

Device Synchronization Using a Computerize Face Detection and Recognition System for Cyber security

Ayorinde Henry Omopintemi^{a*}, Promise Irebami Ayansola^b, Kehinde Gbemisola Ogundijo^c

^{a,b,c}Computer Science Department, University of Ibadan, Oyo State, Nigeria

^aEmail: Omopintemiayorinde@gmail.com , ^bEmail: payansola@gmail.com, ^cEmail: gbemiogundijo@gmail.com

Abstract

Face recognition system is an application for identifying someone from image or videos. Face recognition is classified into three stages i.e. Face detection, Feature Extraction, Face Recognition. Face detection is an application for detecting object, analyzing the face, understanding the localization of the face and face recognition. It is used in many application for new communication interface, security etc. The face detection algorithm converts the input images from a camera to binary pattern and transverse the face location of candidates using the AdaBoost Algorithm. AdaBoost Algorithm selects the best set of Haar features and implement it in cascade to decrease the detection time. Face recognition is a pattern recognition technique and one of the most important biometrics; it is used in a broad spectrum of applications. The accuracy is not a major problem that specifies the performance of automatic face recognition system alone, the time factor is also considered a major factor in real time environments. Recent architecture of the computer system can be employed to solve the time problem, this architecture represented by multi-core CPUs and many-core GPUs that provide the possibility to perform various tasks by parallel processing.

Keywords: AdaBoost Algorithm; Haar; cascade; Face detection and recognition system (FRDS).

1. Introduction

Face recognition has gained substantial attention over in past decades due to its increasing demand in security applications like video surveillance and biometric surveillance. Modern facilities like hospitals, airports, banks and many more organizations are being equipped with security systems including face recognition capability. Despite of current success, there is still an ongoing research in this field to make facial recognition system faster and accurate. The accuracy of this recognition system strongly depends on the face detection system. This system can successfully detect human face from a given image containing face/faces and from live video involving human presence.

* Corresponding author.

The main methods use for face detection are feature based and image based. Feature based method separates human features like skin color and facial features whereas image based method used some face patterns and processed training images to distinguish between face and non faces. Feature based method has been chosen because it is faster than image based method and its' implementation is far more simplified. Face detection from an image is achieved through image processing. Locating the faces from images is not a trivial task; because images not just contain human faces but also non-face objects in clutter scenes. Moreover, there are other issues in face recognition like lighting conditions, face orientations and skin colors. Due to these reasons, the accuracy of any face recognition system cannot be 100%. Face recognition is one of the most important biometrics methods. Despite the fact that there are more reliable biometric recognition techniques such as fingerprint and iris recognition, these techniques are intrusive and their success depends highly on user cooperation. Therefore, face recognition seems to be the most universal, non-intrusive, and accessible system. It is easy to use, can be used efficiently for mass scanning, which is quite difficult, in case of other biometrics. Also it is natural and socially accepted. Moreover, technologies that require multiple individuals to use the same equipment to capture their biological characteristics probably expose the user to the transmission of germs and impurities from other users. However, face recognition is completely non-intrusive and does not carry any such health dangers.

2. Related Work

Biometrics is a rapidly developing branch of information technology. Biometric technologies are automated methods and means for identification based on biological and behavioral characteristics of an individual. Face detection is the elementary step in the face recognition system and acts as a stone to all facial analysis algorithms. Data is entered into and stored in a computer, it IS generally referred to as information with the move from local application to a web based ones such that data is created and access through the database [1], a database is part of data management system [2] which will undergo some profound changes, many databases that we find on the web today are derived from other databases. [3] it's also a single collection of structured data stored with a minimum duplication of data item so as to provide a consistent and controlled pool of data.[4]. Using the internet service driven network as a new approach to the provision of network computing that concentrates on the services you want to provide as adopted in [5] database has experienced a rapid increase in growth since the development of a rational data base, the progress in database systems and applications has produced a large scope of specialized technology areas that have often become the exclusive domain of research specialists. [6]. Different methods have been employed to secure and protect the shared and sensitive data.[7] However, the significant roles of encryption algorithms are numerous and essential in information security. [8].

The prediction of incoming attacks is achieved in a timely manner which enables security professionals to install defense systems in order to reduce the possibility of such attacks in Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security. [9] .Further information on an intelligent spam-scammer filter mechanism using bayesian techniques [10] was reviewed, It is against this background, that various research has been carried out with the aim of solving detection and preventing such intrusive attacks [10]. The proposition of a two stage hybrid face detection system composed of the probability based face mask pre-filtering and pixel based. [12], also a face detector consist of 4 phase cascade structure

based on MCT-transformed images using the Adaboost learning algorithm [13]. A proposed face detection method is implemented using nine FPGA boards for the Transmogriifier-2 configurable hardware system. [14], also a proposed neural network primarily based face detection on the Virtex-II Pro FPGA[15] and face detection using FPGA for scaling input pictures and mounted-point expressions. [16] A biometric attendance management system was developed to verify the workload performance of an online operation activities [17] and accompany the implementation of a framework on Big Data for extraction of knowledge based [18]. The technical testing of biometric devices and divided it into five subsystems: data collection, signal processing, transmission, data storage, decision [19]. The practical results demonstrated that, the Hybrid Parallel Recognition is the fastest algorithm variant among the all, because it gives an overall speed up around (82) times [20]. The CPU Parallel gives an overall speed up around (71). Finally, the Hybrid Mono gives a little improvement about (1.04). [21]

3. Concepts of Imaging Applications

RGB color Space: RGB color space is the combination of red, green and blue color components. For the 24 bits per pixel, the range of R, G and B varies from 0 to 255. If R, G and B are all 0 then the resulted color will be black. If R, G and B are all 255 then the output color will be white. The concept of the RGB color space is specified in figure 2.4.1. Here the x-axis represents blue color range, y-axis represents green color range and Z-axis represents red color range. As explained above, we can see that black color is represented at the origin and white color is represented at the other corner where red, green and blue are 255 each. Similarly we can have other color values at different corners of cube corresponding to different RGB values.

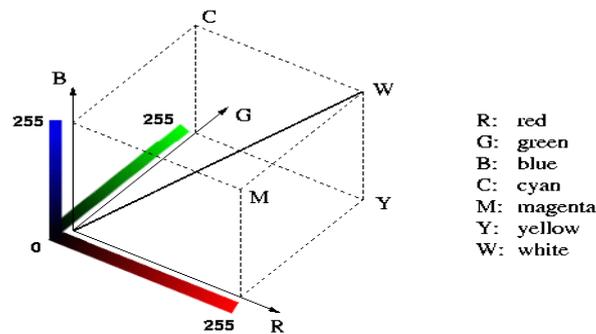


Figure 3.1: RGB color model.

Source Thierry, h. Chang, (2016) pp., 504

A face must be detected to increase the possibility of recognition and speed up the process by choosing one location in the image. To detect a face, two steps must be done before the recognition. The first step is to resize the image to standard size (determine by the administrator),

Decision module: This module accepts or rejects the user depending on the matching score or security threshold.

Figure 1 presents such a system and possible attack points.

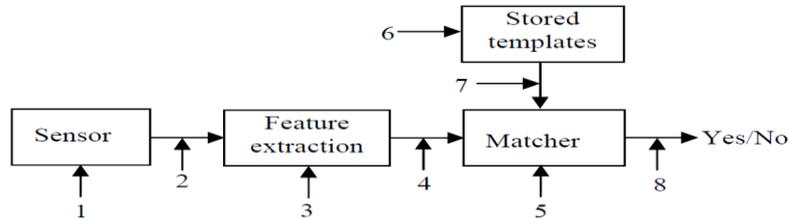


Figure 3.2: Attack points of a biometric system.

Source; Parallel face recognition (2008) pp., 342

4. CPU Parallel Face Recognition

In the parallel face recognition process, two tasks can be done simultaneously. The process of uploading training face images in the memory and the process of getting face features from the training face images. The multithreading capability can be.

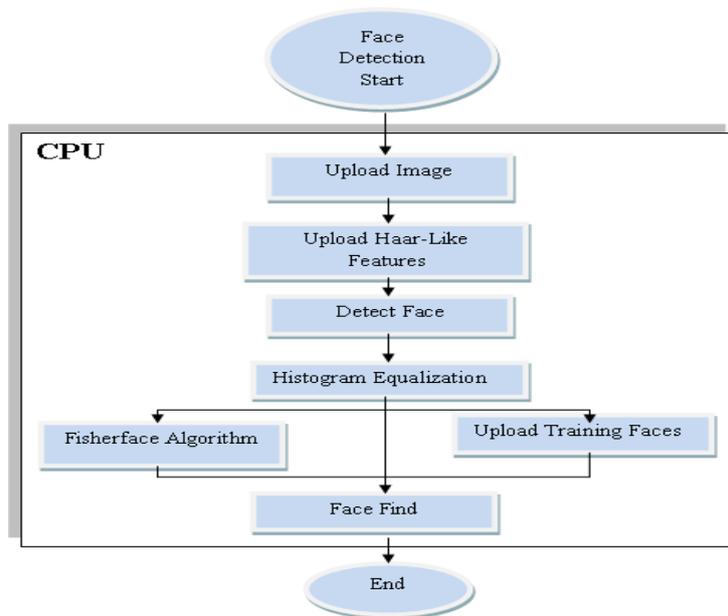


Figure 4.1: CPU Parallel Face Recognition.

Viola-Jones (2008) pp., 607

Hybrid Mono and Hybrid Parallel. Fisherface algorithm is employed to implement recognition phase and Haar-

cascade algorithm is employed for the detection phase. In addition, these implementations are based on industrial standard tools involve Open Computer Vision (OpenCV) version The experiment consists of applying 400 images for 40 persons' faces, defining, training, and recognizing these images on these four variants, the experiment is taken place on the same environment (laptop computer Intel core i7 processor 2.2 GHz, Nvidia GPU GeForce GT 630M, 7GB RAM). The speed up factor is measured with respect to the CPU Mono implementation (the slowest than all other three variants). The practical results demonstrated that, the Hybrid Parallel Recognition is the fastest algorithm variant among the all, because it gives an overall speed up around (82) times. The CPU Parallel gives an overall speed up around. Finally, the Hybrid Mono gives a little improvement about (1.04). Thus, employing parallel processing on modern computer architecture can accelerate face recognition system.

4.1 Program Structure

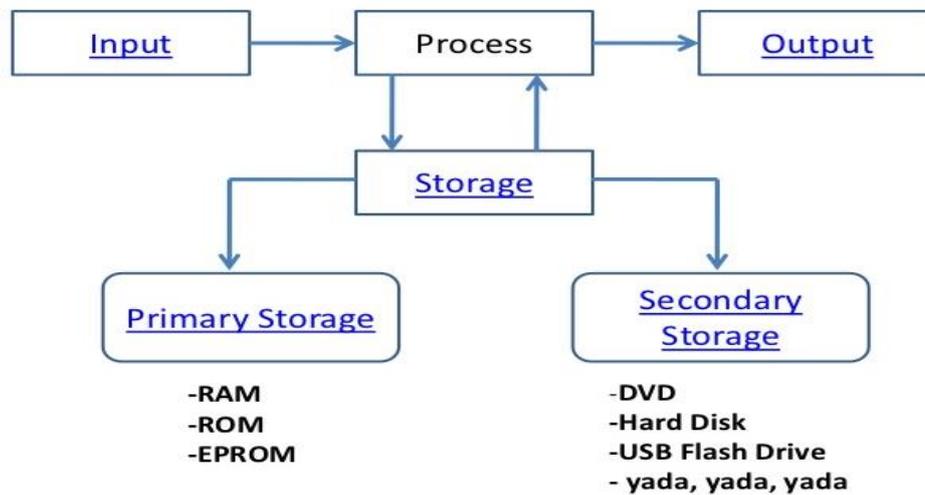


Figure 4.1.1: Program Structure

Source: Wayman (2016) pp., 899

5. Process

This paper dispatch the system architecture that comprise the system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture, collectively these are called architecture description languages (ADLs) Process architecture is the structural design of general process systems and applies to fields such as computers (software, hardware, networks, etc.), business processes (enterprise architecture, policy and procedures, logistics, project management, etc.), and any other process system of varying degrees of complexity. Processes are defined as having inputs, outputs and the energy required to transform inputs to outputs. Use of energy during transformation also implies a passage of time: a

process takes real time to perform its associated action. A process also requires space for input/output objects and transforming objects to exist: a process uses real space. A process system is a specialized system of processes. Processes are composed of processes. Complex processes are made up of several processes that are in turn made up of several processes. This results in an overall structural hierarchy of abstraction. If the process system is studied hierarchically, it is easier to understand and manage; therefore, process architecture requires the ability to consider process systems hierarchically. Graphical modeling of process architectures is considered by Dualistic Petri nets. Mathematical consideration of process architectures may be found in CCS and the π -calculus.

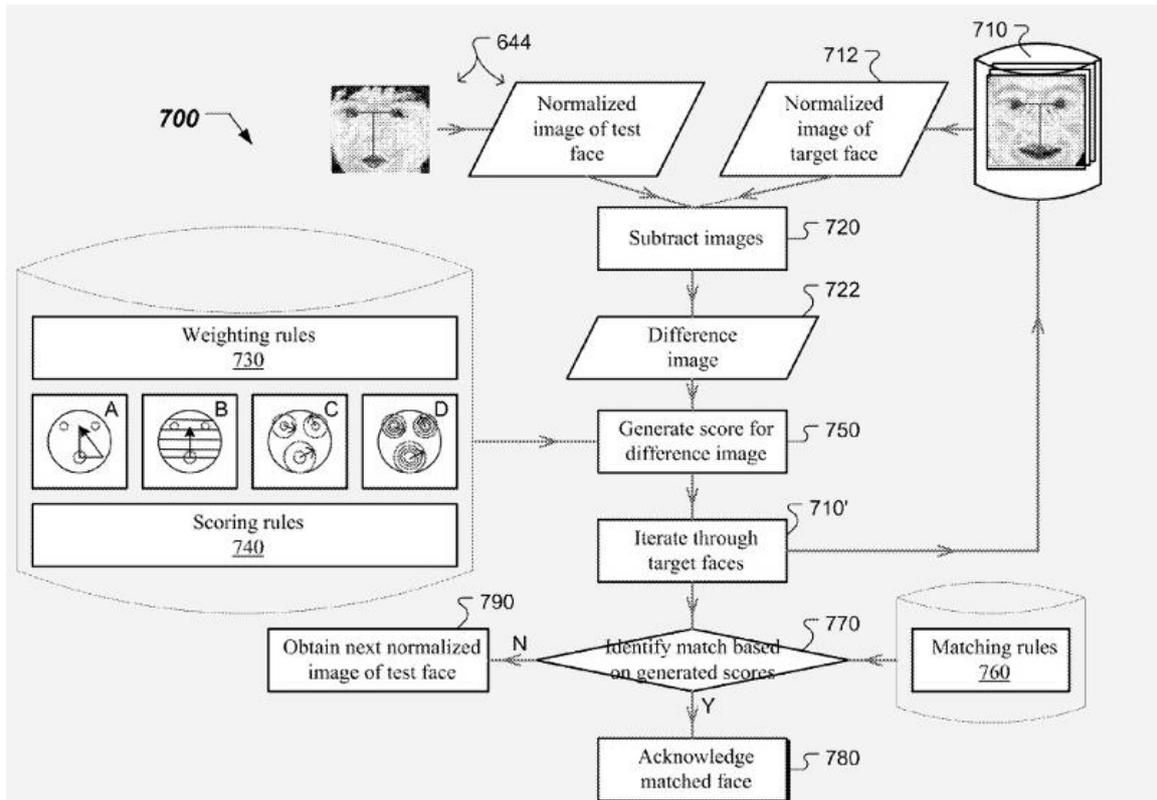


Figure 5.1.1: Process design structure.

Source: Process Architecture (901) pp., 401

5.2 Program Flow Chat/Diagram

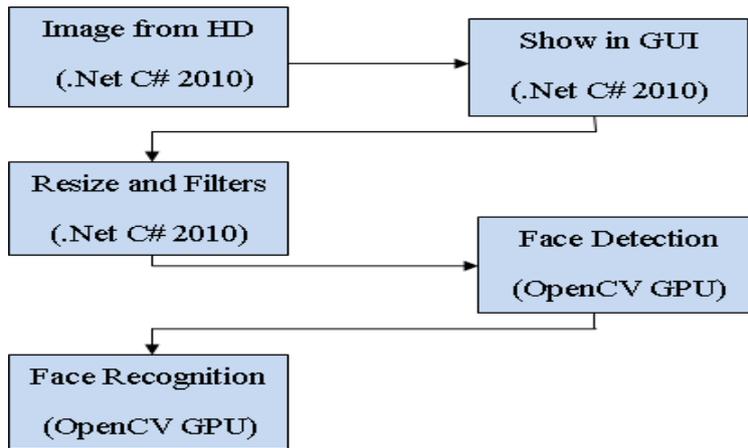


Figure 5.2.1: program flow chat.

6.1.1 Output Specification and Design

The researcher modelled the system by mode and design the system output, and the output design which is a graphical user interface helps the user to operate the system effectively.



Figure 6.1.2: Welcome Screen.

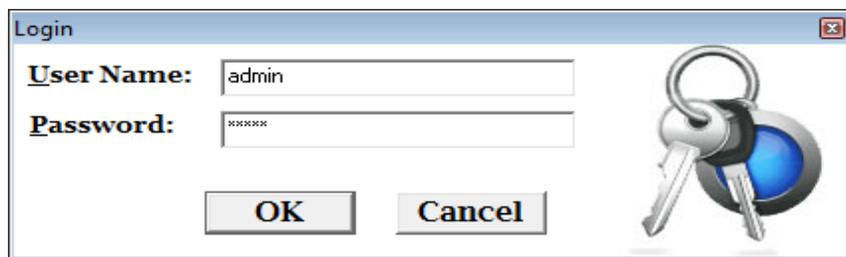


Figure 6.1.3: Login screen.

6.2 Face detection and recognition screen



Figure 6.2.1

The results in this section show the performance evaluation of device synchronization from different FS techniques using a range of classification methods. The evaluation code of each cyber access techniques are explored in Section 6.2.1 by automatically storing the detail of device users to enhance security standard. In the result implementation phase, the project reaches fruition. A critical phase in SLDC is the successful implementation of the system; implementation simply means bringing the new system into operation. Due to our well-written documentation and user training methods developed by the experts will aid the user staff so that they can use the system efficiently and effectively. Firstly install the software and start using. As the software has been implemented for performing all the tasks related to security client information system and as a result it will reduce the complexity at work and enhance cyber security. . There is no absolute solution of cybercrimes but we can do our best by using device synchronization and online work safely.

6.3 System Limitation

There are few limitation while doing effective cyber security in an organization or for personal reasons. The networks are not secure enough as there are many unwanted users who can attack and destruct the interventions and the application of both computer and mobile device need to be updated and tested on regular basis to ensure any kind of attacks. Securing data on applications and network need second layer of security which is very challenging. One must protect their data very highly by two factor authentication so that no one can easily access it. Protecting data 100 percent on cloud is very challenging as its require large amount of innovation and every type of security from login to space, from chat to banking which again require conscious user's involvement. Quite importantly, Cybercrimes is one of the largest crime in today's time. Hackers and thief are like sitting online and watching all data online. Cases like tracking of online banking and personal data is common and most increasing crime. There are data available where we can see daily cybercrime like OTP call, online money transfer, personal information data, etc. Even organization is facing these crimes like leaking

information of their work, project, plans, infrastructure details etc

6.4 Program Pseudo Code

1. Initialization

Select *how to get image*

open file dialog to select image

Create Bitmap → P

Put new image in P

Send P , image-viewer width , height and quality=72

to Resize new image and set its quality 72

Calculate time

Add log →DB

2. CPU part (Face detection)

Load Haar cascades XML and objects → H

H→detect(P)

Create new CPU bitmap P_CPU

Send H.result→ P_CPU

Calculate time

Add log →DB

3. CPU part (Face saving)

If (P_CPU not = empty) then

P_gray→ P_CPU. grayscale

Take face name from GUI P_name

Create image file P_file

P_file→P_gray

P_file.name = P_name + random Numebr

Save P_file in Hard Disk

Calculate time

Add log →DB

7. Conclusion

The accuracy of the system is achieved above 80%. This paper is good for the pictures of people in different races and colors and it is good to detect the frontal faces present in the images files but not able to detect the side-views faces. The failure of detection on the pictures with very dark backgrounds colors are also the limitation of the system just like other systems. Overall it is a good system by which I have gained valuable knowledge of image processing and the steps required for any successful face detection. The advancement can be achieved as the future goal to make most parts of the system automated for surveillance and vision based

applications for cyber security. .

References

- [1] Graham, and A. Pentland, (2001) Eigenfaces for Recognition, *Journal of Cognitive Neuroscience*, vol. 3, no. 1. 2018, pp. 71-86.
- [2] Lane, Williams and .K. Paliwal, (2004) "Fast Principal component analysis using fixed-point M. Turk, A. Pentland, Eigenfaces for Recognition, *Journal of Cognitive Neuroscience*, vol. 3, no 1. 2013, pp. 71-86. [CrossRef]
- [3] Siau (2003) Springer-Verlag, ICBA, Hong Kong, China (2004), pp.724-730.
- [4] French and, M.M. Ahmed, I. Taj, M. Humayun, F. Hameed, (2016) "Design of High Performance FPGA based Face Recognition System", *PIERS 2008 in Cambridge, USA*, 2-6 July, 2008, 2006. pp.1232-1298
- [5] Adeniji, S.D, Khatun, S, Borhan, MA,Raja, RSA , —A design proposer on policyframework in IPV6 networkl. 2008 IEEE International Symposium on Information Technology.Vol 4,pp 1-6 (2008)
- [6] Filippas, J., Amin, S.A., Naguib, R.N.G., and Bennett, M.K. (2000) 'Parallel virtual machine implementation for the image identification of normal and cancerous colonic mucosa'. *Proceedings of the World Congress on Medical Physics and Biomedical Engineering, 'World Congress on Medical Physics and Biomedical Engineering'*. Held 23-28 Jul 2000 in Chicago, USA. 5044-7619
- [7] Breaker, and Hellerstein, (1998) *Elementary Linear Algebra*, ninth edition, Oxford University Press, 1998 pp. 138.
- [8] Logunleko K.B., Adeniji. O.D., Logunleko A.M, —A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Securityl. *International Journal of Scientific Research in Computer Science and Engineering* Vol.8, Issue.1, pp.45-51, 2020.
- [9] Adeniji O.d., Olatunji O.O . —Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security”.*International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 18, No. 3,pp 111- 118 , 2020
- [10] Adeniji O. D , Olubukola Adigun, Omowumi O Adeyemo — An intelligent spam-scammer filter mechanism using bayesian techniquesl*International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 10, No. 3 pp 126, 2012.
- [11] Ukam, J.J, Adeniji O.D.lPerformance Evaluation of Error Rate in Immune Inspired Concepts with Neural Network for Intrusion Detection in Cybersecurity.*International Journal of Advanced Research in Computer and Communication Engineering* Vol. 9, Issue 6,pp 16-22 , 2020.

- [12] Froba and Ernst(2002). "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 5, pp. 93-99, May 2013.
- [13] Guo, Connell J.H., Bolle R.M., (1990) An Analysis of Minutiae Matching Strength, Proc. 3rdAVBPA, Halmstad, Sweden, June 2001, pp. 223-228.
- [14] McCready, J. P. Hespanha, and D. J. Kriegman, (1998) "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 1997, pp. 711-720.
- [15] Sadri etal, K.K. Paliwal (1997), "Fast Principal component analysis using fixed-point algorithm",
- [16] Wei etal (2003)., Impact of artificial "gummy" fingers on fingerprint systems, in Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677 of Proceedings of SPIE, pp. 275 289
- [17] I.R. Idowu & O.D. Adeniji Performance Evaluation and Analysis of Biometric Workload Attendance Management System Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech. Vol. 6, No. 2. Pp 47-56 , 2018.
- [18] Eze Chika Victor, Adeniji Oluwashola David, —Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure To Curb Forgery MenaceINTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,pp. 66-70. , 2014.
- [19] Wayman (2007), J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. no. 7, 1997, pp. 711-720.
- [20] X. He, S. Yan, Y. Hu, P. Niyogi, and H. Zhang, "Face Recognition Using Laplacian taces", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 3, 2005, pp. 328-340.
- [21] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 1997, pp. 711-720.