been represented with image fingerprint, voice, hand geometry, facial recognition, iris and DNA. Biometric extraction consists of indicator matching and decision module. This has been shown in the section labelled 2 of Figure 2, followed by the Digital Forensic Readiness (DFR) layer. The DFR section consists of the biometric database, agent and potential digital evidence collection. This has been shown in the section labelled 3. The last part of the framework is the digital investigation layer which consists of initialization process, acquisitive process and investigative process labelled as 4 in Figure 2. The framework is explained in more details in the sections to follow.

4.2.1. Multimodal Biometric input and Acquisition

This layer operates either in serial or parallel mode. It is tasked with taking in multiple modalities. In this context, the multiple indicators may undergo multiple matching for identification. This is shown in the part labelled 1 of Figure 2. The process of multimodal input may include; face and fingerprint, right index finger and thumb, attempting index finger twice, using multiple sensors example; optical and capacitance or using double matchers, but it solely depends on the number of traits, features and sensors. Lu, Wang, and Jain [10], describes these techniques as extraction of different features from a subject and integrating the output of the corresponding classifiers to the match level. The following indicators have been used in the framework as inputs but are not limited to any other biometric indicators; image, fingerprint voice, hand, geometry, facial, recognition, iris recognition and DNA.

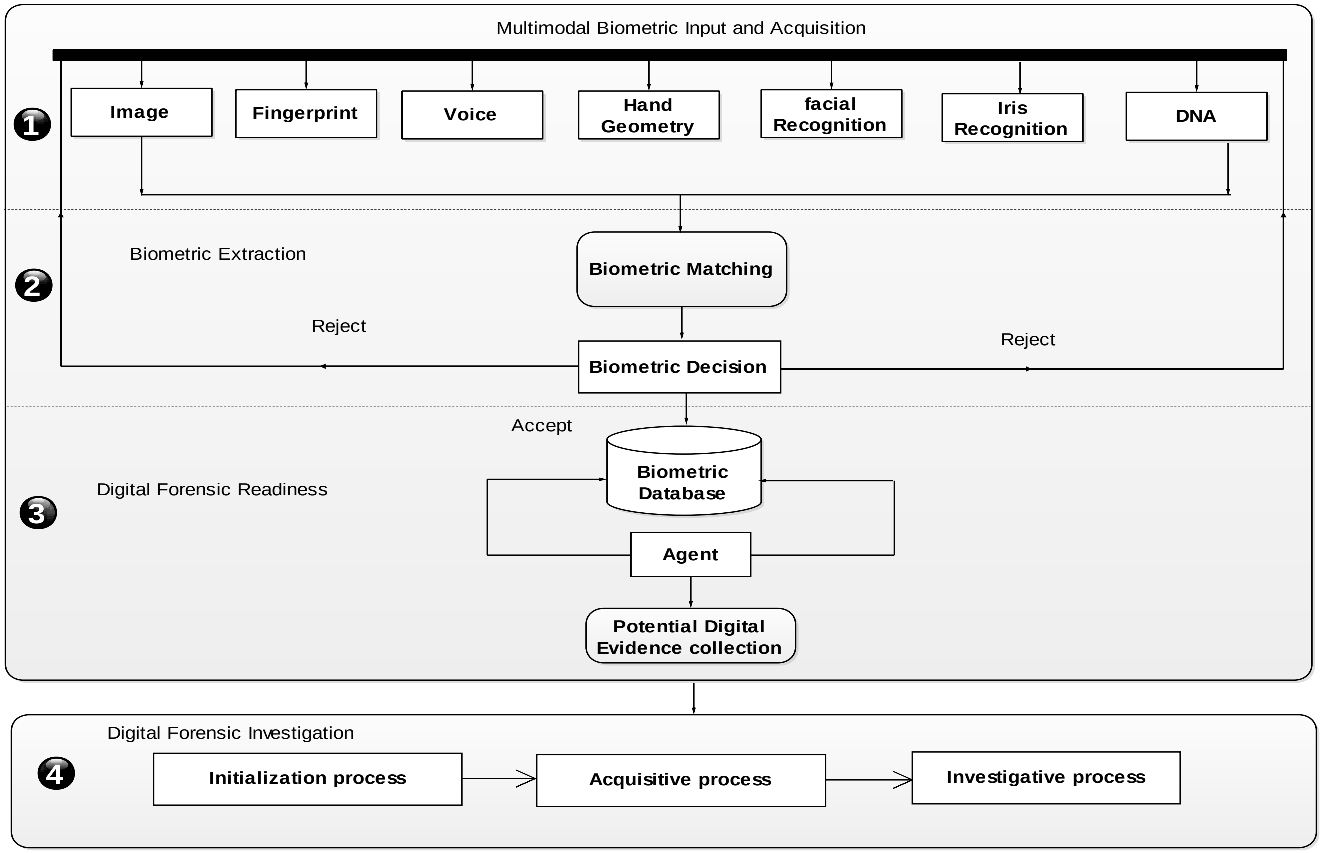


Figure 2: A Framework for Integrating Multimodal Biometric and Digital Forensics

4.2.2. Biometric Extraction

Extraction as shown in the section labelled 2 includes matching information from different modalities for possible processing. This is expected to yield an exact representation of the traits that are taken in as inputs. If the traits happen to be exact, they are then forwarded to the biometric decision which gives an accept or reject status as shown in the framework in Figure 2. If an accept status is given then the digital information proceeds to the biometric database otherwise control is redirected to the biometric input.

4.2.3. Digital Forensic Readiness

This is a proactive process that includes getting forensic preparedness for security incidents arising from biometrically digital data moving to the biometric database as shown in the section labelled 3 in Figure 2. In this section digital information that can be used as admissible digital evidence in a court of law is captured using an agent as it moves to the database. The agent is a key component that is used to access resources and collect digital evidence in a forensic readiness manner. Evidence collected by the agent is hashed and stored in a database which will then be used as potential digital evidence if a security incident is detected.

The process happens before an incident is identified. This allows the environment to be ready for security incidents. This is done in accordance with the readiness guidelines that have been proposed in the standard if ISO/IEC 27043: 2015 [3]. This standard presents guidelines that cover incident investigation principles and security techniques. By encapsulating these guidelines the effort required to perform a digital forensic investigation process is reduced.

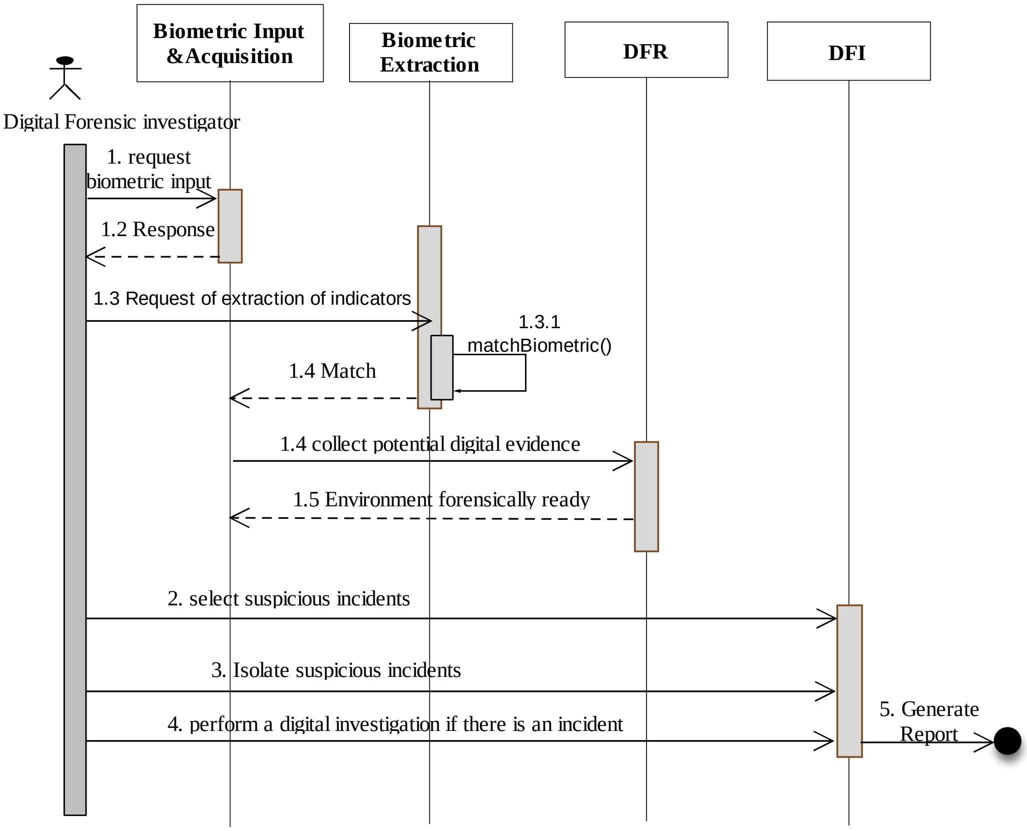

Biometric Input &Acquisition
Biometric Extraction
DFR
DFI
Digital Forensic investigator
1. request biometric input
1.2 Response
1.3 Request of extraction of indicators
1.3.1 matchBiometric()
1.4 Match
1.4 collect potential digital evidence
1.5 Environment forensically ready
2. select suspicious incidents
3. Isolate suspicious incidents
4. perform a digital investigation if there is an incident
5. Generate Report

Figure 3: Procedural Flows for the Framework

4.2.4. Digital Forensic Investigation

This is a reactive process dealing with the scientific process of digital investigation. It is divided into three parts as shown in figure 2, initialization, acquisitive and investigative process. According to ISO/IEC 27043, initialization process deals with starting the digital investigation process and handling first response of the incident. Acquisitive processes are concerned with acquisition of potential digital evidence and processes involved. On the hand, investigative process is the actual incident investigative process, evidence analysis, interpretation and forensic reporting, presentation and investigation closure.

4.3. Procedural flows of the framework

Figure 3 shows a sequence diagram of procedures within the framework as each of the procedure described above has been represented. Firstly, the digital forensic investigator, requests for biometric input and acquisition in step 1 of Figure 3.When a response is given back in Step 1.2, extraction of the indicators follows. This include checking the multimodal inputs for traits, sensors and feature sets, classifiers and performing identity matching in step 1.3.1. Depending on the match from the decision the process will be repeated or forwarded to the biometric database. In step 1.4 the agent previously described in Figure 2 collects potential digital evidence to be used for digital forensic readiness purposes. When potential digital evidence exists, the DFI has three options when a security incident is detected. These include; selecting suspicious incidents, isolating suspicious incidents and performing the DFI process in step 2, 3 and 4 respectively. Finally, a report is generated in step 5.

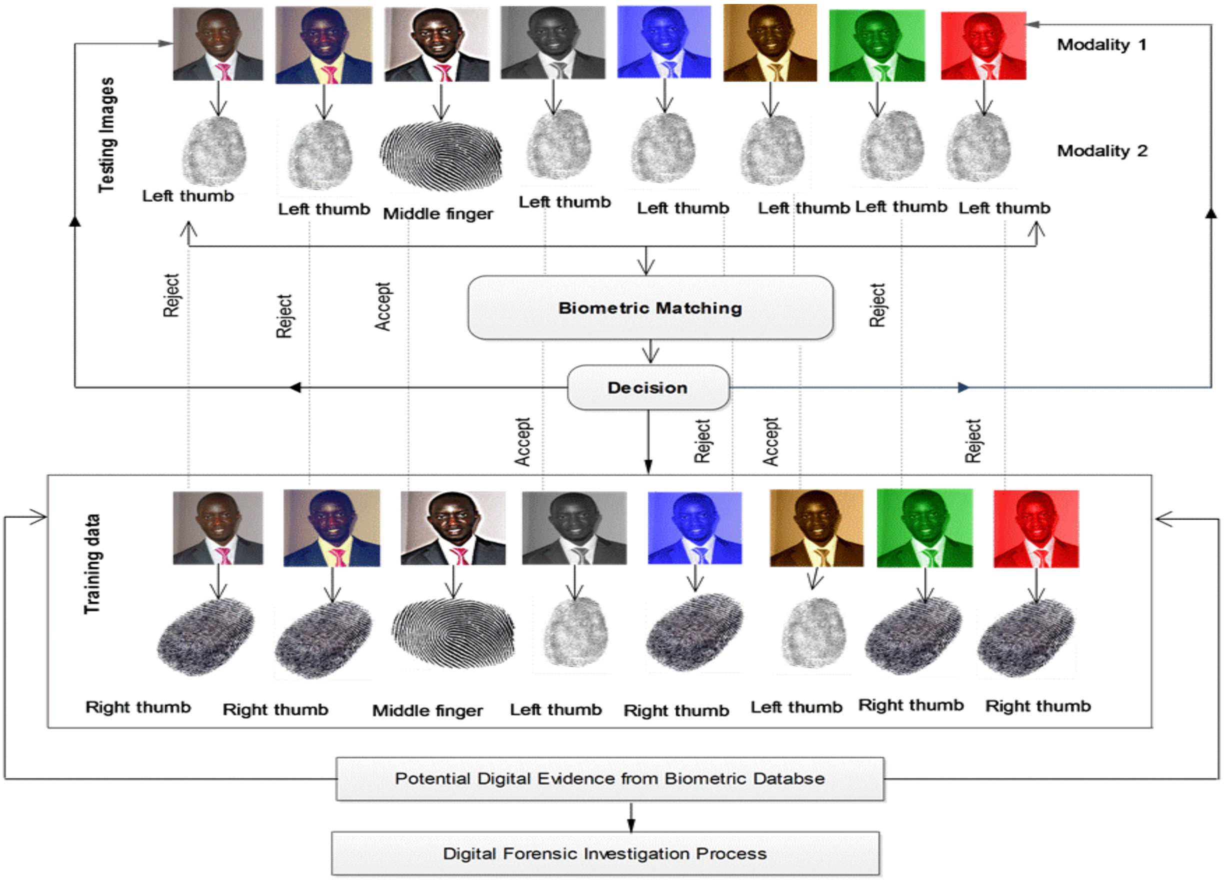


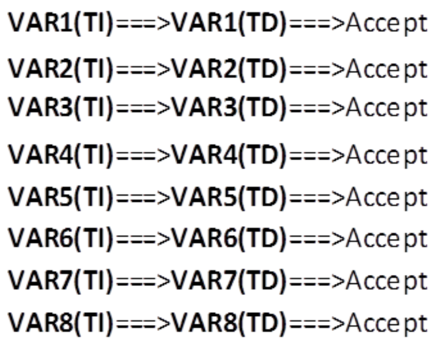
Figure 4: Scenario

5. HYPOTHETICAL SCENARIO

In this section, we present a multiple biometric trait that identifies a combination of two modalities [face and finger prints] as a hypothetical scenario. The pixel intensity of the face in the training set and the testing images is the same but significantly different from the 8 variants due to the pose and the lighting. The variants can be seen in Figure 4. From the given modalities, the training set holds different face variants while it holds the following finger print variants; Right thumb, middle finger and left thumb. In this scenario, the task is to use the classifiers to match the multimodal inputs and to pick the digital data and the status as potential evidence for possible digital forensic investigation.

6. EVALUATION OF HYPOTHETICAL SCENARIO

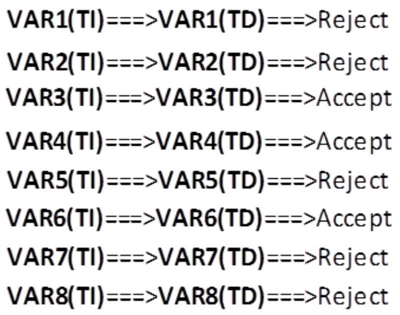
From the scenario given in Figure 4, a digital forensic investigation begins with the availability of potential digital evidence (PDE). In this context PDE exists as biometric digital data represented as face and finger print. In step 1 of biometric matching, each individual test image is classified with an accept status because the 8 variants matches with the training data but the finger print test image and training data produces different outputs. This has been represented as Test Image (TI), Test Data (TD), Variant (VAR) and Status (Accept/Reject) shown below.



VAR1(TI)===>VAR1(TD)===>Accept
VAR2(TI)===>VAR2(TD)===>Accept
VAR3(TI)===>VAR3(TD)===>Accept
VAR4(TI)===>VAR4(TD)===>Accept
VAR5(TI)===>VAR5(TD)===>Accept
VAR6(TI)===>VAR6(TD)===>Accept
VAR7(TI)===>VAR7(TD)===>Accept
VAR8(TI)===>VAR8(TD)===>Accept

(1)

The equation highlights a biometric match between the TI for the face image and the TD for the face image from variant 1 to variant 8.We also represented the TI for the finger print and the TD as shown below.



VAR1(TI)===>VAR1(TD)===>Reject
VAR2(TI)===>VAR2(TD)===>Reject
VAR3(TI)===>VAR3(TD)===>Accept
VAR4(TI)===>VAR4(TD)===>Accept
VAR5(TI)===>VAR5(TD)===>Reject
VAR6(TI)===>VAR6(TD)===>Accept
VAR7(TI)===>VAR7(TD)===>Reject
VAR8(TI)===>VAR8(TD)===>Reject

(2)

Based on equations (1) and (2), it is evident that the aspect of gathering sufficient potential evidence in multimodal biometrics highly depends on the choice and the number of biometric traits. Nevertheless for proper identity management and identification the level through which information is provided by multiple traits should be integrated for proper correlation. Additionally the modalities presented in Figure 4 do not need to be acquired in a simultaneous manner but they have a relationship. In the next section we give a critical evaluation of the proposed framework. The variants have also been represented in Table 1 and Table 2 shown below.

Table 1.Performance of the modality of face variant

No	TI [Face]	TD [Face]	Decision Status
1	VAR(1)	VAR(1)	Accept
2	VAR(2)	VAR(2)	Accept
3	VAR(3)	VAR(3)	Accept
4	VAR(4)	VAR(4)	Accept
5	VAR(5)	VAR(5)	Accept
6	VAR(6)	VAR(6)	Accept
7	VAR(7)	VAR(7)	Accept
8	VAR(8)	VAR(8)	Accept

Table 2. Performance of the modality of fingerprint variant

No	TI [Finger Print]	TD [Finger Print]	Decision Status
1	VAR(1)	VAR(1)	Reject
2	VAR(2)	VAR(2)	Reject
3	VAR(3)	VAR(3)	Accept
4	VAR(4)	VAR(4)	Accept
5	VAR(5)	VAR(5)	Reject
6	VAR(6)	VAR(6)	Accept
7	VAR(7)	VAR(7)	Reject
8	VAR(8)	VAR(8)	Reject

PERFORMANCE RESULTS

Based on the proposed framework and the scenario presented in Figure 3 and Figure 4, the two modalities have been evaluated based on a decision status of Accept and Reject through matching the 8 different training set of the modality 1(Face) and modality 2(Fingerprint) which has different pixel intensity, however, the 8 variants remains the same for the test data with face. Moreover, the variants for modality 2 (Finger print) with respect to the TD and TI differs

Table 1 and Table 2 have been drawn to show the performance of the matching threshold for modalities for the training set and the training images. The results portray the feasibility that exists between inherent biometric traits and how that aspect can be used to conduct digital forensic investigations through successful acquisition of biometrically stored digital images.

Integration of digital forensic processes in these modalities entails comprehensive application of scientifically proven methods to try to prove the occurrence of a digital event from the biometrically stored digital images through the process of digital forensic investigation.

7. CONCLUSION AND FUTURE WORK

We revisit the problem statement, which stated that there is lack of effective and standardised methods for performing digital investigation across multimodal biometric indicators. Nevertheless, there are also no proper digital forensic biometric management strategies in place.

This paper has proposed a framework for integrating multimodal biometric with digital forensics. Further, the framework has shown how biometric modalities can be used for digital forensic purposes through an approach of a hypothetical scenario. In the scenario, we examined how samples of the training data and test images are matched and integration of digital forensic processes.

For future work, we will include a functional prototype in the cloud environment for the aforementioned aspects for proper verification and validation.

8. REFERENCES

1. Akilan, P., Gunasekaran, K., Saravanan, D.: Design of Two Tier Security ATM System with Multimodal Biometrics By Means of Fuzzy Logic. International Journal of Innovative Research in Science, Engineering and Technology, Vol.3, Special Issue 1 pp. 1283-1288(2014).

2. Beebe, N. L., Clark, J. G.: A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147-167(2005).

3. ISO/IEC 27043: Information Technology-Security Techniques Incident Investigation Principles and Processes,[online], 2015 Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44407

4. Jain, A. K., Hong, L., Kulkarni, Y.: A multimodal biometric system using fingerprint, face and speech. In *Proceedings of 2nd Int'l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC* (pp. 182-187) (1999, March).

5. Kant, C., Nath, R.: Reducing Process-Time for Fingerprint Identification System, International Journals of Biometric and Bioinformatics, Vol. 3, Issue 1, pp.1-9(2009).

6. Karie, N. M., & Venter, H. S.: Towards a framework for enhancing potential digital evidence presentation. In *Information Security for South Africa, 2013* (pp. 1-8). IEEE(2013, August).

7. Kebande, V. R., & Venter, H. S.: A Cloud Forensic Readiness Model Using a Botnet as a Service. In *The International Conference on Digital Security and Forensics (DigitalSec2014)* (pp. 23-32) (2014). The Society of Digital Information and Wireless Communication.

8. Kenneth R.: Behavioral biometrics, A Remote Access Approach, © 2008 John Wiley & Sons, Ltd. ISBN: 978-0-470-51883-0

9. Köhn, M., Olivier, M. S., Eloff, J. H.: Framework for a Digital Forensic Investigation. In *ISSA* (pp. 1-7) (2006, July).

10. Lu, X., Wang, Y., Jain, A. K.: Combining classifiers for face recognition. In *Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on* (Vol. 3, pp. III-13). IEEE(2003, July).

11. Ricci S.C., Ieong.: Digital forensics investigation framework that incorporate legal issues. pp 29-362006.

12. Ross, A., Jain, A.: *Multimodal biometrics: An overview* (pp. 1221-1224) (2004). na.

13. Usharani, V., Saravanan, S.V., Multi Modal Biometrics Using Palmprint and Palmvein. Journal of Theoretical and Applied Information Technology, Vol. 67 No.1 pp. 177-185(2014).

14. Valjarevic, A., Venter, H. S.: Harmonised digital forensic investigation process model. In *Information Security for South Africa (ISSA), 2012* (pp. 1-10). IEEE(2012, August).

15. Waheeda Al-Mayyan.: Performance Analysis of Multimodal Biometric Fusion, Ph.d Thesis, De-Montfort University (2012).

16. Yang, Y., Lin, K., Han, F., Zhang, Z.: Dynamic weighting for effective fusion of fingerprint and finger vein. PICA: Progress in Intelligent Computing and Applications, 1(1), 50-61(2012).

17. Yasinsac., Erbacher, RF., Marks, D., Pollit, M.M"Computer forensics education". IEEE Security & Privacy (2003).

18. Pollitt, M. M. An ad hoc review of digital forensic models. In *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on* (pp. 43-54). IEEE (2007, April).

19. Revett, K. PhD: Behavioral biometrics, A Remote Access Approach, © 2008 John Wiley & Sons, Ltd. ISBN: 978-0-470-51883-0(2008).

20. Besbes, F., Trichili, H., & Solaiman, B.: Multimodal biometric system based on fingerprint identification and iris recognition. In *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on* (pp. 1-5). IEEE(2008, April)..

21. Vijay M, Jadhav D.: Review of Multimodal Biometrics: Applications, challenges and Research Areas. pp 90-95, 2010.

22. Waheeda A.: Performance Analysis of Multimodal Biometric Fusion, Ph.d Thesis, De-Montfort University(2012).