Remote Access Control System using Iris Signature

Falohun A. S, Omidiora E.O, Akanni A.O, Awofadeju A.S

***Abstract*-** Modern day technology has come with many problems of authentication. For instance, in E-Business transactions where potential buyers and sellers do not meet physically, it might be difficult to verify the identity of the people involved. Also of concern is the high rate of hacking on networks and the internet.
In this work, a remote access login system that used iris templates is done to grant access to legitimate users and deny same to unauthorized fellows. The system developed was tested with our indigenous black iris data sets from Nigeria (representing the black race populace) while the result was benchmarked with that obtained from the very popular, foreign and standard, CASIA iris database. The result evaluation was done using False Acceptance Rate (FAR), False Rejection Rate (FRR) and Recognition Accuracy.

Keywords- Open search, synchronization, Feature Extraction, Thresholding.

I INTRODUCTION

The need for security on lives and properties in this 21st century cannot be overemphasized, as it is one of the major challenges facing individuals, corporate organizations and nations. From tangible to intangible properties, everyone is becoming more alert to the need for efficient means of security.
In the past, authentication was based on:

- What a person has such as smart card, ID card. This was overtaken by impersonation.
- What a person knows like password, PIN code. This scheme also has been defeated by hacking.

But nowadays, authentication and verification is better done using biometrics, which is a measure of what one possess .i.e, who one is, which has so far proven unbeatable.
Biometrics can be rightfully described as the science and technology of verifying a person's identity. It measures the physical characteristics that make everyone distinctive, like the eye's retina or iris, fingerprint, face, hand, voice - and uses those dimensions to confirm personal identity. Passwords are easy to steal and difficult to remember. Driver's licenses, keys, and passports can be lost or forged [1]. On the other hand, the human body can not be forgotten, stolen, forged or lost.

Falohun A.S is with Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. (leye_falohun@yahoo.com)
Omidiora E.O is Prof. of Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. (eoomidiora@lautech.edu.ng)
Akanni A.O. is with Department of Computer Engineering, Osun State polytechnic, Iree, Nigeria. (ayoakanni1@gmail.com)
Awofadeju A.S is with Department of Civil Engineering, Osun State polytechnic, Iree, Nigeria. (awofadejuas@yahoo.com)

Practical uses for such biometrics are everywhere and include maintaining the security for both physical space and cyberspace.
However, in this work, attention is given to human physiological identity called the **iris.**

II IRIS RECOGNITION SYSTEM

A typical iris recognition system [6] is shown in Figure 1, which involves four main modules: the image acquisition module, the pre-processing module, the template generation module, and the pattern recognition module.

- Image acquisition. This module captures one or multiple iris image(s) from the subject using an iris camera.
- Pre-processing. At this step, the image is enhanced first. The enhancement includes contrast adjustment and noise filtering. The next step is to perform edge detection and thresholding. The pupillary boundary (inner boundary of the iris), the limbic boundary (outer boundary of the iris), eyelids, and eyelashes are detected. In this way, the iris patterns can be extracted from the iris image. Usually, normalization between the pupillary boundary and the limbic boundary is performed in this step to reduce the effect of the pupil constrain or dilate.
- Template generation. The extracted iris patterns are not ready for comparison yet. In this step, the template is created from the extracted iris patterns. In the literature, there are various ways to generate the templates. This include Gabor wavelet, zero-crossing wavelet, local variance, spatial filters, and 1D local texture pattern approaches.
- Pattern recognition. The newly generated iris template is compared with the iris templates in the database. If a match is found, this iris would be identified. The matching methods include binary code matching method and similarity matching method.

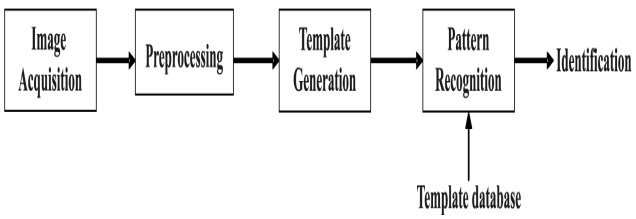

Fig 1. A typical Iris recognition system (source: [6])

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III AREAS OF APPLICATION

These include ATM Operations, Police Affairs, Electronic-Government Affairs, Network Security, Impersonation, Immigration Systems, Airports, Border Control, Safety and reliability of Electronic-Commerce, Confirmation of student identity for distant learning and examinations to mention but a few.

IV REVIEW OF RELATED WORK.

The history of iris recognition goes back to mid 19th-century when the French physician, Alphonse Bertillon, studied the use of eye colour as an identifier. [2]. However, it is believed that the main idea of using iris patterns for identification, the way we know it today, was first introduced by an eye surgeon, Frank Burch, in 1936. [5]. In 1987, two ophthalmologists', Flom and Safir (1987), patented this idea. Daugman, a Professor at Harvard University studied the possibility of developing an iris recognition algorithm based on the recommendation proposed by Bertillon. Currently, Daugman's iris recognition system is installed in several airports worldwide. A few years after the publication of the first algorithm by Daugman, other researchers developed new iris recognition algorithms. Systems presented by [11] ; [3] ; [9]; [12] ; [10] are some of the well-known algorithms so far.

In 2012, Falohun *et.al.* employed Control Engineering's ability to automate a security door system that granted access only to legitimate users whose iris templates were earlier stored in a database.

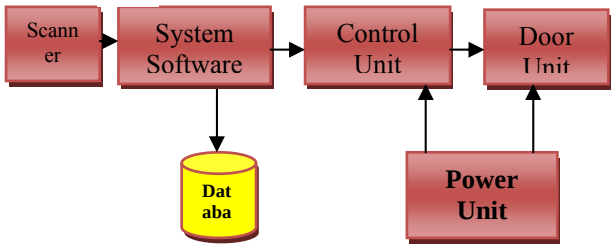

Fig 2. Block diagram of an Iris - based access system used.(Source: [7])

V METHODOLOGY

Design Consideration and Background Theory

In other to put up a web-based iris recognition system, At least two PCs are required (could be more) whereby one of the PCs will work as the server where the MATLAB application interface will be running and the other(s) as the client(s).

The first stage of web-based iris recognition system begins with building the database of individuals that will use the online facility. Firstly, the iris image of all involved alongside some personal information such as name, date_of_birth, sex, age, user identification etc are allotted iris Id. Each image captured is given a unique identification code which serves as the primary key attached to each person's data form. This uniquely identifies each user's iris images even if all users have all other information in common.

VI DATA NEED

Image acquisition for the black iris images was done using a high resolution, 5.0 Megapixels Frontech webcam improvised alongside an application software coded in Visual Basic 6.0 to capture, resize and gray-scale the irises while the CASIA images were downloaded from their site.

CASIA: Chinese Academy of Science's Institute of Automation(CASIA) provides a public and freely available iris image databases for biometric purposes , the most widely used for iris biometric research (captured under good positioning and illumination condition).Here we used CASIA Version 1 of 108 subjects, 7 images per person.

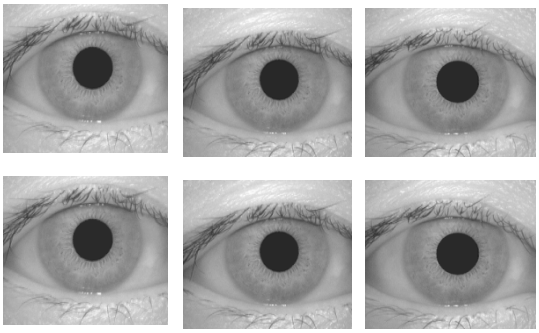

Fig 3a CASIA iris images.(Source: http://www.sinobiometrics.com., 2009)

BLACK FACES IRIS: Iris images captured within Nigeria people was also used to test the performance of the recognition system. A total of 150 images were collected for experimentation from 15 subjects with 10 samples each.

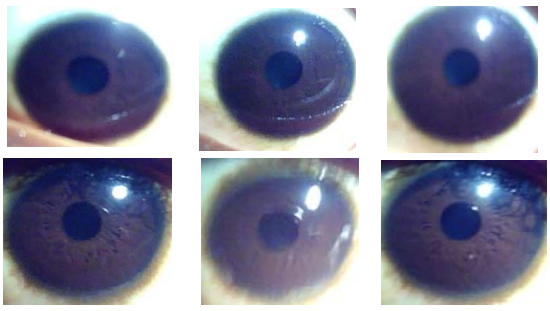

Fig 3b Black iris images.

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Segmentation

Two-level segmentation technique combining Circular Hough Transform and Daugman's Integro-Differential Operator was used.

Hough Transform performs better than other localization techniques in case of occlusion due to eyelids and eyelashes**.** It is an automatic segmentation algorithm employed to deduce the radius and center coordinates of the pupil and iris region. It's parameters are the centre coordinates x_c and y_c, and the radius r, which are able to define any circle according to the equation

$$x_c^2 + y_c^2 - r^2 = 0 \quad (1)$$

It also detect eyelids, approximating the upper and lower eyelids with parabolic arcs, which are represented as

$$(-(x-h_j)\sin\theta_j + (y-kj)\cos\theta_j)^2 = a_j((x-h_j)\cos\theta_j + (y-kf)\sin\theta_j \quad (2)$$

Where a_j controls the curvature, (h_j, k_j) is the peak of the parabola and Ø is the angle of rotation relative to the x-axis. And because inner and outer iris boundaries are not concentric like the pupil, integrodifferential operator is performed around the pupil center and the iris radius in order to find the iris center according to equation 3.

$$max_{(r,x_0,y_0)} |G_\sigma(r) * \partial \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds| \quad (3)$$

Where I(x, y) is the eye image, r is the radius to search for, Gσ (r) is a Gaussian smoothing function, and s is the contour of the circle given by r, x_0, y_0. The operator searches for the circular path where there is maximum change in pixel values, by varying the radius and centre x and y position of the circular contour.

Feature Extraction

A feature extraction based on Enhanced Inverse Analytical Fourier-Mellin Transforms was used to extract the isolated iris texture.[7] .

Feature Matching

The Hamming distance gives a measure of how many bits are the same between two bit patterns [4]. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one.

In comparing the bit patterns X and Y, the Hamming distance, HD, is defined as the sum of disagreeing bits (sum of the exclusive-OR between X and Y) over N, the total number of bits in the bit pattern.

VII Interconnecting Client Systems To The Server

Three PCs were interconnected via a wireless LAN to a main server on which the Iris recognition interface was deployed. An adhoc connectivity was created on the server; serving as a base for all the other PCs to connect through. The server was configured with an IP address of 192.168.0.4; all other PCs were also given IP addresses in the same IP range.

After the three PC's has been configured and networked, whenever any of the remote client user put in the IP address of the server (i.e 192.168.0.4) on its port's http terminal in its browser, the server index automatically pops up as shown in Fig. 4.

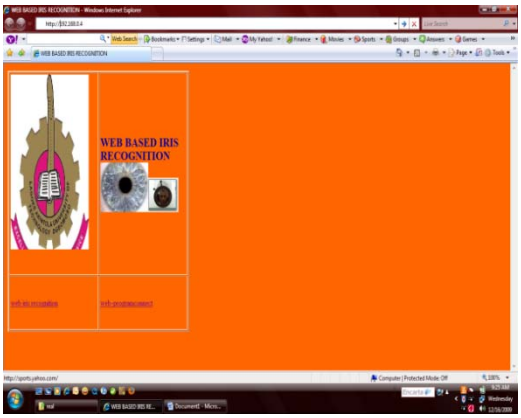

Fig 4. Web-Based Iris Recognition Interface

VIII ANALYSIS OF HOW THE SYSTEM WORKS ON THE WEB

The iris recognition system link on the index, 'web-programconnect' is first clicked to ensure remote synchronization with the client PC after which the exec utable form ('web_iris_recognition) is launched so that the system can either download or run the iris recognition interface straight from the server.

The iris recognition system on trigger, remotely allows as many as possible individuals to be added into the iris database and for resource users to be authenticated by matching them with the new user presently enrolling to check if the iris has earlier been added into the database in an open search.

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Registration Interface

This interface presents the registration platform for the iris template where the iris template is loaded and registered with a unique user name. The registered iris template is processed and saved in the database (Figure 5).

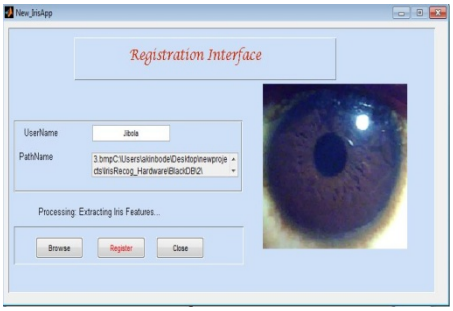

Fig 5. Registration Interface

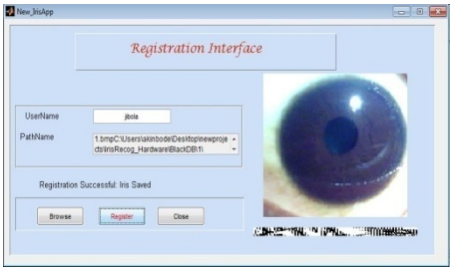

Fig 6. Extracted Iris

Authentication Interface

This interface compares the already registered iris template with the captured template. Figure 7 shows a matched template which prompted a green light indicating an access signal. But in a situation of 'non-match', an error message "iris not recognized: access denied" is flagged (figure 8) which means, an "end of the road" to operation

.

Fig 7. Authentication interface showing access granted

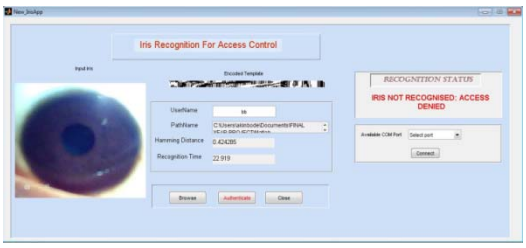

Fig 8. Authentication interface showing access denied

Meanwhile, to evaluate the efficacy of the system, it was mandatory to measure its performance at different thresholding points .i.e at varying hamming distances between 0.26 and 0.45 to reveal the False Acceptance Rate(FAR), False Rejection Rate (FRR) and Recognition Accuracy. Table 1 showed the result obtained with the black man's 150 iris images from 15 subjects, 10 per person while Table 2 showed the evaluation results on 756 eye images of 108 subjects (7 per individual) from the CASIA database.

Table 1. Black Iris Recognition Accuracy

Hamming Distance	FAR(%)	FRR(%)	ACCURACY(%)
0.26	0.00	88.00	12.00
0.30	0.03	46.67	53.30
0.35	0.17	26.67	73.16
0.39	0.33	20.00	79.67
0.45	0.57	3.33	96.10

Table 2. CASIA Iris Recognition Accuracy

Hamming Distance	FAR(%)	FRR(%)	ACCURACY(%)
0.26	0.00	26.13	73.87
0.30	0.00	15.43	84.57
0.35	0.00	6.69	93.31
0.39	0.00	2.78	97.22
0.45	2.78	26.10	71.12

IX RESULTS AND DISCUSSION

The proposed system has been tested with a number of iris templates, and is found to work accurately i.e recognizing every enrolee on every of the PCs on the network immediately a registration is done at any point while at the same time granting access to the server's resources after subject's authentication and denying access request to impostors as corroborated by Figures 7 and 8 .This "control system" will authenticate any subject remotely in various forms of transactions and even electorates, and can guide against multiple casting of votes during election.

At evaluation point, it was found, that the optimum Hamming Distance(HD) was reached at 0.39 which yielded a recognition accuracy of 97.22% for the CASIA but then, that for the black irises yielded 79.67% at same HD. This is because (1) the iris camera used here in Nigeria is an improvised one that is not as standard as the one used in

ISBN: 978-988-19252-3-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

CASIA. (2) CASIA images were captured with totally controlled illumination for iris recognition researches and (3) the black iris has poor contrast unlike the white man's, where there is a sharp contrast between the pupil- iris, iris-sclera boundary.

X CONCLUSION

A biometric – based access control system that used iris templates in a network of systems has been developed which will grant access to legitimate enrolees and guide against multiple enrolment whenever the subject tries to re-surface at another registration point. Just as in the case of an election, represented by another node in the network, details of the previous enrolment with exact time of registration would be noted while denying access to the registration interface immediately. This guarantees a high level of security. The testing of the system was done using eye images from black and white populace.

ACKNOWLEDGEMENT

Many thanks we give to the director, Biometric Research Centre (a World Bank assisted Biometric Centre in Nigeria), Professor T.S Ibiyemi of the department of Electrical Engineering, University of Ilorin, Nigeria for providing us with all the iris capturing equipments used in this work. The Centre's contributions really helped in our image acquisition and pre-processing activities.

REFERENCES

[1]. M. S. Ahmad, " Iris Recognition using Discrete Cosine Transform andArtificial Neural Networks." Journals of Computer Science, vol.5, pp 369 – 373. 2009

[2]. Bertillon, "Person Identification Technique using human Iris Recognition", citeseerx.ist.psu.edu/viewdoc/summary. , 1885.

[3]. W. Boles and B. Boashash., "A Human Identification Technique using Images of the Iris and Wavelet Transform.", IEEE Transactions on Signal Processing, 46 vol 4: 457- 459. 1998.

[4]. J. Daugman, "High Confidence Visual Recognition of persons by a test of Statistical indepencence". IEEE Transactions on Pattern Analysis and Machine Intelligence, 1148 – 1161, November 1993.

[5]. J. Daugman, "High Confidence Visual Recognition of persons by a test of statistical independence", IEEE Transactions on pattern analysis and machine intelligence, 15 vol 11, pp 1148 – 1161, 2001.

[6]. Du et al., 2005 A typical Iris recognition system.

[7]. A.S. Falohun, "Development of a Feature Extraction Method for IrisRecognition using Enhanced Inverse Analytical Fourier-Mellin Transform". Unpublished Ph.D.Thesis. April 2012.

[8]. A.S. Falohun, E.O. Omidiora , O.A. Fakolujo , O.A. Afolabi, A.O. Oke , F.A. Ajala,"Development of a Biometrically-Controlled Door System (Using Iris), with power Backup." American Journal of Scientific and Industrial Research., vol 3, No 4, pp 203-207. , 2012.

[9]. C. Tisse, L. Martin, L. Torres and M. Robert (2002) "Personal Identification technique using human iris recognition", In proceedings of ICVI' 02, pp. 294 – 299.

[10]. S. Lim, K. Pae, K. Lee, O. Byeon and T. Kim. "Efficient Iris recognition through improvement of feature vector and classifier", ETRI Journal, Vol 23, No 2, pp 61 – 70. 2001.

[11]. R. Wildes "Iris Recognition An Emerging Biometric Technology", proceeding of the IEEE, 85(a), pp 1348 – 1363, 1997.

[12]. Y. Zhu, T. Tan., Y. Wang , "Biometric personal Identification based on Iris Patterns." Proceedings of the 15th International Conference on Pattern Recognition, (ICPR'00)- 2: 2801.video sequences.", Journal of Electronic Imaging., Vol 19, No 3, 2000.