University of Ibadan
Journal of Science and Logics in ICT Research

An Enhanced Security Measure to Eradicate Examination Malpractice in Nigerian Universities: A Biometric Authentication Approach

Ndunagu, J. N.
jndunagu@noun.edu.ng

Computer Science Department, Faculty of Sciences,
National Open University of Nigeria

Abstract

Examination malpractice has eaten deep into the fabrics of Nigerian educational system to the extent that the credibility of certificates issued by the Universities is now in doubt. Impersonation as a type of examination malpractice is the core focus of this study where one claims to be another person. Impersonation is difficult to detect with mere traditional method of authentication. The objective of the study is to introduce Iris Recognition Technology (IRT) in addition to the traditional method already in use in the universities to identify candidates for examinations. Iris recognition as a method of biometric authentication is pattern-recognition technique based on high-resolution images of the irises of an individual's eye. Iris is the best in terms of accuracy and security enhancement among other types of Biometrics. The enrolment and verification are done within the database and consist of the following steps: (a) Photo Capture (b) Iris Image acquisition (c) Pupil detection and Iris localization (d) Iris Normalization (e) Feature extraction (f) Matching-Accept or reject. The integration of IRT will generate an effective means of student identification, weeding out impersonators who pose as examination candidates and further protect the integrity of the Nigerian Educational System.

Keywords: Iris recognition, Examination malpractice, Enrolment and verification, Data Security

I. INTRODUCTION

Nigeria has one hundred and fifty two (152) universities comprising 40 Federal, 44 State and 68 Private Universities. National Universities Commission (NUC) is responsible for regulating and accrediting Universities in Nigeria. Assessment is a major instrument used for the evaluation of learners' achievement and it is a *sine qua non* for determining goal attainment in Nigerian Universities. Examination which is one of the measures of assessment in Nigerian Universities is the pivotal point around which the whole system of education revolves and the success or failure of the system of examination is indeed the success or failure of the education system [1].

Assessment in Nigerian Universities has many merits, except for examination malpractice which is a violation of official examination rules and the effect places a candidate at unfair advantage [1]. Examination misconduct is regarded as a deceitful practice that can lead to harm and dishonour. This unwholesome practice has led employers of labour to conduct series of tests before recruitment of graduates in order to ascertain the credibility of their certificates. Examination Malpractice is one of the greatest social menace and cankerworms that has eaten deep into Nigerian education system and because of this ills, NUC has directed all universities to carry out aggressive awareness campaigns against examination malpractice and its consequences on campuses and also to set up committee with the sole objective of eradicating academic vices in their universities [2].

With the directives of the NUC, some Nigerian Universities have complied by expelling and rusticating some culprits [3] [4]. The threats to the reliability and validity of examination in the Nigerian education system jeopardize the authenticity of certificate issued and the reliability of the products of the school, due to the prevalence of examination malpractices. The factors that prompt students to engage in examination malpractice include difficult questions, peer influence, parental effect, harsh examination condition, unequal student treatment, excess course load, fear of failing, inadequate preparation and lecturer/teacher inefficiency. The first examination malpractice in Nigeria occurred in 1914 during the Senior Cambridge Local Examination papers which were leaked before the scheduled date of examination [5].

Impersonation which is one of the types of Examination Malpractice is the concern of this study and it is one of the dangerous security threats in which somebody claims to be "somebody" else. The issue of impersonation is considered as a major cause of concern and it is perceived as an even greater risk by the academic community [6]. Akaranga and Ongong have it that students who want to cheat willingly reveal their login details to another person for the purpose of impersonation. A student cannot 'accidentally'

Ndunagu, J. N. (2017). An Enhanced Security Measure to Eradicate Examination Malpractice in Nigerian Universities: A Biometric Authentication Approach, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, Vol. 1, pp. 49 – 56

impersonate another during assessment, it is a conscientious act.

Authentication is the process of verifying the credentials used to request access to a resource and it is a process by which the identity of an entity is valid. Authentication establishes the identity of some entity under scrutiny. It is performed by the evaluation of credentials supplied by the user. An individual is deemed authentic if the measured aspects match previously recorded data and the accuracy of matching determines the quality of authentication. Credentials can take the form of “Something you know or Shared Secret knowledge” such as a password, “Something you have” or “physical object” (Smartcard, passport and ID card) or “Something you are” or “Biometric devices by measuring physical characteristics of the human body” (fingerprints, Iris, Face, gait, DNA, keystroke dynamics, voice and hand geometry). The combination of “something you know” and “something you have” are classified as Traditional approach of authentication. Out of the three factors, the biometric factor is the most convenient and convincing to prove an individual’s identity [7]. Biometrics has numerous benefits compared with traditional recognition since one can present a fake identification card and can shave off one’s beard, but one cannot change his/her biometrics.

Finally, the integration of Biometrics and the traditional authentication will reduce the problem of impersonation during examination in Nigerian universities since iris patterns are part of one’s body and thus not easily forgotten, misplaced, stolen, forged or shared. Also, one has to be personally present in order to confirm his presence. With the adoption of Iris Recognition Technology system in Nigerian universities’ registration and examination processes, the doubt on the actual person taking examination will be minimized. This approach will encourage students to study very hard, increase employers’ confidence in the employees and as a result, optimize employability and increase efficiency of Nigerian graduates.

II. RELATED WORKS

A. Traditional Authentication

The traditional method of authentication is easy to counterfeit, the security is relatively low, cannot meet the needs of social development, passwords are the most widely used authentication credential and are subject to more fundamental attacks and are easily transferable and can be deciphered by guessing and have a lot of drawbacks and offer little security [8]. The rapid development of global economy, science and technology makes the modern society of increasingly high demand to information security need. The traditional identification methods cannot meet the need of information security, so people proposed biometric identification technology by using biometric identification, such as fingerprint, iris and voice [9]. The password is gradually becoming obsolete and biometric technology increasingly provides an effective alternative [10].

B. Biometric Authentication

Biometric authenticates individuals by identifying their physiological or behavioural characteristic. The physiological features include fingerprint, hand geometry, retina scan, iris scan, signature dynamics, keyboard dynamics, voice print and facial scan. Biometrics for identification/authentication is unique for each individual and it can be readily measured and also is invariant over time [11] [12].

C. Iris Recognition Technology (IRT)

This is the type of biometric mechanism that uses iris of the eye and compares iris patterns for identifying a person. Iris pattern are distinctive and their structures are composed of complicated unique patterns that are not changed till the end of life. With 266 mathematically unique features composed of pigmented vessels and ligaments, the chances of 2 irises to match are very negligible.

As the technology is iris pattern-dependent not sight-dependent, it can be used by blind people and also iris is highly protected, non-invasive and ideal for handling applications requiring management of large user group [12]. The accuracy of iris recognition systems is proven to be much higher compared to other types of biometric systems like fingerprint, handprint and voiceprint. Statistically, it is more accurate than DNA fingerprinting. It’s also non-contact, as the individual simply presents their eye to the device, which avoids problems with hygiene. Iris recognition system is mainly categorized into five processes namely: Image acquisition, iris segmentation, feature extraction, template matching and authentic/ poster processes.

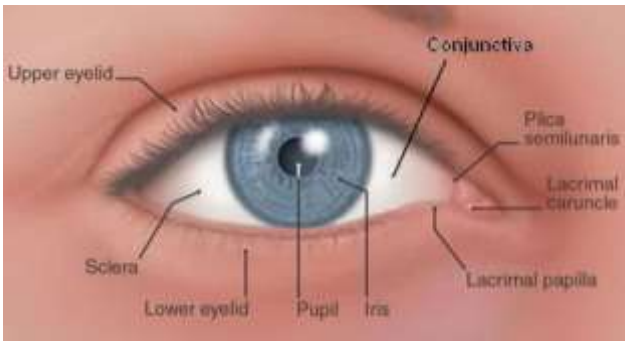

Fig 1: Structure of the human eye.

D. Merits of IRT

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

- It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognise after years of certain types of manual labour.
- The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil [13]. This makes the iris shape far more predictable than, for instance, that of the face.

- The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation. Like the fingerprint, it is very hard (if not impossible) to prove that the iris is unique. However, there are so many factors that go into the formation of these textures (the iris and fingerprint) that the chance of false matches for either is extremely low. Even genetically identical individuals have completely independent iris textures.
- An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person being identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece (like looking into a microscope.

E. Demerits of IRT

Many commercial iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing.

- The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession.
- The accuracy of scanners can be affected by changes in lighting.
- Iris scanners are significantly more expensive than some other forms of biometrics, password or proxy-card security systems
- Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition.
- Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera.
- As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enrol rates. As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

F. Iris at a distance

Iris at a distance (IAD) performs iris and portrait acquisition. The acquired data can be used for both registration and verification purposes. IAD features are (1) fastest possible throughput with an acquisition time under one second (2) easy to use (3) simultaneous capture of two irises and face (4) easy to integrate into an existing environment.

A number of iris recognition at a distance systems have been developed including; Iris on the Move (IOM), operating at 2-3 meters with subjects walking at normal speed [14]; Eagle-Eyes, operating at 3-6 meters and a capture volume of 3×2×3m3 [15]; Stand-off-Iris, operating at 1.5 meters [16]; Pan-tilt-zoom Iris, operating at 1.5-10 meters [17]; and Long range iris acquisition system, operating at 8-12 meters [18]. An Iris recognition system uses a video camera to capture the sample while the software compares the resulting data against stored templates.

A video camera is mounted at the wall of the university’s examination hall and there is a designated point where the candidate stands and stares at the camera. The process captures both the iris and the portrait and the same process can be performed for both registration and verification.

G. Daugman's Algorithm

Daugman, pioneered the formulation of iris recognition algorithms required for image acquisition and one-to-many matching and become the basis of almost all currently commercially deployed iris-recognition systems. His algorithm locates the iris boundaries using an integro-differential operator that finds the circles in the image where the intensity is changing most rapidly with respect to changes in the radius. Once located, the iris image is converted to a Cartesian form by projecting it to onto a dimensionless pseudo-polar coordinate system. The iris features are encoded and a signature is created using a 2-D complex-valued Gabor filter. Finally, two images are said to be independent if their fractional Hamming distance (Hd) is above a certain threshold, otherwise they are a match. Hd is equal to the number of mismatching bits divided by number of compared bits [19]

The proposed method for iris recognition identification is divided into four main phases processing: Image Processing; image localization; IER detection and image recognition. The first phase of authentication involves iris image acquisition. User stares at the special camera for some seconds and the camera scan the eye image. The captured digital image is processed by an algorithm and iris is extracted. The iris image is normalized to solve the imaging discrepancies. The patterns that constitute the iris and its surroundings (circular iris, eye lids and pupils) are located using the formula:

The equation is as follows:

$$\max_{(r,xp,\,yo)} \left| G_\alpha * \frac{\Delta}{\Delta x} \oint_{(r,xp,y0)} \frac{I(x,y)}{2\pi r}\, ds \right| \qquad (1)$$

Equation 1: Daugman's Integro-Differential Equation

Where:

I(x,y) – Eye image, r – Radius, G_σ –Gaussian Smoothing Function, s – Contour of the circle given by r, x_0, y_0

Gσ is a smoothing function, the smoothed image is then scanned for a circle that has a maximum gradient change, which indicates an edge. The above algorithm is done twice, first to get the iris contour then to get the pupil contour. It worth mentioning here the problem is that the illumination inside the pupil is a perfect circle with very high intensity level (nearly pure white). Therefore, we have a problem of sticking to the illumination as the max gradient circle. So a minimum pupil radius should be set. Another issue here is in determining the pupil boundary the maximum change should occur at the edge between the very dark pupil and the iris, which is relatively darker than the bright spots of the illumination. Hence, while scanning the image one should take care that a very bright spot value could deceive the operator and can result in a maximum gradient. This simply means failure to localise the pupil.

H. Hamming Distance

The Hamming distance is the matching metric employed by Daugman, and calculation of the Hamming distance is taken only with bits that are generated from the actual iris region.

The Hamming distance between two strings of bits (binary integers) is the number of corresponding bit positions that differ. This can be found by using XOR on corresponding bits or equivalently, by adding corresponding bits (base 2) without a carry. For example, in the two bit strings that follow:

The Hamming distance (H) between these 10-bit strings is 6, the number of 1's in the XOR string.

The iris is compared to previous stored iris code to compute the Hamming distance between them.

$$\mathrm{HD} = \frac{I}{N}\sum_{J=I}^{N} \mathrm{Xj}(\mathrm{XOR})\, Yj$$

Hamming distance is simply the fraction of bits that the two iris codes disagree. Hence the Hamming distance of an iris code to itself is 0, the Hamming distance to its complement is 1 and the expected Hamming distance between 2 random iris codes is 0.5. The Hamming distance can be computed using the elementary logical operator XOR (Exclusive-OR) and thus can be done very fast. To compensate for possible tilt of the head, the comparison is made with several different relative shifts along their angular axes [20].

In feature extraction significant features of the iris are extracted for the accurate identification purpose. Feature extraction identifies the most prominent features for classification. The features are encoded in a format suitable for recognition. Finally, matching, - authenticates via identification (one-to-many template matching) or verification (one-to-one template matching), a template created by imaging the iris is compared to a stored value template in a database. The matching metric will give a measure of similarity between two iris templates and a decision of the high confidence level is made to identify whether the user is authentic or not [21]. In the year 1990, Daugman developed the algorithm that implemented iris recognition technology [22]. The Daugman algorithm is considered as among the most accurate iris recognition that is used today.

I. Iris segmentation

Iris segmentation plays a key role in the performance of an iris recognition system. This is because improper segmentation can lead to incorrect feature extraction from less discriminative regions (e.g., sclera, eyelids, eyelashes, pupil, etc.), thereby reducing the recognition performance.

However, iris segmentation is the most time consuming step in the iris recognition system and so become the bottleneck in real time environments. Iris segmentation is difficult task and faces some challenges such as specular reflection, contrast enhancement, blurred images and occlusion.

J. Challenges in Iris Segmentation

Iris segmentation refers to the process of automatically detecting the pupillary (inner) and limbic (outer) boundaries of an iris in a given image. This process helps in extracting features from the discriminative texture of the iris, while excluding the surrounding regions. Segmentation of an iris image is a classical image processing problem. Processing non-ideal iris images is a challenging task because of the following reasons:

- The iris is often partially occluded by eyelids, eyelashes, and shadows.
- The iris is sometimes occluded by specular reflection.
- The iris and the pupil are noncircular, and the shape varies depending on how the image is captured.
- Some of the other challenges of iris segmentation are defocusing, motion blur, poor contrast etc. These challenges are taken care by measuring the quality of input iris image and then continue with segmentation of the good quality image only.
- The noise in images is considered to be of these types- the iris obstruction by eyelids or eyelashes, specular or lighting reflections, poor focused image, partial or out-of iris image, motion blurred as belonging to the iris.

Two main challenges of iris segmentation of realistic eye images are addressed: segmentation accuracy and processing speed.

K. Existing iris segmentation methods

A significant number of iris segmentation techniques have been proposed in the literature. Two most popular techniques are based on using an integro-differential operator and the Hough transform, respectively. The performance of an iris segmentation technique is greatly dependent on its ability to precisely isolate the iris from the other parts of the eye. Both the above listed techniques rely on curve fitting approach on the edges in the image. Such an approach works well with good quality, sharply focused iris images. However, under challenging conditions (e.g., non - uniform illumination, motion blur, off-angle, etc.), the edge information may not be reliable. Table 1 summarizes the different algorithms for iris segmentation proposed by various researchers.

Table 1: Overview of prominent existing methods of iris segmentation

Author	**Iris Segmentation techniques**
Daugman *et al.(2001)* [23]	Integro-differential operator
Wildes *et al.(2005)* [24]	Image intensity gradient and Hough transform
Ma *et al.(2005)* [25]	Hough transform
Ma *et al.(2004)* [26]	Gray level information, canny edge detection, and Hough transform
Masek (2003) [27]	Canny edge detection, and Hough transform
Abhyankar *et al.*(2005) [28]	Active shape model
Basit & Javed *et al.* (2005) [29]	Maximisation of the difference of intensities of radial direction
M. Vatsa *et al.(2007)* [30]	Modified Mumford – Shah functional
K. Nguyen *et al.(2010)* [31]	Shrinking and expanding active contour methods

The best known and thoroughly examined iris segmentation method is Daugman *et.al.*[23] method using Integro differential operators, which are a variant of the Hough Transform, act as circular edge detectors and have been used to determine the inner and the outer boundaries of the iris. They also have been used to determine the elliptical boundaries of the lower and the upper eyelids. The Hough transform is a standard computer vision algorithm that can be used to determine the parameters of simple geometric objects, such as lines and circles, present in an image. The circular Hough transform can be employed to deduce the radius and centre coordinates of the pupil and iris regions. Firstly, an edge map is generated by calculating the first derivatives of intensity values in an eye image and then thresholding the result. From the edge map, votes are cast in Hough space for the parameters of circles passing through each edge point.

L. Feature Encoding and Matching:

For accurate recognition result, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between irises can be made. In order to study the effects of iris segmentation on the iris recognition accuracy performance Log Gabor filters are used to extract the textural information (encoding) from the unwrapped iris. Further, the feature vectors are compared using a similarity measure for which matching algorithm is used.

III Methodology

The methodology section of this paper answers two main questions: How the data was generated and how it was analysed. The data were collected during enrolment and stored in the database for further action during verification.

The enrolment of university students can be done manually or electronically, though this study was about the electronic enrolment. The procedure for Iris recognition technology in Nigerian universities to reduce examination malpractice is as follows:

- The special cameras would be mounted at designated places of the Universities for capturing students for enrolment and verification.
- At a distance (see Figure 2), each candidate stares at the special camera for some seconds and the camera scans the eye image.
- Figure 3, showed the processes of extracting the iris using an algorithm method.
- (a) In fig 4, four processes were performed namely: Image acquisition, Iris segmentation, feature extraction and storage – the database. The acquired image is processed by an algorithm and iris is extracted and the outputs were stored at a database. This is for an enrolment exercise.
- (b)Also, in fig 4, which is for authentication/identification of candidates, five processes were performed, the same four (4) processes in (4a) with an additional processing of matching- which help to determine the status of the candidate for examination. The result could be either having access or denial to the examination hall.

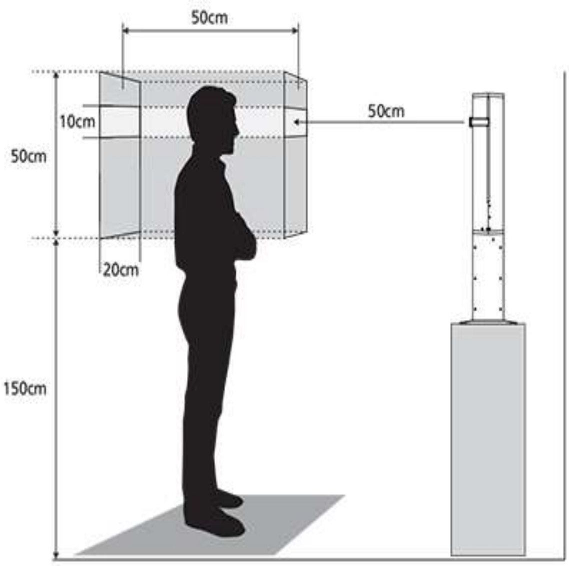

Figure 2: Pictorial illustration of Iris at a distance.

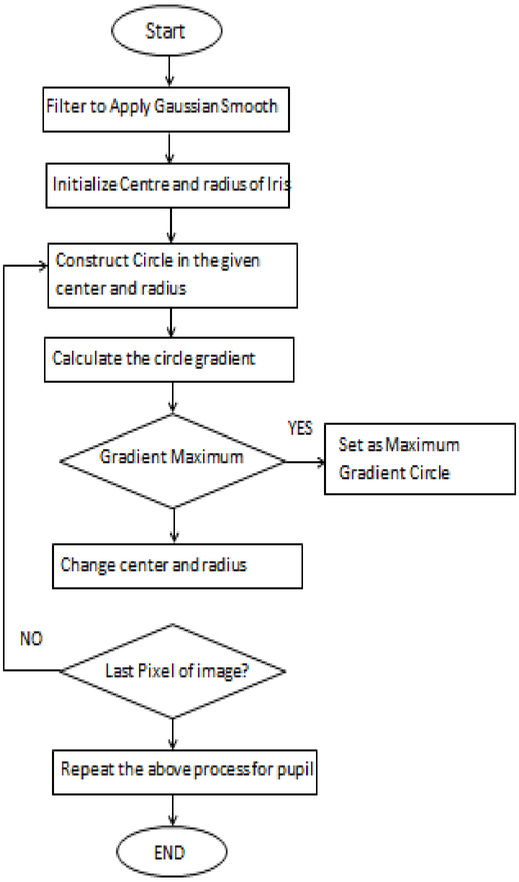

Figure 3: Flow Chart Describing Dangman's Method

A. Algorithm used for Implementation of Integro differntial operator:

Step 1: Initialize r_{min}=95, r_{max}=105 & scaling=0.25.
Step 2: Coarse search for iris centre.
Step 3: Perform line integration.
Step 4: Carry out the differentiation.
Step 5: Obtained the blurred image using Gaussian filter.
Step 6: Determine the maximum value of blurred image for the coarse centre Coordinates and radius.
Step 7: Implement equation

$$\max_{(r,xp,yo)} \left| G_\alpha * \frac{\Delta}{\Delta x} \oint_{(r,xp,y0)} \frac{I(x,y)}{2\pi r} ds \right|$$

Step 8: Fine search around this roughly located centre.
Step 9: Initialize rmin and rmax for pupil
Step 10: Repeat step 3 to step 6.
Step 11: Draw the circle using iris centre and radius.
Step 12: Draw the circle using pupil centre and radius.

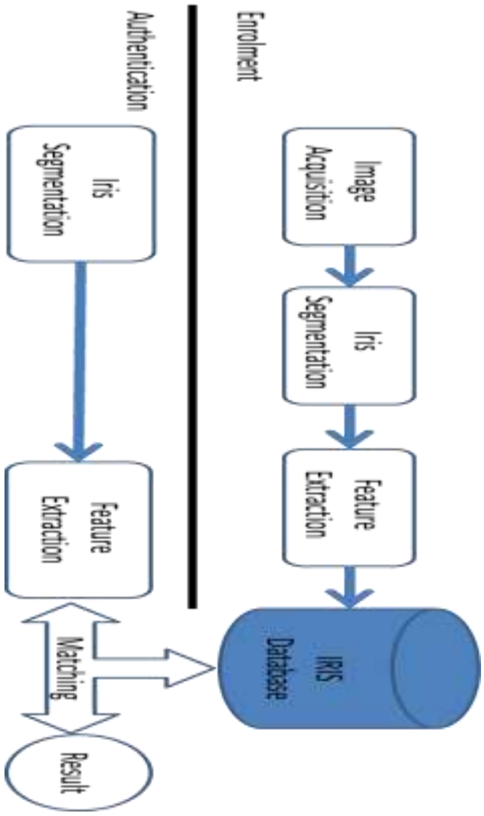

Figure 4: Iris recognition process

IV Results and Discussion

Iris at a distance is very simple and convenient to use because the only thing the user needs to do is to look at the sensor screen for a second from a designated position. The study found out that candidates who are captured at a close distance of 0.6≤ x≤ 1 ensure images of sufficient quality. This yielded more accurate result in verification than images captured on the move or longer distance from the camera.

Images captured at a distance were more accurate in identification/identification of candidates for examination. This fact is in tandem with the International Standard Organization (ISO) released in 2005 [19]. However, images captured on move and at a longer distance have more challenges [20] [14][15][16][17][18].

With the integration of iris recognition technology in addition to the traditional approach already in place for identifying examination candidates in Nigerian universities, it is expected that there will be reduction in the number of imposters during examination as the new system of authentication will naturally scare and also identify the culprit if any. This idea would fortify the traditional method of authentication which is easy to counterfeit; the security is relatively low and cannot meet the needs of social development. Traditional method is subject to more fundamental attacks and are easily transferable and can be deciphered by guessing and have a lot of drawbacks and offer little security, this is in tandem with [8, 9, 10]

V Conclusion*:*

The proposed system will serve as a double check of identification since iris recognition technology has a lot of advantages in terms of security, speed and accuracy. The new idea when adopted will drastically reduce the impersonation type of examination malpractice in Nigerian Universities.

In the future we intend to analyse and evaluate in full details, the iris recognition technology and its potentials for socio-economic developments in the society.

References

[1] Chizoma, J. (2016). "The Involvement of Undergraduates in Examination Malpractice in Nigerian Universities.," Project , 2016.

[2] National University Commission (2016), "ATBU," May 2016. [Online]. Available: http://www.atbu.edu.ng/app/assets/files/NUC%20on%Paper%20Grade%20sorting%20in%20Nig.pdf. [Accessed August 2017].

[3] Daily Post (2016), "UNILAG expels 125, rusticates 198 students," Daily Post, Lagos, October 17, 2016.

[4] Daily Trust (2016), "Law School tackles examination malpractices," Daily Trust, January 27, 2016.

[5] Akinrefon A.,. Ikpah, O. C., Bamigbala A. O and. Adeniyi O. I, (2016) "On Examination malpractice in Nigeria Universities: Factor Analysis Definition," *Bulgarian Journal of Science and Education Policy* (BJSEP), vol. 10, no. 1.

[6] Akaranga S. and Ongong J. (2013), The Phenomenon of Examination Malpractice: An Example of Nairobi and Kenyatta Universities, *Journal of Education and Practice*, vol. 4, no. 18, 2013.

[7] McDaniel P. (2006), "Authentication," Pennsylvania State University, 2006.

[8] Ndunagu J. and Okuade O. (2012). Diffusion of Cybercrime in the Nigerian Cash-Less Economy: Using Double Level Authentication, *Journal of Information and Communication Technology*, vol. Vol.2, No. Issue 7.

[9] Gao, X., Feng S.and Cui, H. (2015). Enhanced Iris Recognition Based on Image Match and Hamming Distance, *International Journal of Smart Sencing and Intelligent System*, Vol. 8, No 2

[10].Mahnken S, (2014) "Today's authentication options: The need for adaptive multifactor authentication," Elsevier Science.

[11] Mbamalu C. B., "Comparatice Analysis of Biometric Identification System. A case study of National Identity Management Commission," An MSc Thesis (Unpublished), 2016.

[12] M. Sujithra and G. Padmavathi, "A survey of Biometric Iris Recogntition Security, Techniques and Metrics," Asian Journal of Information Technology, vol. 14, no. 6, pp. 192-199, 2015.

[13] W. K. Adams, Z. David and S. K. Mohamed, "An Analysis on Iris Code," IEEE transactions on image processing, vol. 19, no. 2, p. 552, 2010.

[14] J. Matey, O. Naroditsky, K. Hanna, R. Kolezynski, D. Lolacono, S. Mangru, M. Tinker, T. Zappia and W. Zhao, "Iris on the move: acquisition of images for iris recogntion at a distance," Proceedings of the IEEE, vol. 94, no. 11, pp. 1936-47, 2006.

[15] F. Bashir, P. Casaverde , D. Usher and M. Friedman, "Eagle-eyes: A system for iris recognition at a distance," in IEEE International Conference on Technologies for Homeland Security, HST '08, 2008.

[16] F. Wheeler, A. Perera, G. Abramovich, B. Yu and P. Tu, "Stand-off iris recognition system, Biometrics: Theory, Applications and Systems (BTAS)," in 2nd IEEE International Conference, 2008.

[17] S. Yoon, K. Bae, K. R. Park and J. Kim, "Pan-tilt-zoom based iris image capturing system for unconstrained user environments at a distance. Advances in Biometrics," in Proceedings International Conference, ICB (Lecture Notes in Computer Science vol. 4642), 2007.

[18] S. Venugopalan, U. Prasad, K. Harun, K. Neblett, D. Toomey, J. Heyman and M. Savvides, "Long range acquisition system for stationary and mobile subjects. Biometrics (IJCB)," in International Joint Conference, 2011.

[19] Z. Yong, T. Tieniu and W. Yunhong, "Biometric Personal Identification Based on Iris Patterns National Laboratory of Pattern Recognition (NLPR)," in Institute of Automation, 2003.

[20] L. Juwei , P. N. Konstatinos and V. N. Anasios, "IEEE Trans. Neural Networks," 2003.

[21] T. Rakesh and M. G. Khogare, Survey of biometric recognition system for Iris, *International Journal of Emerging Technology. Advanced. Eng.* , vol. 2.

[22] Iris Recognition (2006) National Science and Technology Council Commitee on Technology, Homeland and National Security Sub-committee, "Biometrics," 2006.

[23] J. Daugman, “Statistical richness of visual phase information: Update on recognizing persons by iris patterns,” International Journal of Computer Vision , vol. 45, no. 1, pp. 25-38, 2001.

[24] R. P. Wildes, Iris recognition. In Biometric Systems: Technology Design and Performance Evaluation, Spring Verlag, 2005.

[25] L. Ma, T. Tan, Y. Wang and D. Zhang, “Efficient iris recognition by characterizing key local variations,” in IEEE Transactions on Image Processing, 2004.

[26] L. Ma, T. Tan, Y. Wang and D. Zhang, “Local intensity variation analysis for iris recognition,” in Pattern Recognition, 2004.

[27] L. Masek, “Recognition of human iris patterns for biometric identification,” Master's thesis, University of Western Australia, 2003.

[28] A. Abhyanakar, L. Hornak and S. Schuckers, “Off-angle iris recognition using bi-orthogonal wavelet network system,” Fourth IEEE Workshop on Automatic Identification Technologies, 2005.

[29] A. Basit, M. Y. Javed and M. A. Anjum, “Efficient iris recognition method for human identification,” in International Conference on Pattern Recognition and Computer Vision , 2005.

[30] M. Vatsa, Richasingh and A. Noore, “Integrating image quality in 2v-SVM biometric match score fusion,” International Journal of Neural Systems , vol. 17, no. 5, pp. 343-351, 2007.

[31] K. Nguyen , C. Fookes and Sridhasridharan, “Fusing Shrinking and Expanding Active Contour Models for Robust Iris Segmentation,” in 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA), 2010.