DESIGN AND IMPLEMENTATION OF A FACIAL DETECTION AND RECOGNITION SYSTEM FOR DATA SECURITY

Daniel A[1]., Suleiman, I.A[2]

[1]Department of Computer Engineering, Faculty of Engineering, Edo State University Uzairue, Km7, Auchi-Abuja Road, Iyamho-Uzairue Edo State, Nigeria

[2]Department of Agricultural & Bioenvironmental Engineering, School of Engineering Technology, Auchi Polytechnic, Auchi, PMB 13, Auchi, Edo State.`

ABSTRACT

Face recognition has emerged as a powerful and intriguing image-processing application, experiencing rapid advancements over the past 30 years. This research paper presents a comprehensive face recognition system that effectively locates faces in images, compares them with an existing database, and subsequently identifies the individual, if present. The system relies on pre-stored sample images in a designated database, enabling thorough searching and comparison. The proposed face recognition system employs an Image Search method, which calculates a unique digital signature for each image based on its contents. When an input image containing a face is provided, the system calculates its signature and compares it with the signatures of pictures in the search directory. This comparison is facilitated by calculating the distance between the input image's signature and those of the photos in the directory. The smallest space indicates the closest match, and the corresponding image is displayed at the output alongside the detected face and the individual's name. In cases where no match is found, the system displays a "no match" message, indicating that the individual is not in the database. This innovative face recognition system offers a robust and efficient approach to identifying individuals through advanced image processing and digital signature techniques, paving the way for enhanced security and authentication applications.

Keywords*: Face Recognition, Image Processing, Digital Signature, Image Search Method, Database Comparison*

1. INTRODUCTION

A face recognition system is an application for identifying someone from images or videos. Face recognition is classified into three stages, i.e.) Face detection, Feature Extraction, and face Recognition (Singhal *et al.,* 2022). The face detection method is a difficult task in image analysis. Face detection is an application for detecting an object, analysing the face, and understanding the localisation of Face and Face recognition. It is used in many applications for new communication interfaces, security etc. Face Detection is employed for detecting faces from images or videos. The main goal of face detection is to see human faces from different photos or videos. The face detection algorithm converts the input images from a camera to a binary pattern and, therefore, the face location candidates using the AdaBoost Algorithm (Wilson and Fernandez, 2006, Xie et al., 2011). The proposed system explains the face detection-based system on AdaBoost Algorithm. AdaBoost algorithm selects the best set of Haar features and implements them in a cascade to decrease the detection time. The proposed plan for face detection is intended to use Verilog and Model Sim and be implemented in FPGA (Anton, 2015, Cukic and Bartlow, 2009, Jafri and Arabnia, 2009).

Face Detection System to detect the face from images or videos. To see the face from a video or image is gigantic. Now face detection is in vital progress in the real world (Jafri and Arabnia, 2009). In face recognition systems face detection is the primary stage (Raju et al., 2022). Figure 1 shows the various stages of face recognition system before face detection, feature extraction and recognition.

Face recognition is a pattern recognition technique and one of the essential biometrics used in a broad spectrum of applications (Lih-Heng et al., 2010, Ratha et al., 2001). 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. The contemporary architecture of the computer system can be employed to solve the time problem; this architecture is represented by multi-core CPUs and many-core GPUs that provide the possibility to perform various tasks by parallel processing. However, harnessing the current advancements in computer architecture is not without difficulties. Motivated by such a challenge, this research proposes a Face Detection and Recognition System (FDRS). This research provides the architectural design, detailed design, and four variant implementations of the FDRS (Jain et al., 2005, Lih-Heng et al., 2010, Ratha et al., 2001).
Face recognition has gained substantial attention in past decades due to its increasing demand in security applications like video and biometric surveillance (Qiang et al., 2022). Modern facilities like hospitals, airports, banks and other organisations have security systems, including face recognition capability. Despite the current success, there is still ongoing research in this field to make facial recognition systems faster and more accurate. The accuracy of any face recognition system strongly depends on the face detection system. A face detection system can successfully detect human faces from a given image containing faces/faces and live video involving the human presence (Goel et al., 2022). The stronger the face detection system, the better the recognition system. The main methods used these days for face detection are feature- and image-based. The feature-based way separates human features like skin colour and facial features.

In contrast, the image-based approach uses some face patterns and processed training images to distinguish between faces and non-faces. The feature-based method has been chosen because it is faster than the image-based method, and its implementation is far more simplified. Face detection from an image is achieved through image processing. Locating the faces from photographs is not trivial; images contain human faces and non-face objects in cluttered scenes. Moreover, face recognition has other issues like lighting conditions, look orientations and skin colour. Due to these reasons, the accuracy of any face recognition system cannot be 100% (Roberts, 2007, Runarsson, 2011, Sajid et al., 2008).

Face recognition is one of the essential biometrics methods. Even though 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 (Martins *et al.*, 2022). Therefore, face recognition seems to be the most universal, non-intrusive, and accessible system. It is easy to use and can be used efficiently for mass scanning, which is quite difficult in the case of other biometrics. Also, it is natural and socially accepted (Sajid et al., 2008).

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 entirely non-intrusive and carries no health dangers (Sharma and Paliwal, 2007).

Biometrics is a rapidly developing branch of information technology. Biometric technologies are automated methods and mean for identification based on an individual's biological and behavioural characteristics (Sharma and Paliwal, 2007). There are several advantages of biometric technologies compared to traditional identification methods. To take adequate measures against increasing security risks in the modern world, countries are considering these advantages and are shifting to new-generation identification systems based on biometric technologies (Spacek, 2008, Wayman, 2017).

Biometric systems are becoming an essential element (gateway) for information security systems. Therefore biometric systems themselves have to satisfy high-security requirements. Unfortunately, producers of biometric technologies do not always consider security precautions. In publications regarding biometric technologies, the drawbacks and weaknesses of these technologies have been discussed. Since biometrics form the technology basis for large-scale and susceptible identification systems (e.g. passports and identification cards),

the problem of adequate evaluation of the security of biometric technologies is a current issue (Spacek, 2008, Wayman, 2017).

Also, some other face detection and recognition system issues are on individuals with identical faces, like identical twins and others. In a situation like this, the system can make a mistake or error in processing the person's image to grant access to the rightful user. This project aims to design and implement a face detection and recognition system. This system will reduce the fraudulent activity rate as it can track registered users and grant them access upon face recognition completion. This study aims to increase security efficiency, and this research work will help the users maintain data (Wilson and Fernandez, 2006, Xie et al., 2011). Also, the knowledge that would be obtained from this research will assist the management to grow; also, this research work will help the upcoming researcher in this field of study both with the academic students on their research.

2. RESEARCH METHODOLOGY

2.1 SYSTEM ANALYSIS

System analysis can be described as the process in which the existing system is improved upon; it is a computer breakdown of the system into its operations to understand the procedure thoroughly. This enables the easy point out of the places where improvements are needed.

2.2 SYSTEM ANALYSIS AND DESIGN

System Analysis is a detailed study of the various operation performed by a system and their relationship within and outside of the system. The analysis begins when the user or manager begins studying the program using the existing system. Here the key question is what all problems exist in the present system? What must be done to solve the problem?

Data collected on the various files, decision points and transactions handled by the present system are analysed. The commonly used tools in the System are Data Flow Diagrams, Interviews, etc. Training, experience and common sense are required to collect relevant information to develop the system. The system's success depends largely on how clearly the problem is defined, thoroughly investigated and properly carried out through the solution choice. A good analysis model should provide the mechanisms of problem understanding and the solution's framework. Thus it should be studied thoroughly by collecting data about the system. Then the proposed system should be analysed thoroughly following the needs. System analysis can be categorised into four parts.

i. Information gathering
ii. Apply analysis tools for structured analysis
iii. Feasibility study
iv. Cost/Benefit analysis

2.3 PROPOSE NEW SYSTEM

Face detection and recognition is the first semi-automated system. At this time, it uses body parts or features (ear, eyes, nose, and mouth) for detection; face detection system can be capable of detecting frontal view faces of human in real-time. The new system aims to develop software to recognise or see faces instead of typing passwords.

2.4 SYSTEM DESIGN

With analysis, this shows that the old existing system needs to be automatic.
The design of the new system will be made in a way that a casual and novice user will be able to handle; the proposed system aims to improve on the existing system to create an effective, fast detective of face recognition, making the system to be able to identify the owner and to create the system to be in automatic recognition of faces.

3. METHOD OF DATA COLLECTION

Data collection and information-gathering procedures are outlined and analysed here. Data was carefully collected and objectively evaluated to define and ultimately provide solutions to the problems on which the research work is based.

During the research work, data collection was carried out in many places. The top multi-marketing firm was visited in Kaduna, Kano and NCC (Nigeria Communication Commission) in Abuja, which deals with high-level security.

Direct interactions with security personnel helped in the data collection. Forms were also given to members of staff; samples of the form include;

i. Name (optional)_____
ii. Position_____
iii. Profession_____
iv. Clearance level_____

I.e. do you have access to all the rooms in the building?

v. Clearance type _____

i.e., what guarantees you entering a second room or office?

vi. Limitation using the clearance the type_____
vii. Advice_____

3.1 FEASIBILITY ANALYSIS/STUDY

The feasibility study is the study of the impact on the organisation of developing a system. The effect can either be positive or negative. The system is considered feasible when the positives dominate the negatives (Zhang, 2005). Here are the feasibility studies that can be performed in technical and economic feasibility.

3.2 FILE MAINTENANCE ERROR HANDLING MODULE

The researcher took time to design an error-handling module for the new system design, an algorithm on how errors will be tracked down to handle exception cases. This module design operates exceptions in sequence so that each of the units tries to take the mistake, which, if all the teams cannot hold it, runs as an outbound error

3.3 SYSTEM CONFIGURATION

For the effective and efficient functioning of the system being designed, the minimum requirements for both hardware and software have to be considered; the details are shown below:

3.3.1 HARDWARE REQUIREMENTS

A computer system will be used as a local server to enable the website's hosting on a personal computer. This system will have the following configuration:

i. Hard disk drive 100gig
ii. Ram 2gig
iii. Processor 1.50ghz

3.3.2 SOFTWARE REQUIREMENT

i. Eclipse IDE 2019
ii. Jdk7n above
iii. Web camera max 2.0
iv. Java development kit

3.3.3 LANGUAGE CHOICE

During the development of this program, the research used Java Language. This language was chosen due to the object oriented nature of it, also the language runs best on the Windows OS platform. They are used to ensure an effective program.

3.3.5 CHOICE OF THE ENVIRONMENT

Microsoft visual studio 2012 integrated development environment was used to develop the program using the SAP report extension. Among all other java Language development environments, the Studio 2012 environment is one of the best and suits the nature of this program.

3.4 SYSTEMS/PROCESS ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines a system's structure, behavior, and views. An architecture description is a formal description and representation of a system, organised in a way that supports reasoning about the designs and behaviours of the System (Zhao et al., 2016).

The system architecture can comprise system components, the externally visible properties of those components, and the relationships (e.g. the behaviour) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall design. There have been efforts to formalise languages to describe system architecture; collectively, these are called architecture description languages (ADLs).

Process architecture is the structural design of general process systems. It applies to fields such as computers (software, hardware, networks, etc.), business processes (enterprise architecture, policy and procedures, logistics, project management, etc.), and any other complex process system.

Processes are defined as having inputs, outputs and the energy required to transform information into outcomes. The 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 processing system is a specialised system of processes. Processes are composed of processes. Complex processes comprise several methods that are, in turn, made up of several techniques. This results in an overall structural hierarchy of abstraction. If the processing system is studied hierarchically, it is easier to understand and manage; therefore, process architecture requires considering process systems hierarchically. Dualistic Petri nets consider graphical modelling of processor architectures. Mathematical consideration of process architectures may be found in CCS and the π-calculus.

Process Design Structure

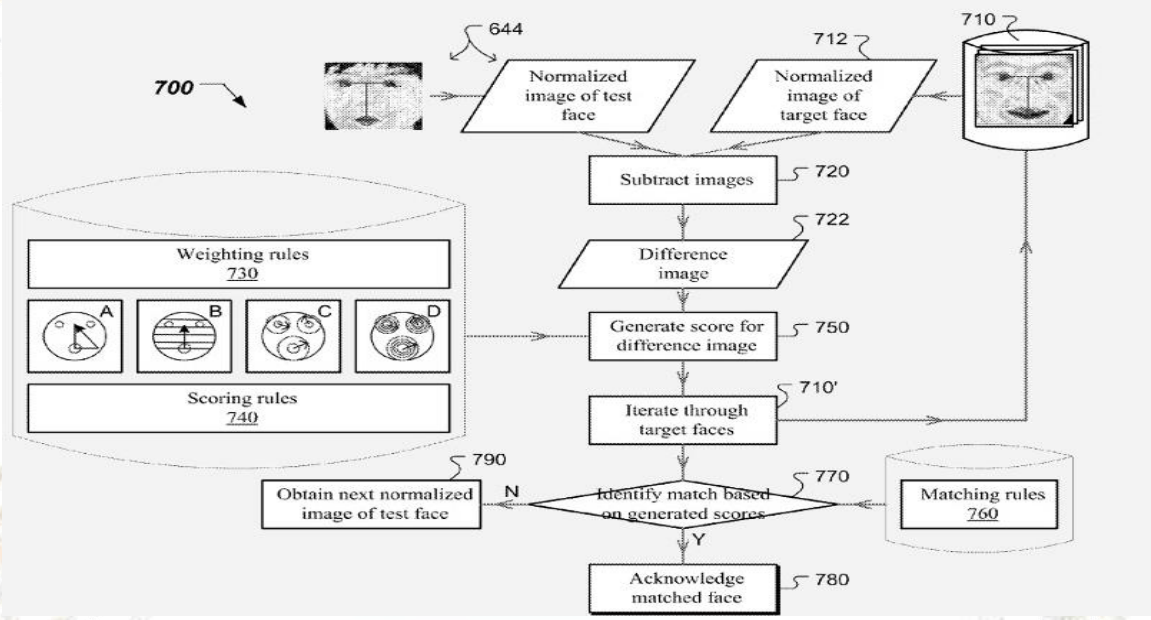

Figure 1: Process design structure.

3.5 COMPONENTS OF THE SYSTEM MODEL

The internal architectural design of computers differs from one system model to another. However, the primary organisation remains the same for all computer systems. The following five units (also called "The functional units") correspond to the five basic operations performed by all computer systems.

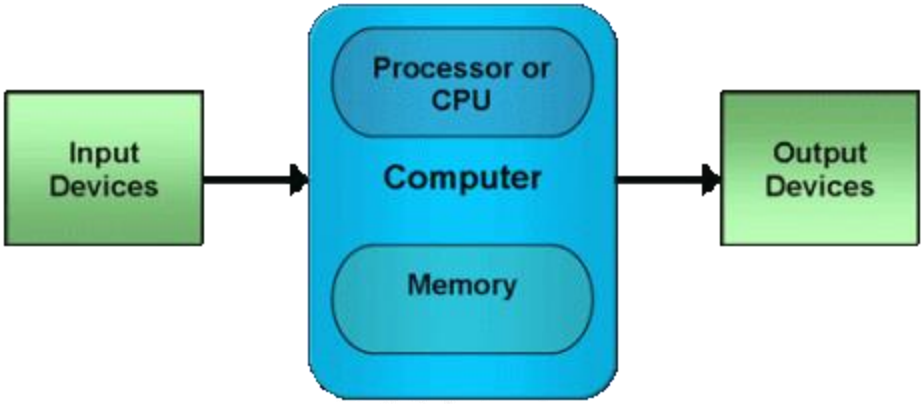

Figure 2: System Model

3.6 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language (UML), activity diagrams are intended to model computational and organisational processes (i.e. workflows). Activity diagrams show the overall flow of control. In FDRS, the main activity is the training phase, and the other is the recognition phase. The activity diagram for the training phase is shown in Figure 1, and the corresponding steps' activities are tabulated in Table

i. Similarly, the activity diagram for the recognition phase is shown in Figure 2, and the corresponding steps' activities are tabulated in the Table.
ii. Also, the pseudo-code for the training and the recognition phases are shown in Figure 3 and Figure 4, respectively.

3.7 PROGRAM STRUCTURE

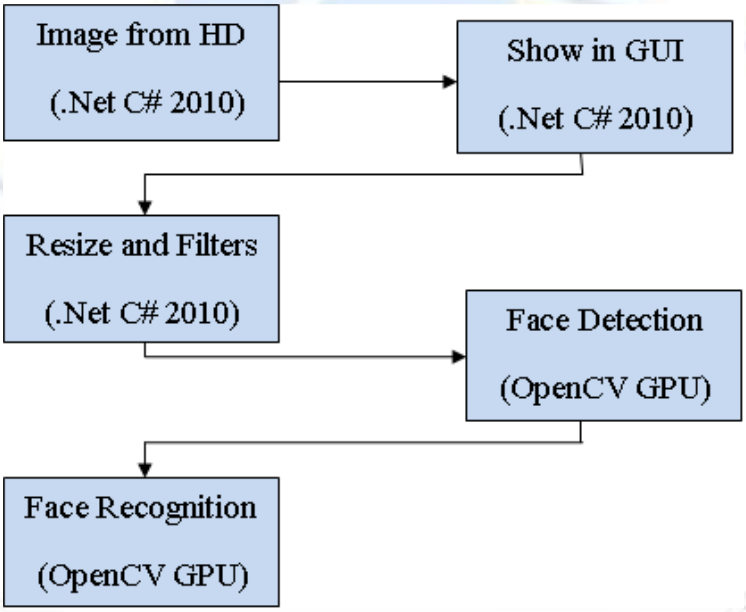

Figure 3: Program flow chat

3.8 DATABASE IMPLEMENTATION

In the implementation phase, the project reaches fruition. A critical stage in SLDC is the successful implementation of the system; performance means bringing the new system into operation. Our well-written documentation and user training methods developed by the experts will aid the user staff in using the system efficiently and effectively. Firstly install the software and start using it. As the software has been implemented for performing all the tasks related to the client information system, it will reduce the complexity at work.

3.9 SYSTEM FLOWCHART

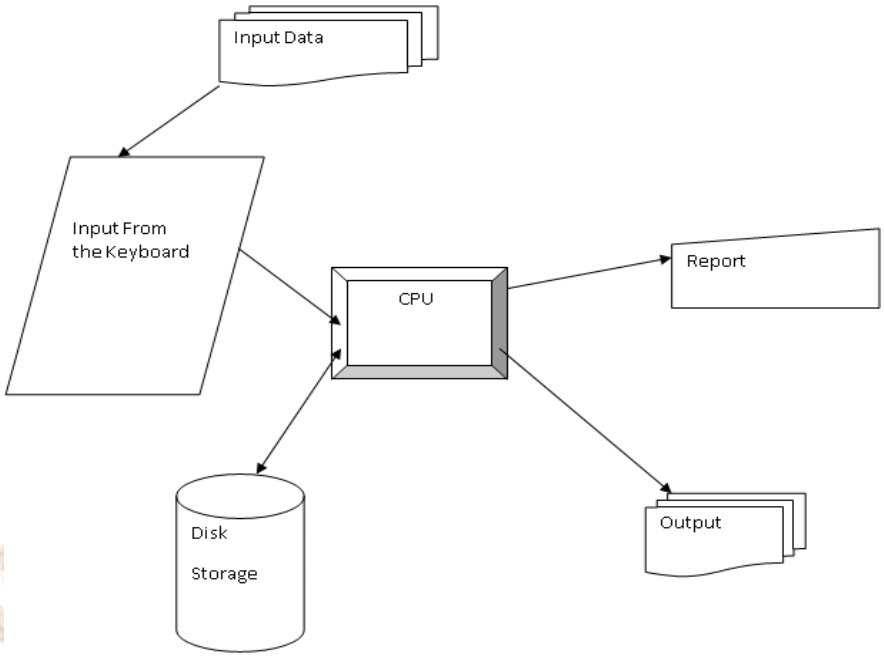

Figure 4: System Flowcharts

3.9.1 DESCRIPTION OF THE NEW SYSTEM

Face detection is the process of finding the human face from an image and, if present, returning its location of it. It is a particular case of object detection. Objects can be anything in the picture, including human and non-human things like trees, buildings, cars and chairs. But, other than humans, objects are least likely utilised in advanced applications. So, finding and locating the human face in the image is an exciting and essential application of modern times. However, locating the beginning is not an easy task in the picture since images do not contain only faces but other objects too.

Moreover, some scenes are very complex, and filtering unwanted information remains tough. When the face's presence and location are found, this information is utilised to implement more sophisticated applications such as recognition and video surveillance. Hence, the success of these applications depends heavily on the detection rate of the image face detection system. Image-based and feature-based methods can do face detection from an image. Image Based methods treat the whole image as a group of patterns, so each region is classified as face or non-face. In this method, a window is scanned against the parts of the image. On every scan, the output is computed, and the threshold value is compared with the output value of the window on the current part of the image. If it is above the threshold value, then that current part of the image is considered the face. The size of this window is fixed and chosen according to some experiments with the help of training image size. The advantage of image-based methods is the higher percentage of face detection hit rate; however, it is slow in terms of computation as compared to feature-based methods. Eigenfaces and neural networks are two examples of image-based approaches. In feature-based forms, features such as skin colour, eyes, nose and mouth are separated first from the rest of the image regions. With the extraction of these features, the non-interested regions of the image are not required to process further; therefore, the processing time is significantly reduced. In feature-based methods, the skin color pixels are separated first because the color processing is faster, resulting in the separation of other features. The feature-based methods' advantage is the fast results but less accurate than image-based methods. Another advantage is the ease of implementation in real-time applications.

In the project, the feature-based method is implemented. The initial step is to get the image as input, and then a feature-based algorithm is applied to detect the face or faces. Once the face region is determined, mark the boundary around it next.

3.9.2 SYSTEM ARCHITECTURAL STRUCTURE/FRAMEWORK

This section describes the architectural design of FDRS, involving: the Mono (sequential) and Parallel face recognition concepts.

Face recognition is the most complex algorithm because it has many steps before it starts the actual recognition. 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 a standard size (determined by the administrator), apply some filter to increase the quality and convert the image into a compatible form. Next, go to detection face, so the vision required to recognise is uploaded in the memory with an Extensible Markup Language (XML) file to detect a face. Finally, go to the recognition step. In recognition, the extracted face will be compared with training faces when uploading to memory and extracting face features by a recognition algorithm.

Any operating system (OS) has multiple ways to deal with a process for different structures. Some functions have a single thread, and others have multithreaded architecture (threads can run simultaneously).

3.9.3 EVERY BIOMETRIC SYSTEM IS COMPOSED OF FOUR MAIN MODULES:

i. **Sensor module**: A sensor acquires the biometric characteristic of an individual and makes a digital description of it.
ii. **Feature extraction module**: The input sample is processed, generating a compressed template image. A template is stored in a database or a smart card.
iii. **Matching module**: This module compares the presented biometric sample with the template. In identification mode, the given characteristic is matched with many templates and generates many matching scores. In verification mode, only one matching is performed, resulting in only one matching score.
iv. **Decision** module accepts or rejects the user depending on the matching score or security threshold.

3.9.4 System And Possible Attack Point

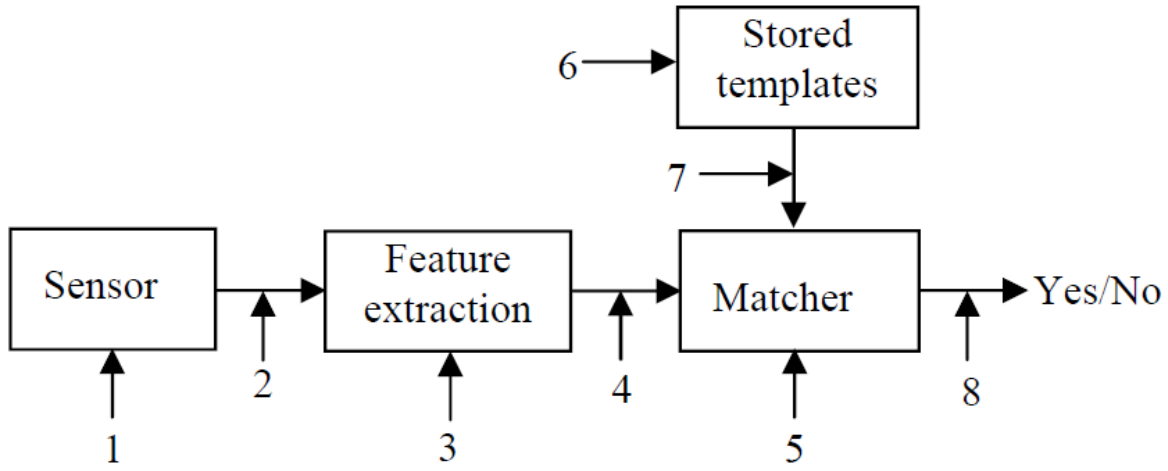

Figure 5: Attack points of a biometric system

(Ratha et al., 2001), Identify eight attack points in this scheme. Let us shortly describe the characteristics of these attacks denoted by numbers i-viii:

i. Presenting a fake biometric sample to the sensor: A fake biometric sample such as a phoney finger, an image of a signature, or a face mask is given to the sensor to get into the system.
ii. A replay of digital biometric signals: A stored call is replayed into the system, ignoring the sensor—for instance, a replay of an old copy of a fingerprint image or a recorded audio signal.
iii. Denial of feature extraction: The imposter forms a feature set using a Trojan horse attack.
iv. Spoofing the biometric feature: Features extracted from the input signal are replaced by fake features.
v. Attacking matching module: Attacks on the matching module result in the replacement of matching scores by fake ones.

vi. Spoofing templates in the database: The database of saved templates can be local or distant. The attacker tries to fake one or more biometric templates in the database. As a result, either a fake identity is authorised, or a rightful user faces a denial of service.

vii. Attacking the channel between the template databases and the matching module: Stored templates are transmitted through a communication channel to the matching module. An attacker can change data in the channel.

viii. Attacking the final decision process: If the hacker can insert or block the final decision, then the authentication system function will be overridden.

ix. A system's structure, architecture, production or implementation may introduce a vulnerability to the biometric system. In some cases, a secondary procedure may be integrated into the biometric system, which possibly makes the biometric system vulnerable.

There are five points of vulnerabilities:

i. Operating systems;
ii. Database management systems (and application software);
iii. Biometric application software;
iv. Software for sensor;
v. Hardware and drivers.

Other primary aspects can be categorised as follows:

i. Management of operations;
ii. Control of parameters (especially FAR/FRR parameters);
iii. System configuration.

CPU Parallel Face Recognition

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

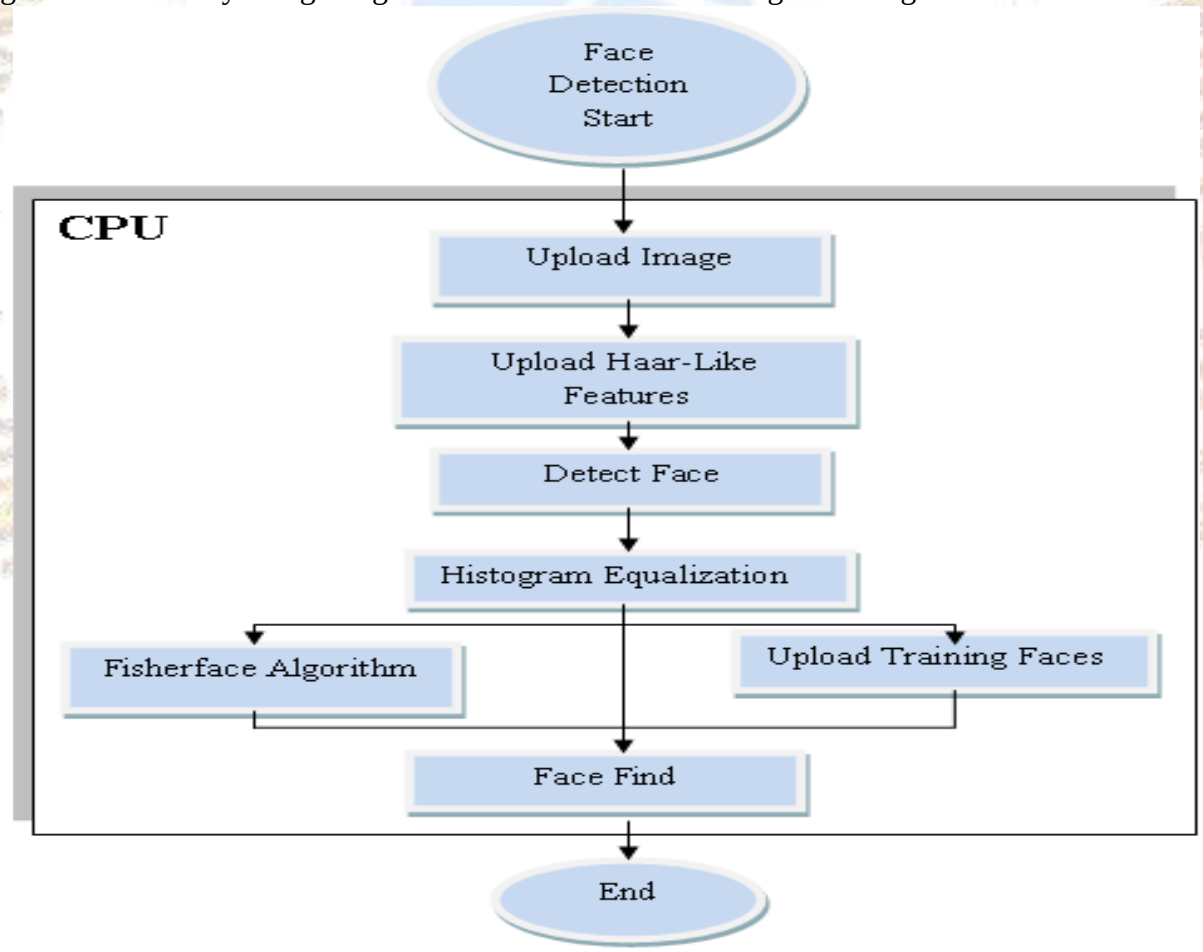

Figure 6: CPU Parallel Face Recognition

3.9.5 SYSTEM FLOWCHART

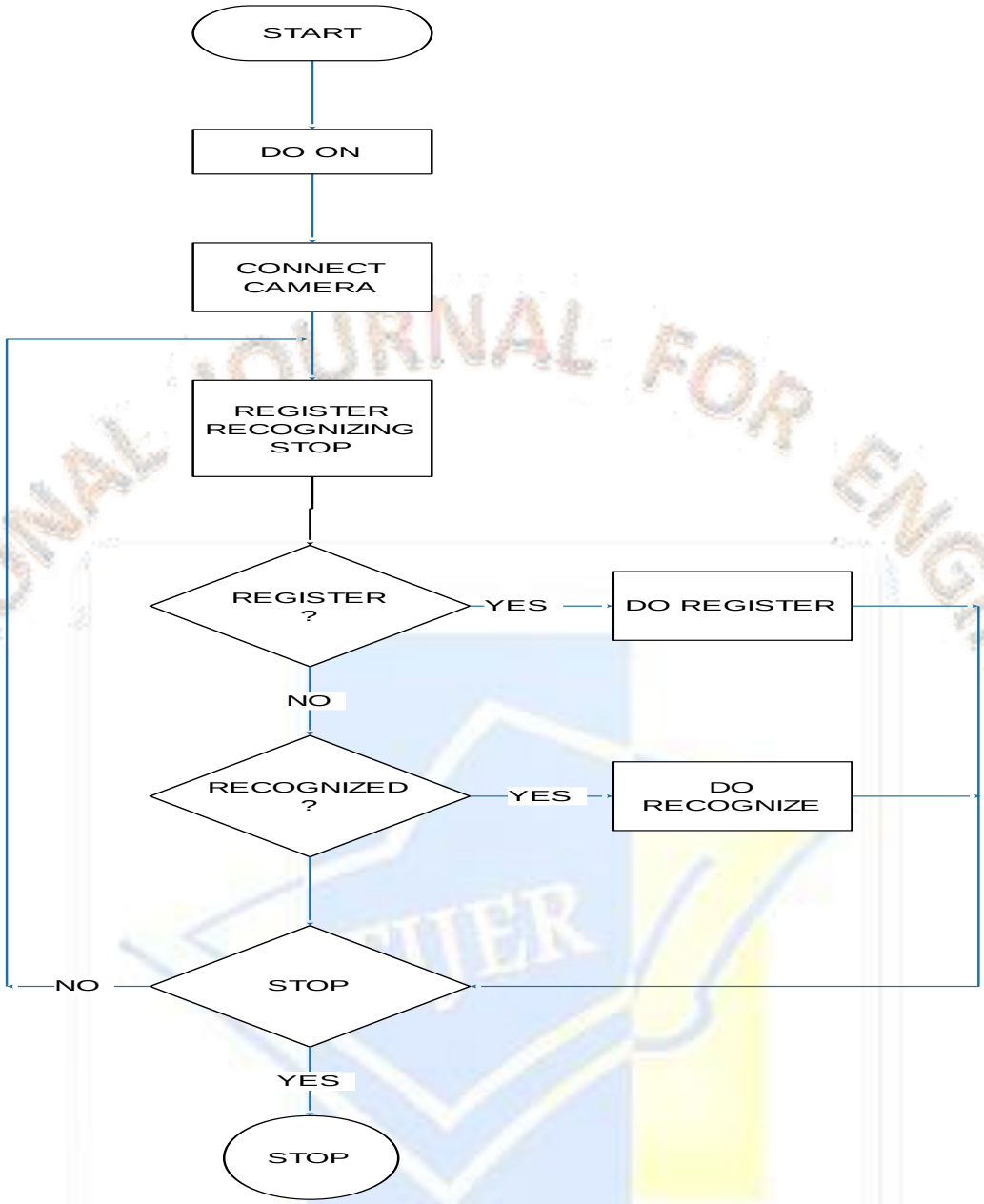

Figure 7: program flowchart

4. RESULT AND DISCUSSION

4.1 SYSTEM DEVELOPMENT

The system development is a life cycle (SDLC) or software developed in systems engineering and the methodologies that people use to develop these systems in software engineering; the SDLC concept underlines many kinds of software development methodologies, which is in the form of framework for planning and controlling the creation of an information system. This system is developed using HTML (Hypertext makeup language, JavaScript, PHP and MYSQL. To view this program, you must have a local host installed in your computer system. The program can be launched using a Wamp server with available software and hardware.

4.2 SYSTEM IMPLEMENTATION

Implementation is the stage of a project during which the theory is turned into practice. All the system programs are loaded onto the user's computer during this phase. It is expected at the end of this implementation that, the system application will have a functional application that people can use in their various systems.

4.3 OVERVIEW OF THE WEB PAGE

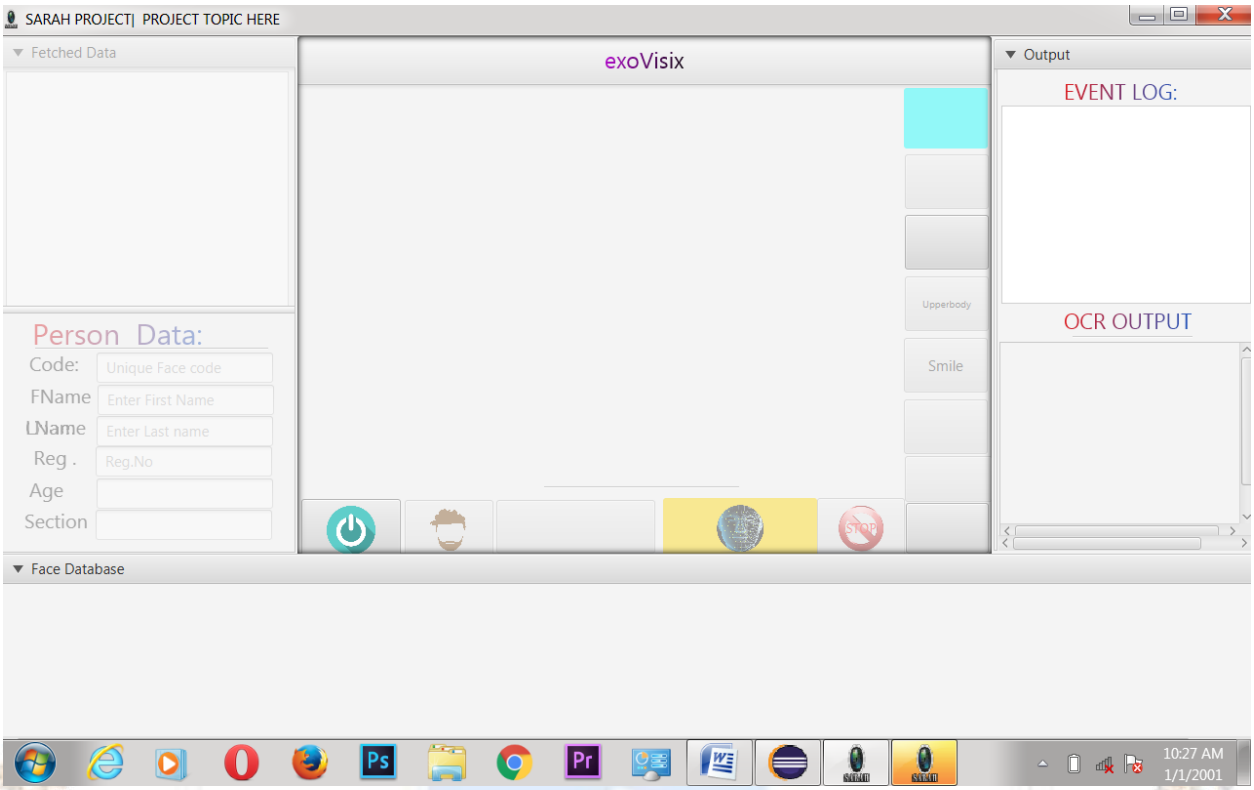

Figure 8: Login page

4.4 SYSTEM TESTING

Testing is the process of detecting errors. Testing performs a very critical role in quality assurance and ensuring software reliability. The results of testing are used during maintenance also. Testing often aims to demonstrate that a program works by showing that it has no errors. The primary purpose of the testing phase is to detect the errors that may be present in the program. Hence, one should not start testing to show that a program works, but the intent should be to show that a program doesn't work. Testing is the process of executing a program to find errors.

Here entire computerised banking system has been tested against requirements of the project have been satisfied or not. Here the whole software system is tested. The reference document for this process is the requirements document, and the goal as to see if software meets its requirements.

4.5 SYSTEM DOCUMENTATION

User guide

For the user to start and use the system, the instructions below must be followed to set up a system

1. Install your webcam max camera if not on System
2. Install the Webcam max report SAP On the System
3. Install OCT.DELL file Also
4. Double-click the program to install and run
5. Setup the installation directory and files
6. log in to the system using user authentication (admin and login) as login details.
7. Perform your operation

5. CONCLUSION

The image face detection is implemented first, and then the same system is used to detect from video sources. The recognition system has also been implemented on the image files. The accuracy of the system is achieved above 80%. The project is good at pictures of people of different races and colours. The project is suitable for detecting the frontal faces in the image files but cannot see the side-view faces. The failure of detection on pictures with very dark backgrounds and colours is also the system's limitation, just like other systems. Overall,

it was a good project by which I gained valuable knowledge of image processing and the steps required for successful face detection. The advancement can be achieved as the future goal to automate most parts of the project for surveillance and vision-based applications. At the end of this research work, the researcher finds this work exciting and recommends it to any security information management institute; also, the researcher recommends that for any other work to be carried out on this topic, the current researcher should consider adding a real-time facial recognition and voice detection to enhance the security level of this system.

REFERENCES

Anton H., C. Rorres, (2015) *Introduce three more components, ninth edition, Oxford University Press, pp. 138.*

Burden R. L. and J. D. Faires, *Numerical analysis, seventh edition,* Thomson, *ISBN: 981-243-106-3.*

Cukic B., Bartlow N. (2009*) The Vulnerabilities of Biometric Systems – An Integrated Look at Old and New Ideas, RGE Color, Technical Report, West Virginia University*, 2005.

Goel, Y., Gupta, I., Rani, P., & Singh, A. K. (2022). A Facial Recognition and Detection System using openVC.

Jafri R. and Arabnia, H. "*A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol. 5, No. 2, pp. 41-68, June 2009.*

Jain A. K., Ross A., Uludag U., *Biometric template security: challenges and solutions, in Proceedings of the European Signal Processing Conference* (EUSIPCO '05), Antalya, Turkey, September 2005.

Lih-Heng C.; Sh-Hussain S. and Chee-Ming T. *"Face Biometrics Based on Principal Component Analysis and Linear Discriminant Analysis", Journal of Computer Science, Vol. 6, No. 7, pp. 693-699, 2010.*

Martins, P., Silva, J. S., & Bernardino, A. (2022). Multispectral Facial Recognition in the Wild. *Sensors*, *22*(11), 4219.

Qiang, J., Wu, D., Du, H., Zhu, H., Chen, S., & Pan, H. (2022). Review on Facial-Recognition-Based Applications in Disease Diagnosis. *Bioengineering*, *9*(7), 273.

Raju, K., Chinna Rao, B., Saikumar, K., & Lakshman Pratap, N. (2022). An Optimal Hybrid Solution to Local and Global Facial Recognition Through Machine Learning. *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, 203-226.

Ratha N.K., Connell J.H., Bolle R.M., *An Analysis of Minutiae Matching Strength, Proc. 3rdAVBPA,* Halmstad, *Sweden, June 2001, pp. 223-228.*

Roberts C., *Biometric attack vectors and defenses, Computers and Security, vol. 26, no. 1, pp. 14–25, 2007.*

Runarsson K. "*A Face Recognition Plug-in for the PhotoCube Browser", M.Sc. thesis, Reykjavik University, December 2011.*

Sajid I., M.M. Ahmed, I. Taj, M. Humayun, F. Hameed, (2013*) "Design of High Performance FPGA based Face Recognition System", PIERS 2008 in Cambridge, USA, 2-6 July, 2008.*

Sharma A., K.K. Paliwal, *"Fast Principal component analysis using fixed-point algorithm", Pattern Recognition Letters, Elsevier*, vol. 28, no. 10, 2007, pp. 1151-1155.

Singhal, P., Srivastava, P. K., Tiwari, A. K., & Shukla, R. K. (2022). A Survey: Approaches to facial detection and recognition with machine learning techniques. In *Proceedings of Second Doctoral Symposium on Computational Intelligence: DoSCI 2021* (pp. 103-125). Springer Singapore.

Spacek L., "*Collection of Facial Images: Faces94", http://cswww.essex,ac.uk/mv/allfaces/ (May 31, 2008).*

Wayman J.L., (2017) *Technical Testing and Evaluation of Biometric Devices, and database in A. Jain, et. al, Biometrics – Personal Identification in a Networked Society, Kluwer Academic Publisher, 1999*.

Wilson P. and Fernandez J. *"Facial Feature Detection using Haar Classifiers", The Journal of Computing Sciences in Colleges,* Vol. 21, No. 4, pp. 127-133, April 2006.

Xie, S. J.; Yang J.; Park, D. S. ; Yoon, S. and Shin, J. *"State of the art in biometrics" in Iris Biometric Cryptosystems*, Yang, J. and Nanni, L., Eds., InTech, , *Croatia, pp. 179-202, July 2011.*

Zhang R., h. Chang, "*A literature survey of face recognition and reconstruction technique", Technical report, University of Texas*, December, 2005.

Zhao W., R. Chellappa, P. J. Phillips, and A. Rosenfeld, *"Face Recognition: A Literature Survey", ACM Computing Surveys, vol. 35, no. 4, 2016, pp. 399-458.*