Access Control in E-Library and E-Examination Using Facial Recognition System

Lawal, O.A.[1], **Adebayo, A.A.**[2], **Adenekan, O.A. PhD** [3] **& Oyedeji, A.I.**[4]
Department of Computer Science, Moshood Abiola Polytechnic, Abeokuta Ogun State Nigeria[1,2]
Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta Ogun State Nigeria[3]
Department of Computer Engineering, Ogun State Institute of Technology,Igbesa, Ogun State Nigeria[4]
E-mails: oyindamola2008@gmail.com[1], debamos04@yahoo.com[2], adenekanolujide@yahoo.com[3], ayooyee@ogitech.edu.ng[4]

ABSTRACT

This paper presented an access control system in e-library and online examination, using facial authentication techniques recognition. A facial authentication system is a technology that is capable of identifying or verifying a person from a digital image. It is used as an access control in securing e-library resources and elimination of malpractices such as impersonification during the conduct of online examination. Numerous on line crimes are committed by people on daily basis where users are taking advantage of personal identities such as ID cards keys, passports, pin numbers or mother's maiden name etc. This research work developed a reliable biometric authentication system and evaluate face recognition system by comparing both the traditional and biometrics system based on the following parameters: speed, memory space, accuracy, reliability and cost.

Keywords: Access, image, authentication, pixel, digital.

24th iSTEAMS GoingGlobal Multidisciplinary Conference Proceedings Reference Format
Lawal, O.A, Adebayo, A.A., Adenekan, O.A. & Oyedeji, A.I. (2020 Access Control in E-Library and E-Examination Using Facial Recognition System. Proceedings of the 24th iSTEAMS GoingGlobal Multidisciplinary Conference Proceedings. The University of Ghana/Council for Scientific & Industrial Research Ghana – Vitually Stationed in June, 2020. Pp 265-272 www.isteams.net/ghana2020

INTRODUCTION

Creating a strong password is simple; remembering it, impossible; reusing it in many places, unacceptable but inevitable. And the victim of a cracked account is always blamed for poor choices. Reliable user authentication is essential. The consequences of insecure authentication in a banking or corporate environment can be catastrophic, with loss of confidential information, money, and compromised data integrity. Many applications in everyday life also require user authentication, including physical access control to offices or buildings, e-commerce, healthcare, immigration and border control, etc. (Araromi, 2011).

Access control system is a security system that ensures the security of a resource(s) by utilizing a person-specific authentication method, in order to grant access to specific persons. An access control mechanism effectively monitors the access activities of resources and ensure that authorized users access information resources under legitimate conditions. (Jing et al, 2020). The system has important features such as, limiting access to only specific people, saving the records of allowed accesses, modernizing security for organization as it grows and expand, and develop complex but easy to use security systems that are still. Providing a secure system among the midst of numerous online fraudulent activities is a challenging task that need to be resolved with to e-library concept in academics' environment.

The term electronic library often shortened as e- library is a computerized information storage and retrieval systems connected to computers and could be accessible by various users scattered all over different locations. One of the significant components to resolve security challenges is to build an efficient and effective access control model that is based on facial recognition system. A facial recognition system is a technology capable of identifying or verifying a person from a digital image by comparing selected facial features from the given image with faces within a database. The biometric information characteristic of the individual (such as Fingerprint, iris, finger vein, face recognition, voice, hand shape, etc.) is measured through the biometric input device. (Sunghyuck and JungsooHan, 2019). This model is applied to manage access to e-library resources by allowing only authorized users who have been authenticated successfully.

1.1 Statement of Problems

The following are the existing problems that the research work would eliminate:

(i) Illegal access to e-library by an outsider/stranger.

(ii) Presentation of fake/lost items, such as identity card to gain entrance into e-library by an illegal users.

1.2 Objectives of the Research Work

(i) To Identify, verify/ authenticate the student image in order to grant access.

(ii) To implement an access control system using facial authentication approach

2. LITERATURE REVIEW

In most of the various crimes, criminals were taking advantage of a fundamental flow in the conventional access control system: the system do not grant access by “who we are” but by “what we have”, such as ID cards keys, passports, pin numbers or mother’s maiden name. None of these means really define us, rather they are merely means of authenticating. Thus, anybody may duplicate or may acquire these identity means which in turns could be applied in today’s network world, the need to maintain the security of information or physical property is becoming both increasingly important and increasingly difficult from time to time. Most of the Cybercrime issues are related with the problems like security of financial dealings, prohibiting maltreatment of credit card information, providing security for information during online transactions, preserving privacy and confidentiality of e-mails and the attack on privacy. (Rita and Vyas, 2016).

Biometric refers to the measurement of people's distinctive physiological and behavioral characteristics to recognize and categorize the individuals, by comparing correspondence with the templates stored in the database. It has unique ability to identify individuals, it prevents both identity theft and fraud. (Vanitha and Akila, 2020). Authentication is the act of confirming the truth of an attributes of a single piece of data or entity. In contracts with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing’s identity, authentication is the process of actually confirming the identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a website with a digital certificate tracing the age of an artifact by carbon dating or ensuring that a product is what its packaging and labeling claim to be in other words, authentication often involves verifying the validity of at least one form of identification (Eliasson, 2007).

The science and technology of measuring and analyzing biological data is referred to as biometric. Biometrics is that kind of system which can provide more security to user. Any fake trait can capture the characteristics and behaviour of human beings. Every human being has their own unique identity that is why it cannot be easily copied by anyone. There are many biometric security systems available such as iris recognition, fingerprint recognition, face recognition, signature recognition, voice recognition, hand geometry recognition, etc. In biometric security system there is no need to remember passwords or PINs, so there is no chance of stolen or forgotten it, therefore it is more secure system than any other security systems (Shraddha and Choudhari, 2016).

Face recognition system is a computer application for automatically identifying or verifying a person from a digital database of images. It is an important branch of pattern recognition which has many applications like security & surveillance, biometric attendance, image indexing system etc. (Shweta et al, 2014). The future of system security must lie in the ability to authenticate users based in methods that will uniquely identify an individual's securely without relying on the individuals to protect the authentication method. Thus, best solution so far, would be regarded as biometric authentication (Moghaddan, 1998). Face recognition is one of the biometric methods that have the merits of both high accuracy and low intrusiveness. It has the accuracy of a physiological approach without being intrusive. (Manisha et al, 2016).

Face recognition has drawn the attention of researchers in various fields from security, psychology and image processing to computer vision. Numerous algorithms have been proposed for face recognition that is, computing models such as artificial neural networks (ANN) and genetic algorithm (GA) are used for various pattern recognition situations in real life. (Mahendra and Neeraj, 2012). The algorithm produces images that are used as password to authenticate a user access. It is secretly kept in the database and even users may not have the idea on what that password is, user only need to upload their security image so called passport in order to log in for a based library. Some biometrics samples are discussed briefly as follows:

I. Face Recognition - The idea of usage of face for authentications has emerged into face recognition systems. The face is captured using high capacity cameras and is used as a template for matching. Now the template is matched using various pattern matching techniques to identify or verify an individual identity.
II. Fingerprint Authentication-A fingerprint consists of loop, arch and whorl patterns.
III. It appears as a series of dark lines and white spaces, when captured from device. The matching is performed using Minutiae based and the pattern matching.
IV. Iris Recognition: The iris of every individual possesses certain unique characteristics that can be used to distinguish individuals. It is a colored muscular ring around the pupil of the eye which contains inner zone as pupillary zone and the outer zone as ciliary zone whereas the iris lies between cornea and lens of the human eye
V. Retina Recognition This biometric profile is based on the pattern of blood vessel within the retina of human eye. The characteristics generated from the blood vessel pattern is unique and can be used for authentication process.
VI. DNA recognition is an intrusive approach and it needs a form of saliva, blood, semen, hair, tissue sample etc., for authentication process
VII. Keystroke Recognition technology examines key stroke dynamics including time taken by a person to type the password, speed and pressure.
VIII. Signature Recognition- Signature biometric trait comes under the category of behavioral characteristic of human. This approach captures informative details namely direction, speed, pressure of writing and shape of signature

IX. Voice Recognition- every individual has his own vocal characteristics, so it can be adopted as a biometric profile to authenticate an individual's identity, this is known as speech recognition. The sensor records the voice signal and further it will be converted into a unique digital code (template) and processed to recognize the person. (Sunil et al, 2019).

2.1 Facial Biometric System

Humans often use faces to recognize individuals and advancements in computing capability over the past few decades now enable similar recognitions automatically. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Major advancements and initiatives in the past ten to fifteen years have propelled face recognition technology into the spotlight. Face recognition can be used for both verification and identification.

A pixel is generally thoughts of as the smallest single component of a digital image, the definition as highly context sensitive. For example, there can be "printed pixel" in a page or pixel carried by electronic signals, or represented by digital values or pixel on a display device, or pixels in a digital camera (photo sensor elements). This list is of exhaustive and depending on context, there are several terms that are synonymous in particular contexts, such as pel sample, byte, bit dot, spot etc. The term "pixels" can be used in the abstract, or as unit of measure, in particular when using pixels as a measure of resolution such as: 2400 pixels per inch, 640 pixels per line, or spaced and 10 pixels a part. The measures dot per inch (spl) and pixels per inch (ppi) are sometimes used interchangeably but have distinct meanings, especially for printer devices where there is a measure of the printer's density of dot (e.g ink droplet) placement. For example, a high-quality photographic image may be printed with 600ppi on a 1200dpi inkjet printer. Even higher dpi numbers, such as the 4800dpi quoted by printer manufacturers since 2002, do not mean much in terms of achievable resolution. The more pixels used to represent an image, the closer the result can resemble the original.

The number of pixels in an image is sometimes called the resolution, though resolution has a more specific definition pixels counts that can be expressed as a single number as in a "three mega pixel" digital camera. This has a nominal three million pixels, or as a pair of numbers as in a "640 by 480 display", which has 640 pixels from side to side and 480 from a top to bottom (as in a VGA display), and therefore has total numbers of 640 x 480 = 307,200 pixels or 0.3 mega pixels. The pixels or color samples, that form a digitized image (such as a Jpchecle used on a web page) may or may not be in one – to – one correspondence with image. In computing, an image composed of pixels is knows as bitmapped image or raster image. The word rosters originate from television scanning patterns, printing and storage techniques.

Each digital image file stored inside a computer has a pixel value which describe how bright that pixel is, and what color it should be. The most common pixel format is the byte image, where this number is stored as an 8-bit integer giving a range of possible values from 0 to 255 registration taken to be black. During this, it is taken to white through certain algorithm, the image files are dividing into grids; it can be 8 by 8grid or 16 by 16 grids. Each grid is being calculated its pixel value with compression algorithm. All grids pixel value will be transform into a single value with compression algorithm once again. This is how pixel value is being produce and acquire for an image in this authentication method, pixel value will be used as authentication key for a username (Perkins, 2003).

3. METHODOLOGY

During the biometric enrollment process, a digital image of the user's face is captured via a digital camera. This image would be normalized, the distance between the eyes, nose, mouth and chin will be extracted. These are recorded as eigenface and put into storage as a template in a database. During the authentication period, a live image of the same user's face is captured again through digital camera.

Again, the eigenface features would be extracted, this would be compared with the previous template stored in the system. If the result of the comparison is confirmed, the user would be granted access to the system, otherwise, the user would be denied.

4. SYSTEM IMPLEMENTATION

The implementation phase of this project is more concerned with planning the structure of the system to ensure it fulfills its objectives and this is achieved by using object oriented programming, C sharp and sequential very language SQL) server. It invariably means that the coding perspective of building the system provides the blue print for the system and helps provide the platform for the user.

4.1. Hardware and Software Requirement

4.1.1 Software Requirements

The following are required for smooth running of the new system

1. Net framework 3.5 of higher version
2. Sequential query language (SQL) server 2005
3. Windows operating system (at least windows vista installed)
4. Anti-virus package to prevent that application from virus attack

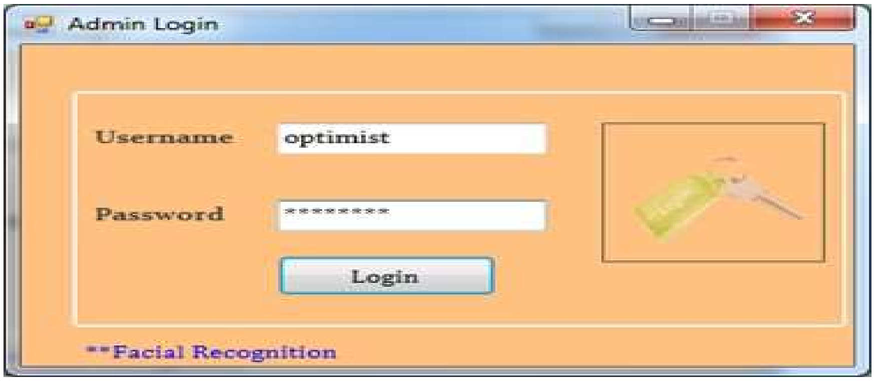
4.1.2 Hardware Requirements

The above listed software will work perfectly with the under listed specification as a computer is not complete without either the software or the hardware

1) 1 gigabyte RAM
2) 1.5GH2 processor
3) Uninterruptible Power Supply (UPS)
4) Mouse and enhanced keyboard
5) i3 laptop (webcam available)

4.2 Implementation Screen Shot

The implementation screen shots of the various phases of the proposed authentication method using digital image processing access control system are shown below



Admin Login

Username: optimist

Password: ********

Fig. 1: Admin Login Page.

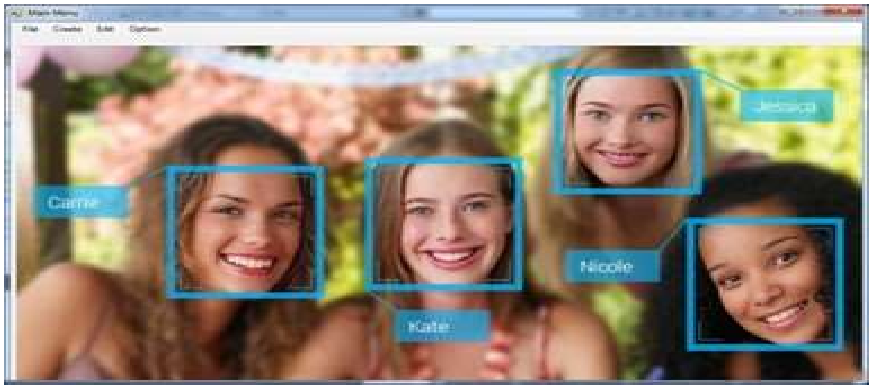
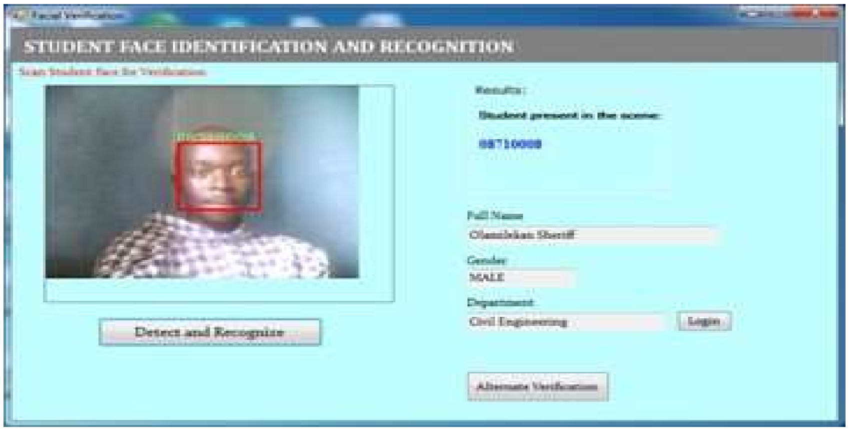


Fig. 2 Admin Main Menu.

The Admin Main Menu is the form that will displayed after a successful login by the administrator.



Facial Verification

STUDENT FACE IDENTIFICATION AND RECOGNITION

Scan Student Face for Verification

Results :

Student present in the scene:

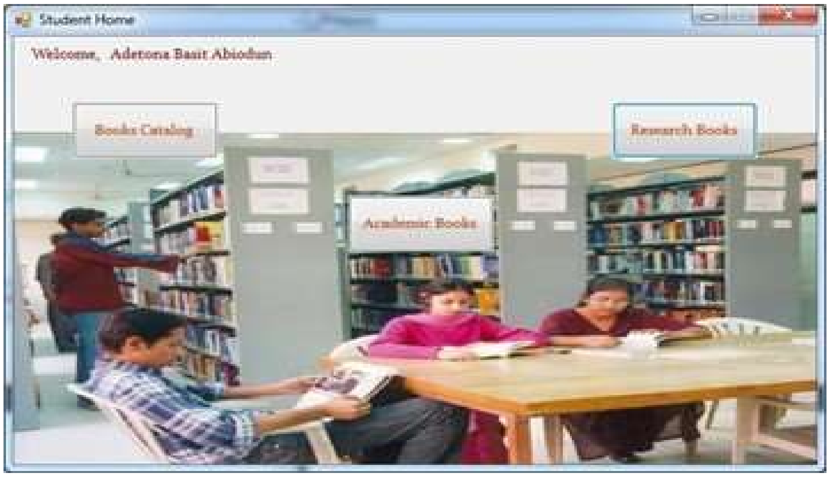
08710008

Full Name: Olamilekan Sheriff

Gender: MALE

Department: Civil Engineering

Fig. 3: Student Face Recognition Form



Welcome, Adetona Basit Abiodun

Fig. 4: E-Library Home

The facial recognition interface is where student face is verified against trained face database. If a face is identified, the application will get the student Full-Name, Gender and Department, and at the same time enable the Login button. But if a student's face cannot be identified, the login button will remain disabled.

After a student have successfully passed the face recognition/identification interface, the student will be redirected to the e-library home, where the student can then have access to some resources of the library

4.3 Evaluation

Table 1 shows a brief comparison between the password and facial biometrics sample.

Table 1: Comparisons between the Password and Facial Biometrics Sample.

	Password	Biometric sample (face)
Speed	High speed	Low speed
Memory Space	Low memory space	Large memory space
Accuracy	Very low	Better accuracy
Realiability	Not reliable	Very reliable
Cost	Not expensive	Costly

5. CONCLUSION

The research work indicated the use of access control based on facial recognition system in e- library and e-exam to prevent unauthorized users from gaining access to resources online. It also defined all the necessary needs and requirements to design/develop an authentication method using digital image processing (face image) for access control applied to. We have therefore achieved the primary goal of this project, which was to use a student's face image as a source of access for an electronic test. We are all witnesses of the fast-growing technology that is changing by the minute so that it cannot be easy to crack, or accessing the library through another user's profile but all interested prospective library users will have to register and follow normal protocol.

REFERENCES

1. Eliasson, C. and Matousek, B. (2007). "Noninvasive Authentication of Pharmaceutical Products through Packaging Using Spatially Offset Raman Spectroscopy". Journal of Analytical Chemistry. Vol.79 (4) pp: 1696–1701. Doi: 10.1021/ac062223z. PMID 17297975.
2. Jing, Q., Zhihong, T., Chunlai, D., Qi, Z, Shen, S. and Binxing, F. (2020). "A Survey on Access Control in the Age of Internet of Things". Journal on Internet of Things. Vol. 7(6), pp: 4682 -4696
3. Lawal, A. Adeniran, O., Akinwale, A. and Folorunso, O. (2011). "A Combined Biometric System approach to users Authentication". International Journal of Research and Reviews in Computer Science (IJRRCS) Vol2 (3) pp 800-805.
4. Mahendra, P.P and Neeraj, K. (2012) "Face Recognition using Genetic Algorithm and Neural Networks", International Journal of Computer Applications Vol 55(4).
5. Manisha, M.K., Debnath, B. and Tai-hoon, K. (2016). "Face Recognition Using Neural Network: A Review", International Journal of Security and Its Applications. Vol. 10 (3) pp: 81-100
6. Moghaddam B., Wasiuddin, W. Pentland, A. (1998). "Beyond Eigenfaces: Probabilistic matching for Face Recognition. IEEE *Int. Conference on Automatic Face & Gesture Recognition, pp: 30-35*
7. Ofodile, J.O., Agbanu, N .A. And Nwankwo, N.G. (2019). "The Use of E-Library Resources as a Correlate of User Satisfaction in University Libraries in Anambra State, Nigeria". International Journal of Social Sciences and Humanities Reviews, Vol.9 (1) p: 103 – 112.
8. Simon, P. and James, T. (2003). "Time -series Novelty Detection using one-class support vector machines: Journal of machine learning research 3, pp: 1333-1356.
9. Prema, N.K., (2014). "Access Control Based on Pixel Value Extraction" International Journal of Innovative Research in Advanced Engineering (IJIRAE) vol 1 Issue 1.pp 45-50.
10. Relly, V and Virgil, P. (2019) "Face Recognition as a Biometric Application". Journal of Mechatronics and Robotics Vol 3(1) pp. 237-257
11. Rita, D. and Vyas, R. (2016). "Cyber Crime: Critical View", International Journal of Science and Research (IJSR) vol 5 (1) pp85-87.
12. Shacham, H and Waters B. (2013). "Compact proofs of retrievability", Journal of CryptologyVol 26 (3) pp442–483.
13. Shraddha, S. G and Choudhari, N.K .A (2016). "Survey Paper On Various Biometric Security System Methods", InternationalResearch Journal Of Engineering And Technology (IRJET)Vol 3(2) pp1279-1281.
14. Shweta, M, Shailender, G., Bharat, B.and Nagpal, C.K. (2014). "Face Recognition using Neuro- Fuzzy Inference System", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.7(1) pp.331-344
15. Silverman Mark, S. L. (2001). A Practical Guide to Biometric Security Technology', IT Professional, 3(1): 27-32.
16. Sunghyuck H., Jungsoo, H. and Guijung, K. (2019) "Security Issues Related to Biometric Security". International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Vol.8 (2) pp: 865-888
17. Sunil, S. H., Balekundri, S.G. and Prashanth, C. R. (2019). "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends", Int. J. Advanced Networking and Applications Vol(10)4 pp: 3958-3968
18. Vanitha, V.C and Akila.D. (2020). "A Survey on Biometric Authentication Systems in Cloud to Combat Identity Theft", Journal of Critical Reviews ISSN- 2394-5125 Vol 7(3) pp: 540-547.