

FACE BASED ACCESS CONTROL SYSTEM FOR DOCUMENT IDENTIFICATION

Oni, E. O

Department of Computer Engineering,
Villanova Polytechnic Imesi-Ile,
Osun State Nigeria
opson2k5@gmail.com,

Oketoyan, R.B

Department of Computer Engineering,
Villanova Polytechnic Imesi-Ile,
Osun State Nigeria
oketoyanruth81@gmail.com,

Abstract

The need for controlling the access of unauthorized users to data and information on personal computers in industries and organizational systems has been done using different methods in the past ranging from cards, passwords, one-time passwords but the complaints from people; forgetting the passwords, hacking of passwords, losing the cards etc. brought the new idea of using biometric recognition which facial recognition is an example. This research work uses facial recognition as a means of controlling access to data and information, The 'FaceAuthApp' developed uses Microsoft Visual C# as the User interface programming language, SQLite database manager because it suits its offline purpose and the need for persistence which is one of the goals of the application to store the data while EmguCV, a .NET wrapper for Open CV shall be used for the facial detection. For document identification, the administrator who logs in will upload documents which will be accessible only to pre-registered users and give a wrong entry error in case of wrong input or face not detected. The system when fully deployed can be used to control access to classified document in an organization. It can also be used by single user to restrict different authorized and unauthorized user from viewing personal document.

Keywords: Biometric; Database; Passwords; Microsoft Visual

A. Introduction

Security management is the identification of an organization's assets (including people, buildings, machines, systems and information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets (ISO/IEC 13335-1:2004).

An organization uses such security management procedures as asset and information classification, threat assessment, risk assessment, and risk analysis to identify threats, categorize assets, and rate system vulnerabilities so that they can

implement effective controls (Trinabrata Das). According to Schatz et al (2017), computer security, cyber security or information technology security (IT security) is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include passwords, biometric scans, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization (Margaret, 2018). There are two mode of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Access control systems provide the essential services of authorization, identification and authentication (I&A), access approval, and accountability) where:

- i. authorization specifies what a subject can do,
 - ii. identification and authentication ensure that only legitimate subjects can log on to a system access approval grants access during operations, by association of users with the resources that they are allowed to access), based on the authorization policy,
 - iii. accountability identifies what a subject (or all subjects associated with a user) did
- Facial recognition is a category of biometric software that maps an individual's facial features mathematically and stores the data as a face print. The software uses deep learning algorithms to compare a live capture or digital image to the stored face print in order to verify an individual's identity. High-quality cameras in mobile devices have made facial recognition a viable option for authentication as well as identification (Margaret, 2019).

B. Literature Review

Access Control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected; the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication (Affendi: Coursehero).

Access control is generally considered in three steps: identification, authentication, and authorization. Identification is an assertion of who someone is or what something is.

Authentication is the act of verifying a claim of identity. There are three different types of information that can be used for authentication, something you know: things such as a PIN, a password, or your mother's maiden name. Something you have: a driver's license or a magnetic swipe card. Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans (Turner, 2016). Authorization, After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization.

Types of Access Control

The main types of access control are:

- i. **Discretionary access control (DAC):** An access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.
- ii. **Role-based access control (RBAC):** A widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions - executive level, engineer level 1 - rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.
- iii. **Rule-based access control:** A security model in which the system administrator defines the rules that to govern access to resource objects. Often these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and role-based access control to enforce access policies and procedures.
- iv. **Attribute-based access control (ABAC):** A methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions (Margaret, 2018).

Authentication Methods

- i. **Passwords:** It is the most common form of system identification and authentication mechanism, A password is a protected string of characters that is used to authenticate an individual, Password should be properly guaranteed, updated, and kept secret to provide and effective security (wikibooks)
- ii. **One-Time or Dynamic Passwords:** It is a token based system used for authentication purposes where the service is used only once, It is used in environments that require a higher level of security than static password provides

- iii. Cryptographic Keys: Uses private keys and Digital Signatures, Provides a higher level of security than passwords
- iv. Memory Cards: Holds information but cannot process them, More secure than passwords but costly. E.g.: Swipe cards, ATM cards
- v. Biometrics: Verifies an individual's identity by analyzing a unique personal attribute or behavior. It is the most effective and accurate method for verifying identification. It is the most expensive authentication mechanism

Biometric Recognition

Biometric recognition is the automated method of identifying a person based on their physiological characteristics. Those physiological characteristics can include biometrics such as fingerprints, finger veins, palms, retinas, irises, faces and voice (*Jain et al, 2008*). Biometrics is better than RFID card credentials, but historically the cost has limited the growth of these systems (*Bob, 2016*). New systems have recently been introduced that are less expensive and yet quite effective. They are also networking attached, making them very easy to install. The IP biometric reader integrates nicely with IP camera systems, and is now part of the overall safety and security system.

Challenges of Facial Recognition Systems

Overcoming the challenges of Facial recognition as explained above, several steps can be taken to optimize security, performance, and user experience.

- i. Automate capture of high-quality images: Software that automates capture of facial images analyzes the streaming video frames in real time. Image capture is automatically triggered once focus, facial positioning, lighting, and other image-capture details are verified for compliance with quality standards.
- ii. Perform robust liveness detection: Liveness detection algorithms distinguish between a printed, digital, video, and a live facial image. Passive liveness detection looks for indicators of a non-live image such as inconsistent features between foreground and background. Active liveness detection prompts the user to blink or shake his or her head to ascertain liveness. The combination of active and passive methods will yield the highest performance matching. Facial recognition analysis applications might also leverage a second modality such as voice to help assure liveness.
- iii. Use high-performance algorithms: In the past few years, machine learning algorithms have become the predominant method for automatically extracting the above information and then comparing it against other images.

Merits of Facial Recognition System

- i. It offers easy storage of templates in database.
- ii. It reduces the statistic complexities to recognize face image.
- iii. It involves no physical contact with the system.
- iv. It is more secured and convenient
- v. It is easy and safe to use also user friendly system
- vi. It saves time in accessing documents.

Demerits of Facial Recognition System

- i. Facial traits change over time.
- ii. Uniqueness is not guaranteed, for example, in case of identical twins.
- iii. If a candidate face shows different expressions such as light smile, then it can affect the result.
- iv. It requires adequate lighting to get correct input

C. Methodology

Design of Face Based Access Control System

The system design phase is the phase at which the system analysis is transformed into a physical design and this usually involves different aspects such as:

- i. Object oriented design (OOD)
- ii. Database design
- iii. System flowchart
- iv. Interface design.

Unified Modelling Language for Face Based Access Control System

A very useful tool for object-oriented design is the UML (Unified Modelling Language) which is an industry standard tool for describing object orientation in form of analysis and design.

Database Design of Face Based Access Control System

One of the goals of any application is persistence and as such, we will need a database manager to help us stick with the rules. In this project, the researcher chose to make use of the SQLite database manager, primarily because it best suits this project for its offline purpose and also its robustness in managing BLOB (**B**inary **L**arge **O**bject) which shall be used to store the actual face in a pictorial format. The database has just one table named "faces" with four columns.

Face Based Access Control System Flowchart

A flowchart is a diagrammatic representation of an algorithm, a workflow or process. According to Wikipedia, flowcharts are used in designing and documenting simple processes or programs. Like other types of diagrams, they help visualize what is going on and thereby help understand a process and perhaps also find less-obvious features within the process, like flaws and bottlenecks.

Document access flowchart, is the platform that allows the user to access the uploaded documents. The user shows face in the camera, view documents otherwise, access is denied and then tried again. When face is detected and scanned through the open face database, if authorized, then access is granted to

The user authorization flowchart, allows the admin to supply its login details and if found to be correct grant an access for face to be scanned, trained, stored in the open face database. If face is not detected or not well shown due to poor illumination, it allows the face to be scanned again then trained and store up in the database.

It allows the admin to train more faces for new users and store it all up in the face database for authentication.

The document upload flowchart describes the only activity that differentiates the admin from the user in the faceAuthApp. After the admin has correctly filled in its details, the admin is permitted to upload document and store it in the locked folder. It allows two options in uploading the document: copy file and move file. Copy file option will allow the copied file to be accessed outside the faceAuthapp while the move file option will completely move the file from the source to the faceAuthapp and will not allow access to the file outside the faceAuthapp.

Face Based Access Control System Implementation

The aim of all meaningful software is to create a usable product that will be implemented and put to use or at least simulating the real world to solve a particular problem. Thus, the analysis and conceptual design of the application (system) is often followed by the actual development of the application (system).

Face Based Access Control System Documentation

System documentation is one of the most important aspects of software development. It is a written report of the entire operations of the designed and implemented program. Improper documentation of the system architecture will bring about difficulty when changes have to be implemented to the system functionality by another programmer. Unless the program modules are initially well written and adequately documented, maintenance is an extremely unattractive past time. The production of documentation must be seen as the writing of code itself. Provision of documentation is one of the greatest points to differentiate between amateur and professional programmers.

Face Based Access Control System Requirement

The system requirement for the development of this program include

- i. Hardware specification
- ii. Software specification

Hardware Specification

The system will require the following hardware components

- i. A complete computer set of at least Dual Core with a reasonable and size able hard disk space of at least 160GB and a RAM Size of at least 2GB.
- ii. External camera for system without inbuilt camera.
- iii. Shareable resources such as printer, scanner, etc. standard keyboard, Microsoft compatible mouse, UPS devices and VGA Color monitor.

Software Specification

The system will require the following software

- i. Microsoft windows 7 or later versions.
- ii. Visual Studio 2010 or later.

System Testing and Debugging

Writing code for a program is not enough to validate the program in other to check whether it produces the correct result. Testing represents the ultimate review of specification design and implementation which is the process of executing a program with the fore-knowledge of locating errors.

Installing the program from the control environment to the operational environment is to produce error, a successful test locates those errors, so that it is able to perform the designated task programmed to run. Testing the program after coding would check if these are functional:

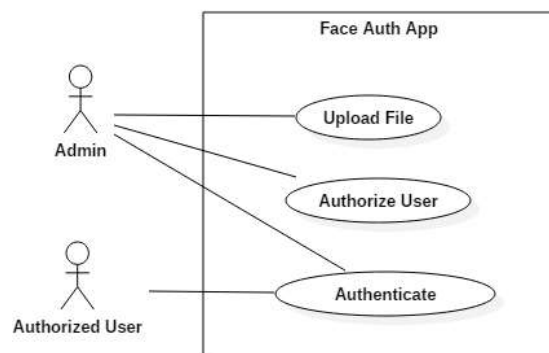
- i. Accurate performance of control function
- ii. Sound communication of data between each of the subprogram
- iii. Definite execution of each component program.

D. Evaluation of the Face Based Access Control System

Evaluation of the face based access control system was done using parameters such as:

- i. The error rate (False Acceptance Rate and False rejection rate).
- ii. Size of the software
- iii. Memory consumption
- iv. Speed of authenticating
- v. Scanning accuracy

There are basically two actors that exist in the modeling of the application, and the actors are the administrator and authorized Users of the application. Both users can access the documents in the locked folder only by passing their face through the camera for authentication while only the Administrator can upload files and store them in the locked folder automatically by the system providing an interface for copying or moving files from the selected source to the destination path, as well as authorizing Users who may have access to the locked files also. Use Case Modeling was used in the analysis.



Use Case Diagrams for Face Auth Access App

Summary of Face Based Access Control System

It is essential to note that the application seeks to secure documents which are placed in a folder, and for such documents in the folder to be secure, there is need to lock such

folder. The application readily locks the folder where all the files are kept, unless an authorized user successfully gains access to the application; in this case, the application unlocks the folder, so as to permit access to those files in the folder.

The user gains access to the documents by authenticating the face with the supplied parameters of ID and Name, if these parameters match with the face of the user, then the user is granted access to the files, otherwise, the user is denied access to the documents. In order to authorize a face or upload documents, the administrator is the only allowed personnel that can authorize face or upload documents, hence, the administrator enters the login parameters to upload documents and then proceeds to train the face in case of authorizing a User.

Face Based Access Control System Evaluation Results

Using the parameters listed in chapter three, the face based access control system was evaluated and it was realised that the error rate is been determined by the illumination of the environment. If the environment is well illuminated it will work accurately in scanning the face of the user and also authenticate the right user. The size of the software is 159MB which is good enough for system based software and for easier installation on systems. The memory consumption is based on the number of users been authorized by the user which is saved in the face database. Speed of authenticating a user for accessing a file is also accepted to be good for optimal performance and the Scanning Accuracy is also evaluated to be accurate enough for controlling the access documents.

E. Conclusion And Recommendation

Conclusion

In an environment where the usage folders and files are essential, it is imperative to secure such files in a way that it is inaccessible to an external user who has not been granted access. While it is easy to crack passwords and in fact, the probability of forgetting passwords are so high these days, it is not that easy, if possible at all to break through a secure system by the means of human characteristics such as the face, Iris, fingerprint to list a few.

It is usually quite difficult to try out something new especially something that may require a higher cost of computation than what it used to be but Clients who will use the application should be keen on being up to date in the area of technological advancements by harnessing the functionalities that this application provides.

This project can be a stepping-stone to a greater feat, which is achievable through a wider range of thinking using the developed application as the basis for an even better application. No single application is perfect, there is always an improvement. Conclusively, authorization and authentication require a higher computing functionality such as the processing power CPU, the RAM, the secondary storage because the human characteristics in the case of this project, the face of the User, has to be trained and stored in the database.

Recommendation

The system when fully deployed can be used to control access to classified document in an organization. It can also be used by single user to restrict different authorized and unauthorized user from viewing personal document.

References

1. Aneem Komachi 2009: <https://faceattendance.blogspot.com/2009/12/>
2. Blick_Maestro: <https://www.coursehero.com/file/39331854/10-Disadvantages-Of-Biometricsdocx/>
3. Bob Mesnik 2016: <https://www.linkedin.com/pulse/fingerprint-facial-recognition-access-control-jensen-gooduun-lion->
4. Dr. Affendi: <https://www.coursehero.com/file/p49gu12/Access-mechanism-Access-to-protected-information-must-be-restricted-to-people>
5. Foreman, P: Vulnerability Management, page 1. Taylor & Francis Group, 2010. ISBN 978-1- 4398-0150-5
6. <https://biometrictoday.com/10-advantages-disadvantages-biometrics-technology/>
7. https://en.wikibooks.org/wiki/Fundamentals_of_information_systems_security/access_control_systems
8. "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A (eds.). *Handbook of Biometrics*. Springer. pp. 1–22. ISBN 978-0-387-71040-2. Archived from the original on 9 March 2011.
9. ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
10. Margaret rouse 2018: <https://searchsecurity.techtarget.com/definition/access-control>
11. Margaret Rouse 2019: <https://searchsecurity.techtarget.com/definition/biometrics>
12. Prof. Hena Vedi: https://www.academia.edu/31640996/BIOMETRICS_A_Seminar_Report
13. Ramya: <http://www.m2sys.com/blog/biometric-hardware/advantages-biometric-identification-management-system/>
14. S. Obaidat, Mohammad & Rana, Soumya & Maitra, Tanmoy & Giri, Debasis & Dutta, Subrata. (2018). Biometric Security and Internet of Things (IoT). 10.1007/978-3-319-98734-7_19.
15. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law*. 12 (2). ISSN 1558-7215
16. TrinabrataDas: <https://rbu.academia.edu/TrinabrataDas>
17. Turner, Dawn M. "Digital Authentication: The Basics". *Cryptomathic*. Archived from the original on 14 August 2016. Retrieved 9 August 2016.