Student Facial Authentication Model based on OpenCV's Object Detection Method and QR Code for Zambian Higher Institutions of Learning

Lubasi Kakwete Musambo
School of Engineering
Dept. of Electrical & Electronics Engineering
The University of Zambia
Lusaka, Zambia

Jackson Phiri
School of Natural Sciences
Dept. of Computer Science
The University of Zambia
Lusaka, Zambia

***Abstract*—Facial biometrics captures human facial physiological data, converts it into a data item variable so that this stored variable may be used to provide information security services, such as authentication, integrity management or identification that grants privileged access or control to the owner of that data variable. In this paper, we propose a model for student authentication based on facial biometrics. We recommend a secure model that can be used in the authentication and management of student information in the registration and access of resources, such as bursaries, student accommodation and library facilities at the University of Zambia. Since the model is based on biometrics, a baseline study was carried out to collect data from the general public, government entities, commercial banks, students, ICT regulators and schools on their understanding, use and acceptance of biometrics as an authentication tool. Factor analysis has been used to analyze the findings. The study establishes that performance expectancy, effort expectancy, social influence and user privacy are key determinants for application of a biometric multimode authentication. The study further demonstrates that education and work experience are regulating factors on acceptance and expectancy of a biometric authentication system. Based on these results, we then developed a biometric model that can be used to perform authentication for students in higher learning institutions in Zambia. The results of our proposed model show 66% acceptance rate using OpenCV.**

***Keywords*—Biometrics; authentication; model; integrity**

I. Introduction

Applying a secure biometric infrastructure is a key in ensuring that organisational and 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 students of a high institution exists [1]-[3]. This study focuses on the University of Zambia (UNZA), which is Zambia's biggest institution of higher learning. The findings can be generalised to cover the rest of Zambia's higher institutions of learning. The current authentication processes for UNZA are paper-based systems installed by the management of the university. Though these authentication processes which are prone to data redundancy are implemented; issues of over payment to ghost students on bursaries always arise, issues of illegal residents at the university arise from time to time, issues of non-availability of student records or non-available student records which were earlier created and filed with the office of Dean of Students arise. To overcome such problems generated by a lack of a secure student authentication system, we present a biometric model based on two-factor authentication that can be used.

II. Literature Review

A. Erroneous Payments

During a student registration process especially for the postgraduate level of studies at UNZA, a student is required to make payment at 4 different points; the Dean of Student office, the School of study, the Office of the Directorate of Research & Graduate Studies and the Library. In this process, students have been known to make erroneous payments to different pay points and correcting this error has been problematic for the student. Students have had to make extra payments in-order to meet the payment plan set by the University.

B. Squatting

The UNZA student handbook prescribes rules and regulations that a student must abide by. The rules indicate the number of students that can share a room for the purposes of being accommodated by the University. In 2018 first quarter, a student living conditions audit necessitated by an outbreak of cholera, a water-borne disease showed that more than 2 students shared a room. This trend referred to as squatting is an illegal activity. A lack of authentication (binding a student to a room) is the problem here as it appears difficult to determine which student is in which room.

Library Access: Access to the UNZA Library resources and access to an examination hall is guaranteed via a student ID card as shown in Fig. 1. No other form of authentication is available. It is possible that one may create a bogus ID card and gain access.

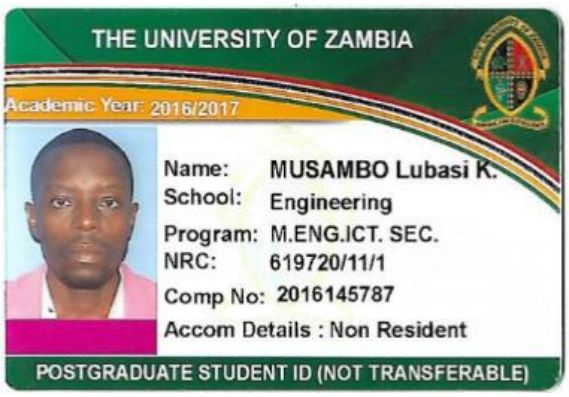

Fig. 1. UNZA Student ID.

C. Ghost Students

In Zambia, all government run instituions are audited annually by the Auditor General's office. The audits are conducted to determine usage of public funds. The audit concludes in what is called The Auditor General's Report. UNZA is a government instituion and as such is audited. The Auditor General's report for the period ended 2016 shows that the Zambian Ministry of Higher Education paid tuition and meal allowances to 543 individuals who were not registered by Zambia's two most prominent learning instituions; The University of Zambia and The Copperblt University (CBU). These funds are termed *'meal and project allowances'*. The report further states that over 8,000 UNZA students had been left out of these payments resulting into the students rioting. These funds are ment to secure accommodation, meal and project allowances for the students. The payments in question are within the region of K8,521,629 (or approximately $852,162.9). These are payments to ghost students. The reason this is possible is because a lack of authentication (entity binding exists). The Higher Eduation Loans and Scholarships Board Management is a Zambian government institution that manages student burseries on behalf of the Zambian government. The board has no mechanisms to authenticate student status due to a lack of unversity presence and reliance on paper based systems that are easily manipulated.

D. Loans and Bursaries

The Government of the Republic of Zambia awards loans and Educational bursaries to deserving students at Zambia's high institutions of learning. These bursaries are meant to ease the pressure of meeting school fees by a student. Payment of school fees is a requirement before one is admitted into school. Verification of who is entitled and who has been registered into this loan scheme is problematic as a clear authentication procedure is weak because it is paper-based. The current authentication solution is that the loans and bursaries board is forced to physically setup office at the institution of learning when learning institutions open. These temporal offices are used as screening facilities to screen and activate accounts of the students that have qualified for the bursaries. This is a labour intense and time consuming activity. A solution provides an automated authentication mechanism that can plug-into the student database system to perform the authentication when students register.

E. Student Registration

Registration at UNZA is a process of being enrolled into the school's student database system. Usually passport photos and physical copies of the student's credentials are needed for filing purposes. The credentials are authenticated by any third party referred to in Zambia as a commissioner of oath. The registration process can be enhanced if a centralised civil registration biometric database bound to an education database existed. This would authenticate a potential student's credentials to a higher institution of learning.

III. Summary of Reviewd Biometic Authentication Systems

Biometrics can be collected from either a physiological characteristic or a behavioral characteristic. A physiological characteristic is a relatively stable human physical feature. An example of a physiological characteristic is a fingerprint, retina 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 [4]. 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. 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.

A. 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. Fig. 2 and 3 show a finger print sample and finger print features. The authentication processes is an automated method of verifying a match among different human fingerprints [5].

1) Advantages

a) Individualistic features guarantee authentication of subject [4].

b) Systems are relatively inexpensive to purchase and install.

c) Longevity of life of the fingerprint pattern's individualistic feature composition guarantees long term usage [4].

d) Once in use a subject does not have to rely on memory for passwords as fingerprint authentication will guarantee access.

e) A fingerprint identity point cannot be spoofed [6].

Fig. 2. Fingerprint image sample [17].

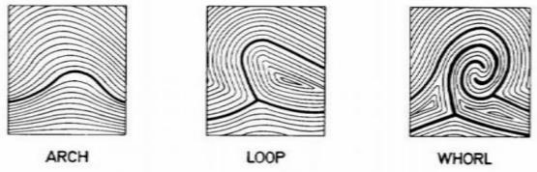

Fig. 3. Fingerprint features [9].

2) Disadvantages

a) 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.

b) Susceptible to FAR (false acceptance error) whereas a wrong subject is enrolled and access is allowed.

c) 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.

d) 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 [7].

B. 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 [8]. An image sample of an eye is shown in Fig. 4.

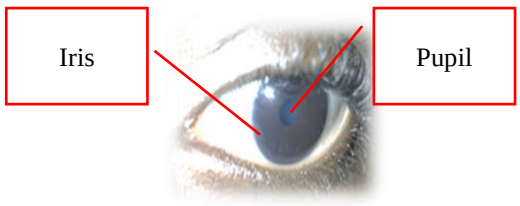

Fig. 4. Eye image sample – for iris Recognition.

1) Advantages

a) Different even in identical twins.

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

c) Longevity of structure throughout life time of subject.

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

e) High accuracy and High recognition process speed.

2) Disadvantages

a) Eye injury or sickness may render this biometric system ineffective.

b) Intrusive technology and may not be welcomed by many individuals.

c) Lighting may affect the accuracy of the reader.

d) Fairly expansive to acquire when compared to other systems of biometrics.

C. 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 provides a rare opportunity to use one's voice to authenticate or identify individuals [3]. A sample of a voice pattern is shown in Fig. 5 below.

1) Advantages

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

b) Voice communications is a natural activity for human beings.

c) 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.

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

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

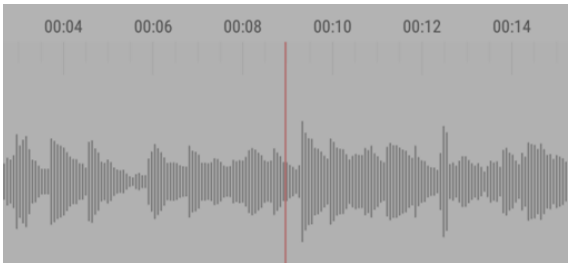

Fig. 5. Voice print. Adapted from [5].

2) Disadvantages

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

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

c) A pre-recorded audio may by-pass this system.

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

e) Certain words have a homonym characteristic this may affect the accuracy of the device.

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

g) Most voice controlled biometrics is expensive.

D. 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. Fig. 6 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 [9].

1) Advantages

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

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

c) Ideal for person tracking and incident reporting.

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

e) 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.

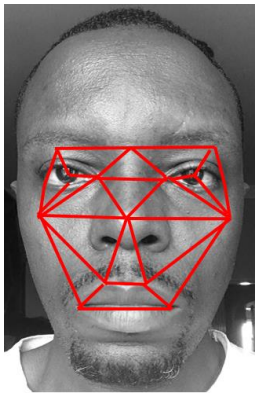

Fig. 6. Facial Image Sample with facial map for Facial Biometrics. Adapted from [5].

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

g) 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 [10].

2) Disadvantages

a) Certain algorithms may NOT work well on black faces.

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

c) Within-person variations may affect the accuracy levels of the technology [11].

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

IV. QR (Quick Response) Code

A typical QR code will have the shape as shown below:

Fig. 7. Sample QR Code [12].

As shown in Fig. 7 above, a QR code is a machine readable imprint made out of an array of black and white squares that normally embed certain information within the print. QR codes were developed by a Japanese company called Denso Wave for purposes of tracking manufacturing processes. QR codes however, provide an opportunity to authenticate as well as identify an entity. In this way QR codes may be used as an added security feature especially in logging into networks. Networks may be designed to read QR codes, verify the data and offer or deny access to an entity. Because QR Code information is non-human readable, this provides a basic form of information hiding in plain sight (encryption). This hidden information can then be transmitted. When used with geo-tagging, QR Codes can be used to determine a location status of an entity [12].

V. Student Authentication and Preferred Biometric Model

A. Problem Statement

Student authentication is equivalent to entity authentication. '*Entity authentication is the assurance that a given entity is involved and currently active in a communication session'.* A need to bind a student registered with a learning institution to a

current resource access of that institution exists [1]. There is need to grant student privileges such as accommodation, bursaries, allowances and loans to a deserving student automatically; a need to allow a student writes an exam without the need for unnecessary paper work is eminent; a need to ensure that a student's location status within UNZA facility exists. To achieve these functions, we recommend a facial biometric solution with a mobile QR Code reader.

B. *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 Fig. 8. The biometric model utilises Haar basis features as used by Papageorgiou et al. [13].

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. [14]. Haar Classifiers process data in grey scale (non-colour). Colour is inconsequential in determining whether an image has a face or not.

1) *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 Fig. 9.

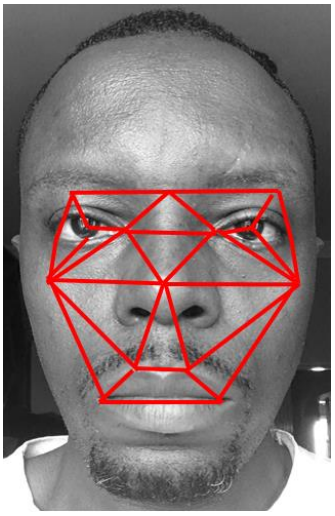

Fig. 8. Identifying features by a biometric reader. Adapted from [5].

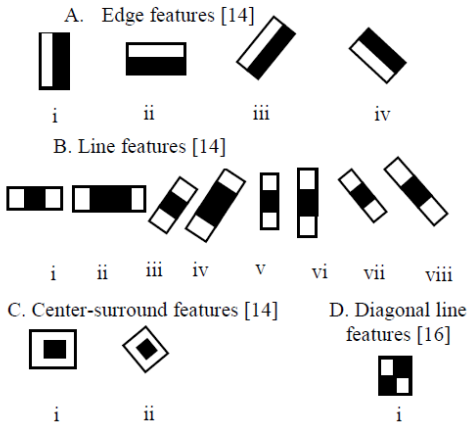

Fig. 9. Example feature determination for extraction [15].

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 [15]. 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 Fig. 10 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.

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:

$$ii(x,y) = \sum_{x' \le x, y' \le y} i(x',y'), \qquad (1)$$

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.

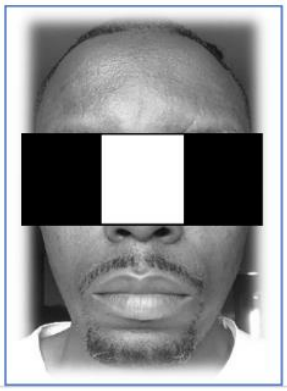

Fig. 10. Feature Determination. Adapted from [18] [20].

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 [14]-[16].

The rectangle itself can be understood to have an object of pixels *W x H* (i.e.to say width x Height) [14]. Fig. 11 shows the determination of a rectangular region of an integral image.

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

$$a = sumRec(pixels) \quad (2)$$

$$b = 1 + 2,$$

$$c = 1 + 3$$

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

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 application that can perform an online web authentication at UNZA where a student is interacting with the institution such as a library service. Between the web and the OpenCV recognisers a batch file mechanism as shown in Fig. 12 below can be incorporated to pass control to the OpenCV recognizers. OpenCv recognizers are developed in python [14]. A means of communication with a web application developed in a programming language python is achieved via the batch files as shown in Fig. 13 below. The algorithm has been set to capture 100 faces per student.

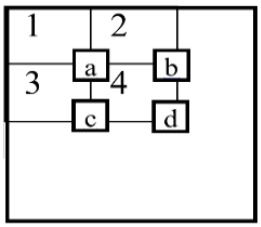

Fig. 11. Rectangular regions of an integral image [19].

```
face_datasets.py
pause
```

Fig. 12. Batch call function from PhP to python.

```
<title>VR|Registration </title>
<base />
<?php include_once 'userheadfiles.inc'; ?>
  <script type="text/javascript" src="js/qrcode_gen.js"></script>
<script type="text/javascript">
function myFunction(){
   WshShell = new ActiveXObject("Wscript.Shell"); //Create WScript Object
   WshShell.run("c://xampp/htdocs/fc/run.bat"); // Please change the path and file nam
execute .exe file as well
}
</script>
<script type="text/javascript">
```

Fig. 13. Batch call function from PhP to python to call for OpenCv face recognizer.

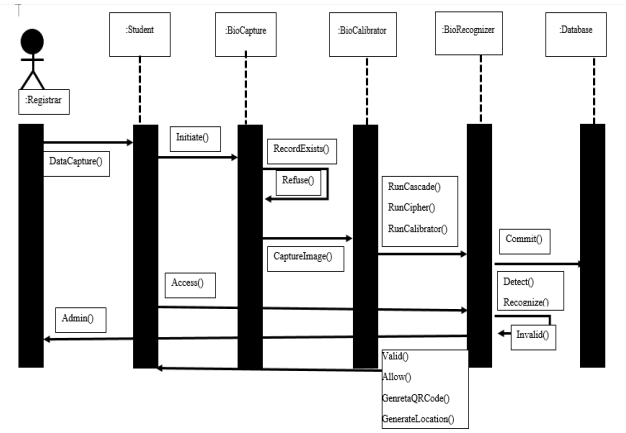

Fig. 14. UML interaction sequence for Student authentication.

A student can be registered only once after that the recognizer would perform the authentication for every other function. The interaction sequence for the student facial model is shown in Fig. 14 above.

VI. Model Test Results

The classifier described in the paper was implemented on authenticating students at different times of the day. This image set collected used 3000 student 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.

We believe that biometric and QR code authentication is the right approach to the management of student authentication. Frontal face biometrics appears easier to confront as it is not expensive to develop.

A web camera mounted in 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 also necessary to understand that trying a new technology requires ownership sense in the users and the subjects in question. An understanding of where a student's biometric data is kept is critical as most students interviewed showed little understanding of where their biometric data must be stored. This survey finding is shown in Fig. 15. It is then important that institutions of higher learning that will implement biometric technology explain to the students where their personal biometric data will be stored. It is recommended that ISO 24745 is used to guide higher institutions of learning in the secure management and usage of biometric data.

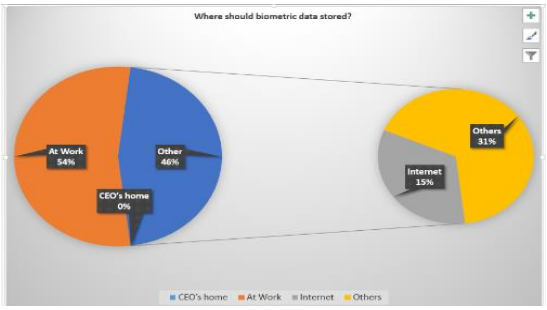

Fig. 15. Public understanding of where biometric data can be stored.

VIII. Conclusion

In this paper, we give the results of the implementation for a student authentication system based on our local university called UNZA. The results can however be generalized to cover other higher institutions of learning. The test results show the proposed system was able to give up to 66% accuracy level. For a developing country like Zambia with no form of automation in student's identification, this would be a good starting point.

Zambia currently does not have technological advancements that cover biometrics in detail let alone a biometric standard to determine suitable security that can be implemented in the use of biometrics. This paper recommends a frontal facial biometric model that can be used to perform authentication at various points within the university but can be generalized to any higher learning institution. The frontal facial biometrics uses OpenCV's boost algorithms which are open source and readily available for adaptation.

IX. Summary

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 developing countries especially higher institutions of learning. 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. For future works, we recommend a large dataset testing compromising of a majority of black people for a full proof authentication system based on facial biometrics is required.

References

[1] 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.

[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] 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.

[4] 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.

[5] 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.

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

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

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

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

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

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

[12] A. Mehta, "QR Code Recognition from Image," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 12, pp. 781-785, 2015 .

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, , J. Gonzalez-Rodriguez, H. Fronthaler,, K. Kollreider and J. Josef, "A Comparative Study of Fingerprint Image-Quality Estimation Methods," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 2, NO. 4, DECEMBER 2007, vol. 2, no. 4, pp. 734-743, 2007.

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

[19] 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.

[20] 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.