ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL

Volume 3 (Issue 1) (2019) Pages 28-39

Identity Management Based on Frontal Facial Recognition for Voters Register in Zambia

Lubasi Kakwete Musambo[1]
School of Engineering
Dept. of Electrical & Electronics Engineering
The University of Zambia
Lusaka, Zambia
[1]*e-mail: lubasimusambo@gmail.com*

Jackson Phiri[2]
School of Natural Sciences
Dept. of Computer Science
The University of Zambia
Lusaka, Zambia
[2]*e-mail: jackson.phiri@cs.unza.zm*

***Abstract*— biometric technology offers a great opportunity to identify individuals, authenticate individuals and separate individuals. Using these advantages, an election or voting model can be developed to perform elections for a country such as Zambia. Zambia currently uses a manual based voting or election model that heavily relies on paper presented documents that must be physically verified and or matched to existing prior collected information before an individual is allowed to participate in an election or a voting system. This paper proposes a frontal facial election based biometric model that can be used to rid the current election system of redundancy and introduce a paperless, accurate and efficient identification, authentication and voting process. A baseline study conducted shows that biometric authentication based on this proposed model improves a work related process such as a voting system. We start by introducing the elements that make a biometric model ideal, we then give an insight into the Zambian based election system and then we review various biometric technologies available and then finally introduce our biometric model.**

Keywords*— *identification, biometric, election, frontal-facial, authentication, model

I. INTRODUCTION

A Biometric is a measurement and statistical analysis of people's unique physical and behavioral characteristics. Biometrics can be collected from either a physiological characteristic or a behavioral characteristic [1]. The essence of biometrics is to accurately distinguish an individual by their inherent physical or behavioral feature. A physiological characteristic is a relatively stable human physical feature. An example of a physiological characteristic is a fingerprint, retina and iris pattern, or a hand-geometry pattern. Physiological measurements are static and non-alterable. This type of measurement is unchanging and irreversible or permanent apart for deformity caused by external significant duress such as ailment or physical injury [2] [3]. A behavioral characteristic on the other hand attempts to resemble a person's psychological makeup. This is affected by a person's build stature and gender among others. Behavioral characteristics can be identified in activities such as speech, hand-writing speed and pressure exerted on paper when writing among others [4]. Four methods of biometric authentication systems were reviewed employing both physiological and behavioral characteristics. These have been reviewed in terms of basic operation, advantage and disadvantage of implementation.

Developments in biometrics entail that within-person variation factors have been taken into account at development as incoherencies can be determined with a level of accuracy by applying:

$$\cup ij = \frac{|a_i - a_j|}{r_{ij}} \quad (1)$$

where |ai−aj| is the magnitude of the vector difference between the two feature variations or drifts a_i and a_j while r_{ij} is the distance between the corresponding feature locations (the variation). The combined potential energy of the drift map characterized by *K* feature drifts is given by [5] :

$$C = \sum_{i=1}^{K} \sum_{j=i+1}^{K} U_{ij} \quad (2)$$

It therefore follows that *'the lower the potential energy C'*, then it is more likely that the images belong to the same person [6] [5].

This then ensures that a biometric feature has longevity of integrity as long as the subject is alive. This consistency of a biometric feature is tied to the fact that a biometric signal is constant in time save for exogenous circumstances like injury

or illness. To achieve biometric consistency, a match which uses a raw signal or fresh input (the biometric template or BT) must be collected from the signal directly at feature matching (the biometric signal or BS). Therefore the biometric, B governed is by BS, BT and B. It therefore follows that a stable biometric signal is a function of [6]:

$$[\![BT]\!]\_s = f(B) \quad (3)$$

II. Understanding Voting systems in Zambia

Applying a secure biometric infrastructure is key in ensuring that organisational or private data is well managed and accessed only by the intended party. It is important that a possibility to authenticate only those individuals that are registered as voters in the Republic of Zambia exists [2] [4] [7].

Elections in the Republic of Zambia are held every 5 years [8] [9]. These elections are held so that the citizenry can elect or choose their preferred leaders. Leaders are categorized into:

a. President,
b. Member of Parliament,
c. Mayor,
d. Council Chairperson and
e. Councilor.

This allows for free choice on the part of the voter. This systems allows the voted for, to run government affairs on behalf of the citizens for a period of 5 years unless under exigency circumstances like death mental health sicknesses and others that may dwell on thieving among others [8].

This type of governance in Zambia was introduced circa 1990 and has been this way to date [10].

The current system of voting introduces issues of ethics and among them is an issue of Identity (ID) theft. ID theft is stealing one individual's personal details that are used to identify and authenticate that the bearer of the details is indeed who they purport to be. Reasons for this theft span from gaining advantage in various forms such as by use of another's identity for fraud purposes or simply to bar the owner of the identity from exercising certain activities such as access to certain facilities [11] [12]. ID theft may damage an individual's reputation [13] and breed war if not countered in events such as elections. A need to stop this activity arises.

The development of Information Systems (ISs) for government operations has enabled a better service delivery in certain sectors of the Zambian economy [14]. There is however a need to ensure that all other government institutions are introduced to e-governance. One such institution with a great impact on the greater Zambia is the ECZ (Electoral Commission of Zambia).

The ECZ is mandated to conduct National, Parliamentary, Mayoral, Councilor and Council Chairmen/Women for the Republic of Zambia. A by the way mandate is to hire the ECZ to conduct other elections such as the FAZ (Football Association of Zambia) or political party elections [9].

In all these election activities of the ECZ, one thing is paramount; a Zambian is involved directly as a participant in an election. Due to this, a need arises to ensure that:

a. An individual cannot vote twice in the same election for the same participant,
b. An individual must be eligible to participate in that election,
c. An individual cannot be represented in proxy,
d. No ghost individual must participate in an election and
e. An individual who participates once in an election cannot deny ever participating.

An element of ID theft is present in the 5 issues highlighted. To ensure the 5 issues above are addressed, it is recommended that frontal facial biometrics is introduced primarily as a tool to eliminate identity theft in voting.

It is the purpose of this research to focus attention on the subject of ID management in an attempt to eliminate ID theft in voting in Zambia.

This study focuses on the registration, storage and authentication of a voter who enrols to participate in elections in Zambia.

It is therefore envisioned in this paper that an optimal business process map for the election process must be premised on optimum authentication. The researchers hold the view that authentication is the fundamental element that yields integrity and defines the ethics in voting.

We, therefore, present our argument by first understanding various literature present in the area of biometrics and voting and then present the issues present in the current literature and finally present our considered view of a biometric identity model that is built on security features that do not compromise performance but still deliver in terms systems expectations.

III. Literature Review

In his paper citing Alexander Trechsel and Kristjan Vassil from their writing "Internet Voting in Estonia: A Comparative Analysis of Four Elections since 2005', European University Institute, 2010", [15] raises concerns about the security of a voter's detail if electronic mean are to be used to deliver an electronic vote [15]. The security question here borders around the concerns of whether Electronic systems can be attacked through various schemes such as denial of service, spoofing, viruses, and man-in-the-middle efforts.

This position held by [15] can be countered however by a having an encrypted authentication of a biometric nature for each voter. It is impossible to having matching biometric data in the form of hand geometry and fingerprint [16]. This feature of a biometric datum is enough to allay fears of ID theft. Secondly once a biometric datum is retrieved from an individual, cryptography

takes over and this guarantees that an encrypted datum is non-understandable even if it is stolen because it is in firm that a third party cannot understand [1]. Once captured it is the duty of ECZ to ensure a third party has no physical access to the system.

In the "Analysis of an Electronic Voting System" paper by [17] there is a fear raised about a possibility of a man in the middle attack which results into the theft of electronic data as it propagates [17]. Though this is a true possibility, a fully secured end-to-end encrypted system can be developed with a MAC (message authentication code). A MAC would counter the issues related to live data theft and subsequent tempering of the same by applying its image resistance properties [1].

[18] holds the view that in order for a voting system to be fair for political parties and voters; 7 elements must be present as follows:

a. **Authentication**: Only authorized voters should be able to vote;
b. **Uniqueness**: No voter should be able to vote more than once;
c. **Accuracy**: Voting systems should record the votes correctly;
d. **Integrity**: Number of casted vote must not be modified;
e. **Verifiability**: Possible to verify that votes are correctly counted in the final tally;
f. **Auditability**: Reliable and demonstrably authentic election records and
g. **Reliability**: Systems must have capability to function uncompromisingly, even when stressed by a number of unsuccessful operations.

In this work, [18] determines that authentication is a central element in elections and should that authentication for some reason have a problem and result into a failed authentication then a failed election may exist. [18] further states that a failed authentication may result into non acceptance of an elected government. It is our position that to counter [18] a biometric authentication can be used. Because most biometric systems use a single trait to perform the authentication as pointed out by [19], fusion method of a digital identity as defined by [2] , [4], [3] and [19]can be used to ensure the authentication utilises multiple biometric units that can counter single biometric entity use.

IV. Reviewing Biometric systems Currently in Use

1. Fingerprint Authentication: Fingerprints are made up of ridge patterns on a person's fingers. These ridge patterns have capacity to uniquely distinguish and identify individuals. Fingerprint features are made up of arches, loops, and whorls. An individual fingerprint will exhibit at least one of these major features. The minor details that are collected from these fingerprint features are referred to as minutiae. Figures 1 and 2 show a finger print sample and finger print features. The authentication processes is an automated method of verifying a match among different human fingerprints [20] .

Advantages:

i. Individualistic features guarantee authentication of subject [3].
ii. Systems are relatively inexpensive to purchase and install.
iii. Longevity of life of the fingerprint pattern's individualistic feature composition guarantees long term usage [3].
iv. Once in use a subject does not have to rely on memory for passwords as fingerprint authentication will guarantee access.
v. A fingerprint identity point cannot be spoofed [21].

Disadvantages:

i. Limitation of capture is reduced to an individual finger with further limitation of capture reduced to a section or part of that finger only and not the entire finger.
ii. Susceptible to FAR (false acceptance error) whereas a wrong subject is enrolled and allowed access.
iii. Hand injury (fingers included), chemical prone jobs and labour prone activities such as brick-laying or metal fabricating present a within-person variation that makes the reading and capture of finger prints difficult.
iv. Washing with a soap detergent or submerging a finger in water for period of time (approximately 30 minutes) works as a contraceptive to finger-print scanners and this may impede the scanners from capturing or enrolling the finger prints until the finger reverts to its original form it was in during capture or enrolment [1].

Figure 1: Fingerprint Image Sample

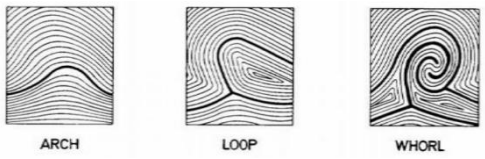


Figure 2. Fingerprint features [23]

2. *Retina Authentication:* This is one of the two forms of eye biometrics; the other being iris recognition. This form of biometrics is one of the most secure authentication systems in place today. The installed technology requires that an impression of a retina pattern must be taken and stored. The authentication process involves evaluating a subject's retina with a stored version (impression enrolled) of that subject's retina. Retina recognition has a low FAR (false acceptance error) as well as low rejection rates [22]. An image sample of an eye is shown in figure 3.

Advantages:

i. Different even in identical twins.

ii. Highly specific with unique structure shape and limits the possibility of fake retina presentation.

iii. Longevity of structure throughout life time of subject.

iv. Wearing of glasses or contact lenses does NOT work as a contraceptive to technological accuracy.

v. High accuracy and High recognition process speed.

Disadvantages:

i. Eye injury or sickness may render this biometric system ineffective.

ii. Intrusive technology and may not be welcomed by many individuals.

iii. Lighting may affect the accuracy of the reader.

iv. Fairly expansive to acquire when compared to other systems of biometrics.

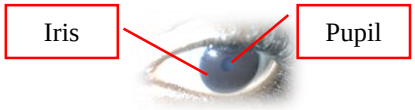


Figure 3. Eye Image Sample – for iris Recognition

3. *Voice Authentication:* This technology allows the conversion of voice or sounds from human voice into an electrical signal that can be coded. Voice recognition software is designed to identify an individual via their unique voiceprint. Voiceprints are generated from physical characteristics of an individual's throat in conjunction with their mouth. Research indicates that no two voices are the same and therefore voice biometrics provide a rare opportunity to use one's voice to authenticate or identify individuals [7]. A sample of a voice pattern is shown in figure 4 below.

Advantages:

i. No need for user training as users can simply speak into the voice biometric reader.

ii. Voice communications is a natural activity for human beings.

iii. Voice communications eliminates the need to learn keyboard operations (and in this way helps to bridge the gap between the able-bodied and individuals who experience restricted capabilities in hand based motion activities such as writing). By eliminating the learning aspect, voice overcomes the need to learn how to operate some complex biometric technology's operations.

iv. It eliminates the need to be accurate in written statements as is for password based authentication.

v. Because one uses voice, the speed of operation is enhanced. People generally speak faster than they are able to write.

Disadvantages:

i. Impulse noise may affect the accuracy of the voice signal and render the system ineffective.

ii. Microphone proximity must be precise for the system to work well.

iii. A pre-recorded audio may by-pass this system.

iv. A person may speak different languages and this may affect the accuracy of the device should that individual use a different language or dialect.

v. Certain words have a homonym characteristic, this may affect the accuracy of the device.

vi. The learning curve for the system may be long as it is trained per voice.

vii. Most voice controlled biometrics are expensive.

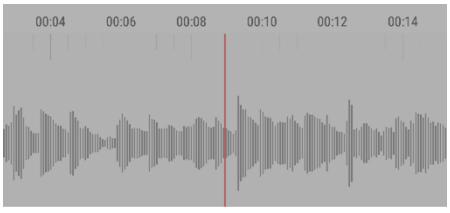


Figure 4. Voice Print. Adapted from [20]

2. *Face:* Facial biometrics divides into two aspects namely the face detection and face recognition programs. Face recognition extracts a face from a given image while face recognition compares a captured face against saved faces in order to match the face. The entire process is run by a series

of complex algorithms. One of the options of face recognition is to select features of a face and match those features to a face. Figure 5 below shows a facial image sample with facial image mapping that is used to collect facial features. The facial features or dataset is normally stored in a database. In ideal situations this database must be encrypted to achieve sufficient security [23].

Advantages:

i. Non-intrusive technology and can be performed stealthily without the subject knowing, therefore, proves ideal for investigation purposes.

ii. Certain algorithms can be adjusted to scan a large scale of a population and thus this technology proves ideal in crowded environments.

iii. Ideal for person tracking and incident reporting.

iv. User friendly as far as users are concerned as no need of complex training for the subjects to be captured.

v. Can be developed and run from a basic computer camera without buying any other tools. This proves to be one of the strongest advantage and reduces the cost of this technology exponentially.

vi. Some easy to install ready to use pre-trained facial calibration tools are available. This again reduces cost of setup.

vii. Facial biometric algorithms have a within-person variation calculation that can detect aging and basic facial deformity and reduce a face to a known variable [24].

Disadvantages:

i. Certain algorithms may NOT work well on black faces.

ii. Light conditions and camera capabilities may affect the accuracy of the technology.

iii. Within-person variations may affect the accuracy levels of the technology [25].

iv. When used for security purposes, extra equipment to provide lighting can increase cost of setup.

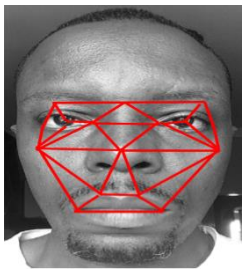


Figure 5. Facial Image Sample with facial map.

V. METHODOLOGY

The methodology is divided into 10 sections as follows:

(1) Baseline which address the process undertaken to determine the information requirements. (2) Descriptive research design which address aspects of research that are within the region of illustrative research concerning the research. (3) Target group which speaks to the identified target for this study. (4) The sample size and why it was taken. (5) The data collection tools which explains which tools were used in the study. (6) The data analysis which explains which analysis tool has been used. (7) The ethical consideration which explains the ethical position of the research. (8) The limitation of the baseline study which states how far the baseline study was stretched. (9) The presentation of the findings section to demonstrate our findings concerning our biometric model. (10) The system design detailing the technical aspects of the system.

A. Baseline Study

Baseline study was used in order to investigate the awareness levels and understanding of biometrics among individuals and organizations and to determine if a biometric standard that defines use and management of biometrics in Zambia is in use. Additionally, the use of the baseline study was to establish if organizations utilize biometrics for one function or another do so within a framework that is defined by government regulators of ICTs. The result of the baseline was used to develop the biometric software model. The model was validated to ensure it would fit into the use of conducting an election through frontal facial biometrics. As a result, the study used a mixed methods research methodology to analyze the data from the respondents.

The researchers hold the view that mixed methods research is the type of research which involves the use of more than one approach to or method of design, data collection or data analysis within a single program of study (e.g. both qualitative and quantitative research), is ideal as it integrates the different approaches or methods occurring during the program of study [26]. Mixed methods approach to research, helps researchers to incorporate methods of collecting or analyzing data from the

quantitative and qualitative research approaches in a single research study. Similarly, researchers can collect or analyze numerical data which refers to quantitative research coupled with narrative data which is the standard for qualitative research such that research question (s) are addressed as defined in any typical research study. Mixed methods designs also provide pragmatic advantages when exploring complex research questions.

Qualitative data was used to deepen understanding of survey responses while the statistical analysis was done to provide detailed assessment of patterns of responses.

B. Descriptive research design

Descriptive research is meant to provide a picture of a situation as it naturally happens. As such, it could be used to justify current practice and make judgment and also to develop theories. As a matter of fact, descriptive research [27]. A descriptive research design is used to explain the state of affairs at present. The researchers used it to obtain pictures of the current prevailing Election registration systems of registration in the Republic of Zambia.

C. Target group

The study was made up of eight types of target groups of the biometric authentication ecosystem comprising: ICT regulators, Standardization bodies, Consumer protection authorities, students in higher education institutions, banks, Government Ministries and departments, Health Support Institutions and general users. The mentioned respondents were sampled from the: University of Zambia (UNZA), Matem University, Bank of Zambia, Proflight, Stanbic Bank, Zambia Bureau of Standards (ZABS), Zambia Information Communication Technology Authority (ZICTA), Ministry of Home of Affairs (Passport Office and Citizen Registration Office), John Snow Initiative (JSi), Ministry of Commerce – National Technology Bureau, Ministry of Information and Broadcasting Services, Competition and Consumer Protection Commission (CCPC), Zambia Development Agency (ZDA) and the study area comprised Lusaka.
The significance of targeting the mentioned groups was meant to capture primary data from the mentioned area through purposive sampling. Purposively sampling signifies how the researcher sees sampling as a series of strategic choices about whom, where and how one does one's research.

D. Sample size

A total number of 100 respondents were randomly selected for interviews. The sample size was manageable and wide enough for valid generalization to the biometric ecosystem in Zambia.

E. Data collection tools & Systems Design

1) Self-administered questionnaires

The self-administered questionnaires were used to collect information from all the respondents. The use of questionnaires was not only simple to administer, but questionnaires were also relatively inexpensive to analyze. When alternative replies are provided in the questionnaires, respondents are able to understand the meaning of questions more clearly [26].

To validate the software, a validation question answered in tandem with software operations was done.

F. Data analysis

Data analysis for the study was done by computer based software known as Microsoft Excel. Microsoft Excel is a paid for computer program that is developed and maintained by the Microsoft Corporation [28].

G. Ethical consideration

Ethical clearance through authorization was awarded to the researchers by the institutions where the research was conducted from, by means of introductory letters which were given to authorities and respondents. Similarly, all questionnaires administered, did not allow respondents to disclose their names or any information that would review their status and ultimately compromise on confidentiality.

H. Limitation of the baseline study

The prototype is designed to enhance the Election registration processes in the Republic of Zambia and as such live tests can only be performed at the Ministry of Home Affairs and partly with the Ministry of Health. Getting permission for a live test with these institutions implies collecting citizen data. This was inhibitive. The other limitation was from some target groups like: commercial banks and some government offices that deal with citizen data who entirely refused to take part in the survey for fear of disclosing the data they collect to the general public.

I. Presentation of findings

The findings have been presented in the section labelled, "*Findings*".

J. System design

The system design is arranged into 4 sections including the system design as follows:

The first is explanation of the Haar Cascade algorithm, the second is the presentation of the Current business process in the Election voting process (which includes registration) and highlights the current problematic areas. The third is the proposed Election voting business process. The fourth presents the overall business process flow for the proposed model. The fifth section introduces the system interaction that a typical user

encounters when they interact with the system illustrated using UMLs' Use Case and Interactive Sequence Diagrams.

i. Understanding the Haar based Frontal Face Biometric Algorithm

Based on a rapid object detection scheme based on boosted cascade of simple feature classifiers introduced by Paul Viola and Michael Jones, a facial biometric model can be developed based on Haar-like features and implemented to detect and recognise a student's face. This recognition facility allows for authentication. Facial features to form a Haar classifier are collected after a facial mapping as shown in figure 8 above. The biometric model utilises Haar basis features as used by Papageorgiou et al [29].

An adaption of the algorithm based on an OpenCV Open Source technology which is readily available from OpenCV has been used. This algorithm uses Haar like features and OpenCV pre-trained classifiers for face detection. A classifier is a program that can decide whether an image is positive or not. A positive image is an image face (image having a face) while a negative image is a non-face image. Classifiers are trained from a huge volume of faces (both positive and negative images) to learn how to classify a new image correctly. This is a machine learning concept. The classifiers used for this student authentication is the HaarClassifier which is earlier developed by Viola et al [30]. Haar Classifiers process data in grey scale (non-colour). Colour is inconsequential in determining whether an image has a face or not.

ii. Haar Classifier function logic

Viola et al states each object has features that are unique and can be used to identify and recognize that object. Haar features can be picked out from edge, line, center and diagonal features of an object as shown in figure 6.

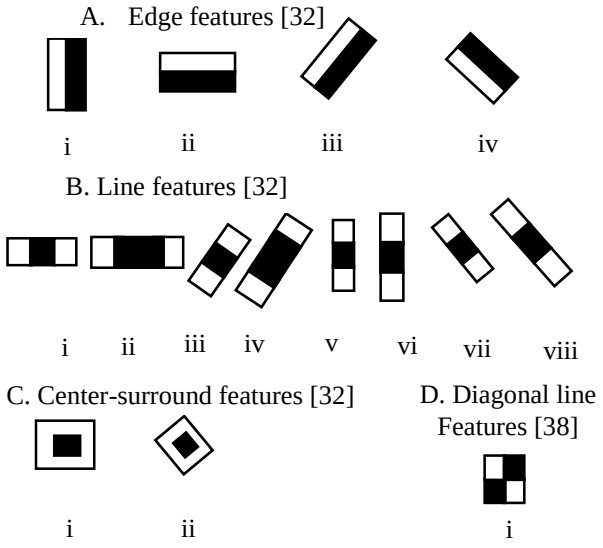


Figure 6. Example feature determination for extraction [31]

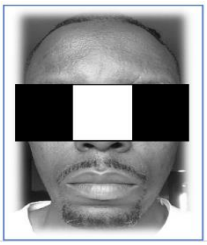


Figure 7. Feature Determination. Adapted from [39] [40]

Edge features are characteristics of an image that are unique and at unique distances from each other. No two people share the same features. The features can be mapped by placing an object identifying feature. A biometric model developed to pick up the readings from the facial recognizer can pick up the features and collectively store them to perform identification and recognition. The features can be collected into small elements referred to as a weak classifier which when collectively used identify and recognize an object [31]. Feature collection is done via rectangles. Haar like features consist of two or more rectangular regions enclosed in a template. Each of the rectangles is a window that is placed on an image as shown in figure 7 that is to be captured and recognized. A feature is extracted from subtracting the sum of pixels under the white part from the black part of that window (rectangle).

In determining the haar like features an understanding that the area around the eyes have a darker area then the nose bridge is used. This view is also held for the cheeks (brighter than other areas), though the data from the cheeks is not necessarily used.

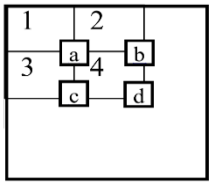


Figure 8. Rectangular regions of an integral image [38]

Rectangles are placed on an image so as to pick the features using a weak classifier. The features of a rectangle are computed using an integral function of the form:

$$ii(x, y) = \sum_{x' \le x, y' \le y} i(x', y'), \qquad (4)$$

In this function an object or image at location *x, y* contains the sum of pixels above and to the left of *x, y* inclusive.

Where *ii (x, y)* and *i (x, y)* is the original image. Using the following pair of recurrences:

$$s(x, y) = s(x, y - i) + i(x, y)$$

$$ii(x, y) = ii(x-i, y) + s(x, y)$$

(Where *s(x, y)* is the cumulative row sum, *s (x-a) = 0*, and *ii (-i, y) = 0)*. Using the integral image any rectangular sum can be computed in four array references [31] [32] [30].

The rectangle itself can be understood to have an object of pixels *W x H* (i.e.to say width x Height) [30]. Figure 8 below shows the determination of a rectangular region of an integral image.

To determine the sum of pixels, the logic can be deduced as follows:

$$a = sumRec(pixels) \quad (5)$$

$$b = 1 + 2,$$

$$c = 1 + 3$$

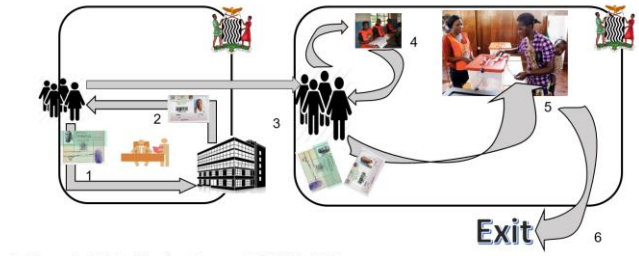
$$d = 1 + 2 + 3 + 4$$

The sum is then derived as $d + a - (b + c)$.

Using the OpenCV library of face detectors and recognizers a function can be developed into a web based biometric application that can perform an online web authentication during elections where an individual would be participating in a voting process.

iii. Business Processes

a. Current business process



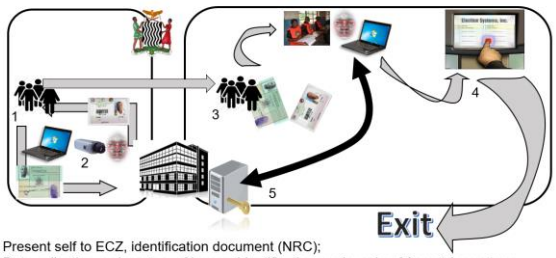
1. Present self, identification document (NRC) to ECZ;
2. Data collection and capture of human identification marks using ***anthropometric system,*** award of Voter ID card by ECZ;
3. Present self, identification documents, verification (accept or reject individual based on Bertillon measurements)
4. If accepted, allow vote

Figure 9. Current business process – Voting Process

A pseudo-code of the current business process is as follows:

START
Get individual
Present identification documents
Collect personal data using Bertillon system
WHILE individual available
Verify identification documents
Authenticate based on Bertillon measurement
IF Bertillon measurement = true
Then allow vote process
ELSE
Reject vote process
ENDIF
ENDWHILE

b. Proposed business process



1. Present self to ECZ, identification document (NRC);
2. Data collection and capture of human identification marks using ***biometric system***
3. Present self to ECZ & Poll Agents, identification documents, biometric authentication (accept or reject individual based on Biometric measurements)
4. If accepted, allow vote through electronic voting system
5. All data shall be saved on secure server at ECZ

Figure 10. Proposed Business process – Voting Process

A pseudo-code of the proposed business process is as follows:
START
Get individual
Present identification documents
Collect personal data using biometric system
WHILE individual available
Authenticate individual using biometrics
Authenticate individual using biometric measurement
IF biometric measurement = true
Then allow vote process
ELSE
Reject vote process
ENDIF
ENDWHILE

Figure 9 above shows the current business process for a voting process. The challenges in the current system can be identified as:

- Bertilloni systems are not accurate measure to identify people [33];
- Individuals may lose identification documents through theft and others;
- Slow process;
- Untrustworthy among the political players [34];
- Defaced documents may result into a reject of a vote process;
- The country has had a presence of duplicated identification documents [35].

To overcome the challenges identified above, a proposed business process as shown on figure 10 can be implemented.

The proposed model would have the following advantages:

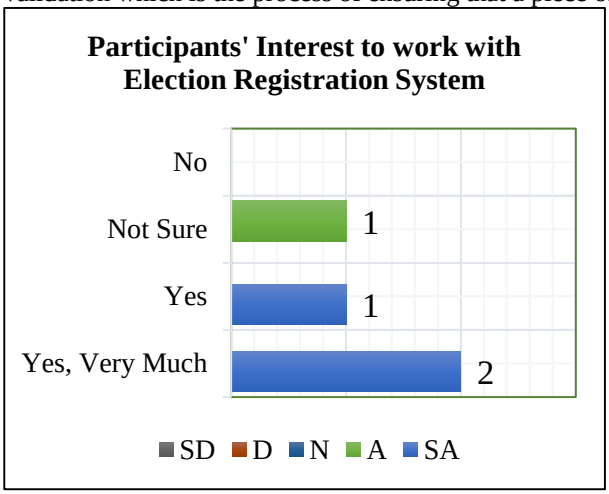
- A biometric is constant [6];
- An individual may lose identification documents or identification marks may be defaced but an individual can still be allowed to participate in a vote process;
- Lessens paper and
- May increase trust due to reduction in human to human interaction.

The methodology used for the analysis, design and development of the software system is the object-oriented systems development methodology (OOSDM) [36] [37]. This research study utilized some of the diagrammatic representations that are present in the unified modeling language (UML) in order to visualize the system from various perspectives [36].

The object-oriented system development (OOSD) approach that was used in the system development process is one that is use case driven. The object-oriented system development life cycle (OOSDLC) was used for the system development in this research study in order to show multiple iterations to be carried out throughout the entire development cycle for the system to be gradually built in small modular increments [37].

VI. Results

In order to ensure this software model we propose can function adequately and meet election or voting processes in Zambia, a validation which is the process of ensuring that a piece of



1) Election System's Ability to meet Job Function

Figure 14. Election System Validation – Participant's Desire to work with System

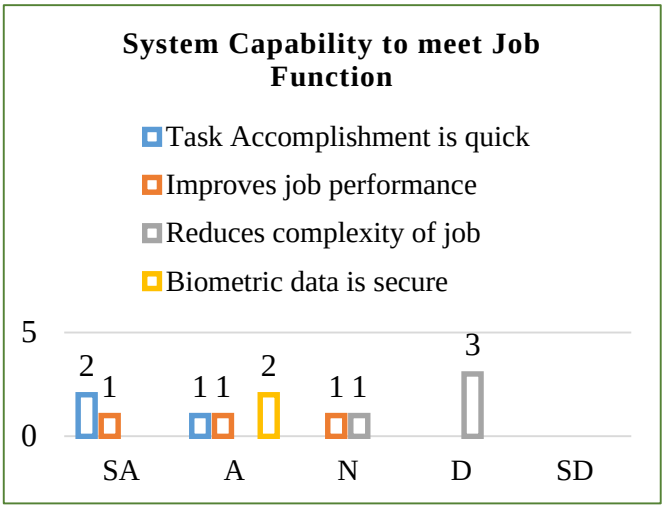
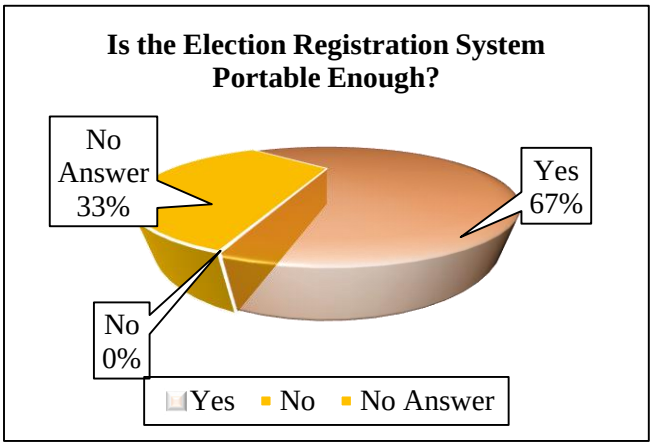


Figure 15. Election System Validation – System Capability to meet job function

The research validation participants were requested to comment on how they viewed the system's ability to meet job functions that a Election registration officer would undertake. Figure 15 above shows that out of the 6 research validation participants

2) System Portability

Given that the Election Registration system can only run if Python, OpenCV's Boost Cascade and Xampp control which are open source programs are installed; the research validation participants were asked to determine if the system was portable enough. Figure 16 below gives the responses to this question. As can be seen, 67% of the participants stated that the system was portable enough while 33% could not respond to the question and none of the participants stated that the system was not portable.



3) System Resources

Given that the Election Registration system requires systems resources of a computer with at least 4GB RAM, Hard disk capacity of at least 500GB and a web camera with a resolution of at least 0.9MP 16:9 (1280 x 720); the system validation research participants were asked to state whether these resources are too ambitious. Figure 17 below shows the responses and as can be seen 3 participants stated that the resources were not too ambitious, 2 participants could not respond to the question and 1 participant was not sure.

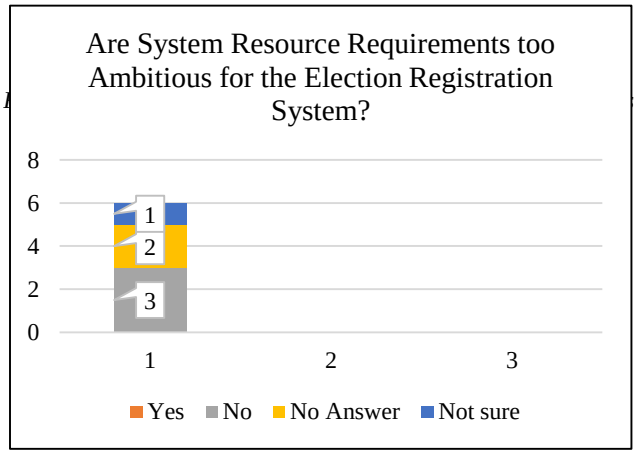


Figure 17. Election Registration System Validation – System Resource Requirements

Figure 18 below shows he UML interaction sequence diagram for the election system model. A citizen can be registered only once after that the recognizer would perform the authentication for every other function.

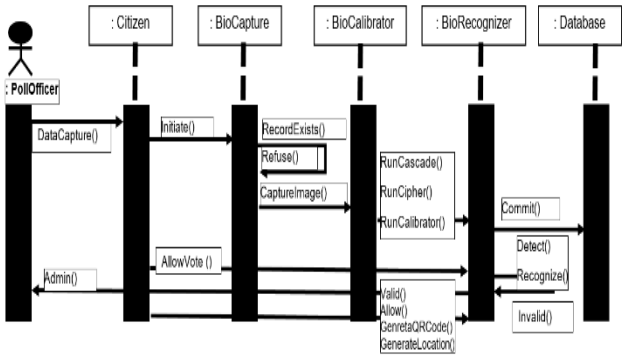


Figure 18. UML interaction sequence for Election Authentication.

The biometric authenticator described in the paper was implemented on authenticating individuals at different times of the day. This image set collected used 3000 image faces. The system achieves a person detection rate of 66% with a 33% false acceptance error.

VII. Discussions

The biometric model is able to yield a positive result of 66%, the false acceptance rate of 33% has been determined to be due to lighting conditions when the images are captured and the dark faces enrolled. Performance of the model has been observed to be higher or accurate when lighter faces are used. The researchers hold the view that that the darker regions around the eyes become fairly complex for the algorithm to determine on black faces. Improving lighting conditions has been observed to correct the recognition and detection process.

A web camera mounted on a laptop or computer is sufficient for this task. It must however be understood that sufficient research is needed into ensuring that false positives are dealt with as frontal face biometrics presents false positive errors. It is recommended that ISO 24745 is used to guide in the secure management and usage of biometric data.

VIII. Conclusion and Summary

In this paper, we give the results of the implementation for an election authentication system based on frontal facial biometrics. The Test results shows the proposed system was able to give up to 66% accuracy level. For a developing country like Zambia, this would be a good starting point. The frontal facial biometrics uses OpenCV's boost algorithms which are open source and readily available for adaptation.

In this paper, we began by a review of the various forms of biometrics that can be used in authentication systems. We then presented the general security challenges in elections especially for developing countries such as Zambia. One of the solutions to these challenges is the integration of biometrics features in the authentication systems. A cheaper solution for most developing countries is the use of open source tools and cheaper devices. Our study was proposing the use of OpenCV for Biometric Facial recognition and simple cheaper Web Camera such as one that comes integrated in most mobile computing devices.

IX. References

[1] K. Martin, Everyday Cryptography: Fundamental Principles & Applications, New York: Oxford University Press, 2012.

[2] I. J. Agbinya, N. Mastali, R. Islam and J. Phiri, "Design and Implementation of a Multimodal Digital Identity Management system using fingerprint matching and face recognition," *Broadband and Biomedical Communications (IB2Com)*, pp. 272-278, 21-24 Nov 2011.

[3] J. Phiri, T.-J. Zhao, H. C. Zhu and J. Mbale, "Using Artificial Intelligence Techniques to Implement a Multifactor Authentication System," *International Journal of*

Computational Intelligence Systems, vol. 4, no. 4, pp. 420-430, 2011.

[4] J. Phiri and J. I. Agbinya, "Modelling and Information Fusion in Digital Identity Management Systems," in *International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006.*, Morne, Mauritius, 2006.

[5] B. E. &. B. Sankur, "Effects of Aging over Facial Feature Analysis and Face Recognition," *Bogaziçi Un. Electronics Eng. Dept.*, pp. 1-4, 2010.

[6] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," *PROCEEDINGS OF THE IEEE*, vol. 91, no. 12, pp. 2021-2040, DECEMBER 2003.

[7] V. a. Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface," *International Journal of Computer Applications*, vol. 14, no. 5, pp. 1-6, 2011.

[8] GRZ, *The Constitution of Zambia*, GRZ, 2016.

[9] ECZ, "Elections," 12 February 2017. [Online]. Available: www.elections.org.zm/elections.php. [Accessed 12 February 2017].

[10] T. Kambilima, "History of elections in Zambia," *Zambia Daily Mail*, 2016..

[11] Sandi, "Identity Theft: When They Steal "You"," TechtTrends, 3 March 2014. [Online]. Available: www.techtrends.co.zm/identity-theft-steal/. [Accessed 25 November 2018].

[12] L. Times, "Zambian Pleads Guilty to Identity Fraud in the US," Lusaka Times, 27 July 2011. [Online]. Available: www.lusakatimes.com/2011/07/27/zambian-pleads-guilty-identity-theft. [Accessed 26 November 2018].

[13] A. G. Johansen, "4 Lasting Effects of Identity Theft," Symantec Corporation, 2018. [Online]. Available: www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html. [Accessed November 25 2018].

[14] ZPPA, "e-Procurement System," 12 February 2017. [Online]. Available: www.zppa.rg.zm/e-procurement-system. [Accessed 12 February 2017].

[15] T. Hall, "Internet Learning, Internet Voting: Using ICT in Estonia," *IPSA*, p. 31, 2012.

[16] M. Rose, "Biometrics," 21 February 2017. [Online]. Available: www.searchsecurity.techtarget.com/definition/biometrics. [Accessed 21 February 2017].

[17] A. S. A. D. R. S. W. TADAYOSHI KOHNO, "Analysis of an Electronic Voting System," *IEEE Symposium on Security and Privacy 2004*, p. 23, 2004.

[18] S. Yadav and A. K. Singh, "A Biometric Traits based Authentication System for Indian Voting System," *International Journal of Computer Applications*, vol. 65, no. 15, pp. 28-32, March 2013.

[19] D. Jagadiswary and D. Saraswady, "Biometric Authentication using Fused Multimodal Biometric," *Elsevier - International Conference on Computational Modeling and Security*, vol. 85, no. 2016, pp. 109-116, 2016.

[20] R. Saini and N. Rana, "COMPARISON OF VARIOUS BIOMETRIC METHODS," *International Journal of Advances in Science and Technology*, vol. Vol 2, no. I, pp. 1-7, 2014.

[21] N. Ferguson, B. Schneier and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Indianapolis: Wiley, 2010.

[22] J. M. Stewart, E. Tittel and M. Chapple, Certified Information System Security Professional, Canada: Wiley, 2008.

[23] F. Alonso-Fernandez, J. Fierrez and J. Ortega-Garcia, "Quality Measures in Biometric Systems," in *IEEE*, 2011.

[24] A. Lanitis, "Facial Biometric Templates and Aging:Problems and Challenges for ArtificialProblems and Challenges for Artificial," in *AIAI-2009 Workshops Proceedings*, 2014.

[25] E. Bilgin and B. Sankur, "Effects of Aging over Facial Feature Analysis and Face Recognition," *Bogaziçi Un. Electronics Eng. Dept.*, pp. 1-4, 2010.

[26] S. MacDonald and N. Headlam, Research Methods Handbook, Manchester: Th Centre for Local Economic Strategies.

[27] P. Pandey and M. M. Pandey, RESEARCH METHODOLOGY: TOOLS AND TECHNIQUES, Romania: BRIDGE CENTER, 2015.

[28] Microsoft, "Get a better picture of your data," Microsoft, 13 April 2018. [Online]. Available: https://products.office.com/en-us/excel. [Accessed 13 April 13].

[29] A. Mohan , C. Papageorgiou and T. Poggio, "Example Based Object detection.," *IEEE Transactions on pattern Analysis and Machine Intelligence*, vol. 23, no. 4, pp. 349-361, 2001.

[30] P. Viola and M. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," in *CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION 2001*, Cambridge, 2001.

[31] S.-K. Pavani, D. D. Delgado and A. F. Frangi, "Haar - like features with optimally weighted rectangles for rapid object detection," *Elsevier*, vol. 43, no. 160-172, pp. 160-172, 2010.

[32] R. Lienhart, A. Kuranov and V. Pisarevsky, "Empirical Analysis of Detection Cascades of Boosted Classifiers for Rapid Object Detection," *MRL Technical Report*, pp. 1-7, 2002.

[33] N. L. E. MUSEUM, "Bertillon System of Criminal Identification," NATIONAL LAW ENFORCEMENT MUSEUM, November 2011. [Online]. Available: http://www.nleomf.org/museum/news/newsletters/online-insider/november-2011/bertillon-system-criminal-identification.html. [Accessed 27 November 2018].

[34] M. Funga, "Voter apathy indictment on ECZ – HH," News Diggers, 27 July 2018. [Online]. Available: https://diggers.news/local/2018/07/27/voter-apathy-indictment-on-ecz-hh/. [Accessed 27 November 2018].

[35] H. Lumba, "Plug Loopholes in NRC Issuance," *Times of Zambia*, pp. 1-15, 2015.

[36] I. Jacobson, M. Christerson, P. Jonson and G. Overgaard, Object-Oriented Software Engineering: A Use Case Driven Approach, Patparganj: Pearson Education, 2004.

[37] D. Avison and G. Fitzgerald, Information Systems Development: Methodologies, Techniques & Tools, Maidenhead, Berkshire: McGraw-Hill Education, 2002.

[38] M. S. Uddin and A. Y. Akhi, "Horse Detection Using Haar Like Features," *International Journal ofComputer Theory and Engineering*, vol. 8, no. 5, pp. 1- 4, October 2016.

[39] D. Yadav, R. Singh, M. Vatsa and A. Noore , "Recognizing Age-Separated Face Images:Humans and Machines," *Pone*, 2014.

[40] R. Rezaei, . H. . Z. Nafchi and S. Morales, "Global Haar-Like Features:A New Extension of Classic Haar Featuresfor Efficient Face Detection in Noisy Images," *R. Klette, M. Rivera, and S. Satoh (Eds.)*, pp. 302-313, 2014.