www.ijecs.in

International Journal Of Engineering And Computer Science
Volume 8 Issue 8 August 2019, Page No. 24805-24813
ISSN: 2319-7242 DOI: 10.18535/ijecs/v8i08.4332

Biometric Authentication System Using Face Geometry

Ibebuogu Chinwe C[1] , Philip Seth[2] and Anyaduba Obiageli J[3]

[1,2]Department of Computer Science, Imo State University, Owerri, Nigeria.
[3]ICT Department, Alvan Ikoku Federal College of Education, Owerri, Nigeria

Abstract

This paper deals with biometric authentication, using human facial geometry as the login verification parameter. Biometric is the measurement and statistical analysis of human's unique physical and behavioral characteristics by mapping face geometry, fingerprints, iris, and voice. The aim of this paper is to develop a functional Biometric Authentication System Using Face Geometry as the authentication method. Facial Geometry Authentication is a category of biometric technology that maps an individual's facial features mathematically and stores the data as face-prints in a database. Meanwhile the objective of this paper is to improve data access security, enhance identification accuracy, and contribute to the improvement of the existing facial recognition systems, focusing mainly on increasing its accuracy performance. On the other hand, hacking into users' privacy, loss of confidential information, and high running costs, among others geared the motivation to develop a biometric authentication system using face geometry. Furthermore, the software engineering methodology adopted in this paper is the Structural System Analysis and Design Methodology (SSADM). The software is developed in Visual C-sharp, and the database in SQL Server 2012; using Microsoft Visual Studio 2012 as the integrated development environment. Besides, OpenCV 2.4.8 library is used for image processing, image mapping, and computer vision. The expected result of this paper include: improved user data security, and increased efficiency in facial detection/recognition.

Keywords: Biometric, Authentication, Facial Geometry, Password, Security, Technology.

1.0 Introduction

Biometric (life and metric) is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. Meanwhile, Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. These identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to face geometry recognition, fingerprint, palm veins, DNA, palm print, hand geometry, iris recognition, and retina.

Furthermore, a facial geometry system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from a given image with faces within a database. Most facial geometry systems function based on the different nodal points on a human face. The values measured against the variable associated with points of a person's face help in uniquely identifying or verifying the person. With this technique, applications can use data captured from faces and can accurately and quickly identify target individuals.

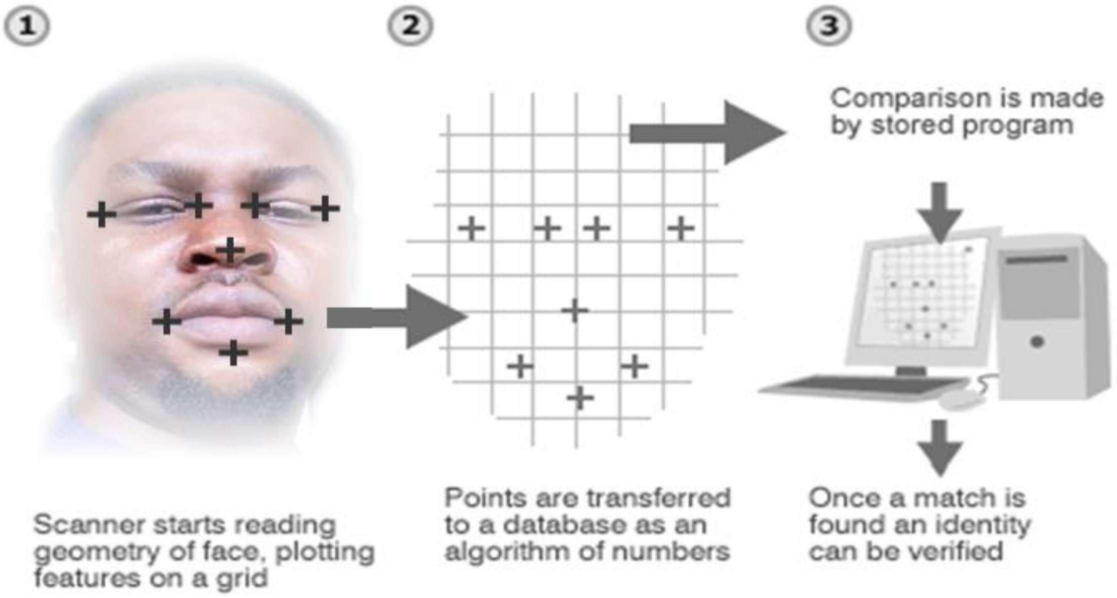
1
2
3
Comparison is made by stored program
Scanner starts reading geometry of face, plotting features on a grid
Points are transferred to a database as an algorithm of numbers
Once a match is found an identity can be verified

Figure 1.0a Face Geometry System

A face geometry authentication system works by:

1. Capturing photo from an image source.
2. Reading the geometry of the captured face-print. Key factors include the distance between the eyes and the distance from forehead to chin is stored in the database. The system identifies the facial landmarks. The result becomes the facial signature.
3. Comparing the facial signature; the facial signature is a mathematical formula, and it's compared to the database of known faces.
4. Matching the extracted data. A determination is made. The face-print may match that of an image in the system's database.

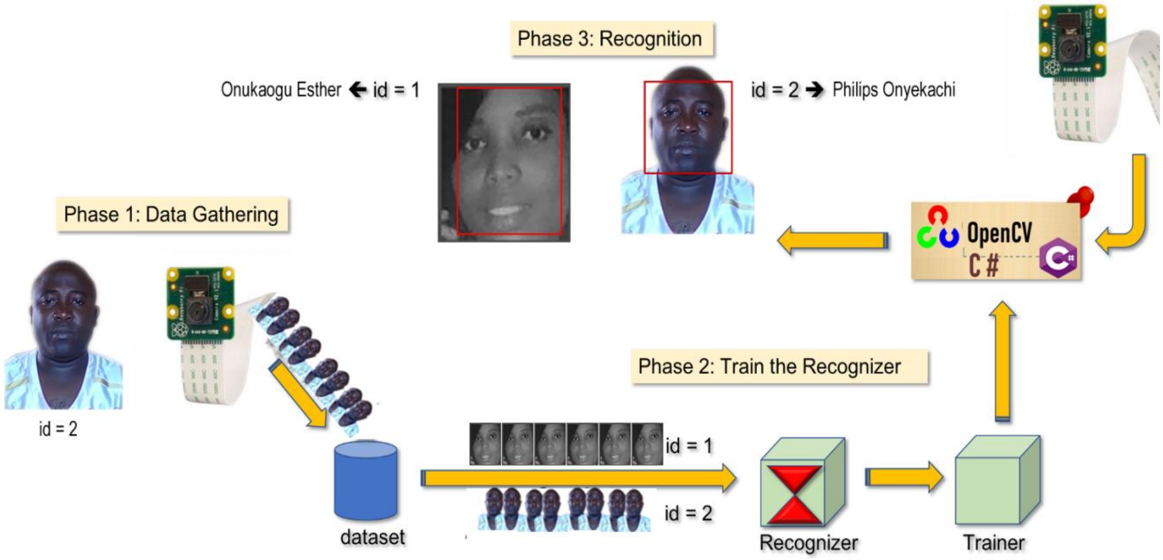

Figure 1.0b How The System Works

This system greatly improves total security measures by ensuring all faces are properly scanned before access is granted. Integration process is made easy as the new system can be integrated with existing system to enforce security. Biometric technologies including face geometry recognition represent the new wave of identity and authentication solutions. With its countless benefits, it's an important option to consider when planning an authentication system.

This system can be integrated at Business entrances and restricted areas, Retailers in stores, Airlines at departure gates, Social media companies on websites, and Universities classrooms. There are many advantages associated with facial geometry authentication systems compared to other biometric techniques; facial recognition is of a non-contact nature. Face images can be captured from a distance and can be analyzed without ever requiring any interaction with the user/person. As a result, no user can successfully imitate another person. Facial recognition can serve as an excellent security measure for login, time tracking and attendance. Facial recognition is also cheap technology as there is less processing involved, like in other biometric techniques.

1.1 Statement Of Problem

Hacking into users' Privacy and Loss of Confidential Information:

Almost 30 million Facebook users' phone numbers, and email addresses were accessed by hackers in the biggest security breach in the company's history. The hackers accessed even more details on 14 million of those users, including the area where they live, their relationship status, their religion, and part of their search history. *New York (CNN) https://edition.cnn.com/2018/10/12/tech/facebook-hack-personal-information-accessed/index.html*

Meanwhile if a system suffers loss of confidentiality, then data has been disclosed to unauthorized individuals. This could be high level secret or proprietary data, or simply data that someone wasn't authorized to see. With the use of Face authentication technology for access login, such incident could have been avoided, and users' privacy protected.

Password Security – Something We Know and Something We Have:

Passwords are our greatest security weakness because they quietly lure us into a false sense of security. The problem with passwords as the common means of authentication is that they've actually become the problem rather than the solution. Although for decades we've relied on passwords to protect our computer systems from hackers, they are no longer fit for purpose. One problem is that people are lazy at creating effective passwords, because we're expected to memorize them; many people choose passwords that are easy to remember to a critical extent. Such critical passwords include: "123456", "QWERTY", and, of course, "PASSWORD". Even best formed passwords also fail because of poor security habits, such as password sharing. Those few people who maintain best complex passwords often write them on a piece of paper, or store them in a Word Document to help remember them. Even if they commit them to memory, they may well reuse the same password for multiple logins or change them infrequently. It's clear that stolen passwords are a leading cause of data breaches.

1.2 Aim and objectives of study

The aim of this research paper is to develop a functional Biometric Authentication System Using Face Geometry. Below are lists of objectives to actualize the aim:

1. To create a user login authentication interface using C-sharp, SQL Server, and OpenCV libraries.
2. To create a login system with Webcam as face-print (image) input source.
3. To create a system with capability of being reused as a surveillance system.

1.3 Significance of study

The importance of this paper includes the following:

1. **Improved Security**: We used to have passwords with numbers, alphabets, symbols, etc. which are becoming easy to hack every day. There are millions of hacking incidents happening every year. Biometric technology brings different types of solutions which are nearly impossible to hack unlike passwords.
2. **Improved Accuracy**: Traditional security systems mess up regularly costing us a big amount of time, money and resources. The most common security systems are passwords; Personal Identification Numbers (PINs) and smart cards, that aren't always accurate. However, biometric works with our physical traits such as face geometry, fingerprints, palm vein, retina, amongst others that will always serve us accurately anywhere, anytime.
3. **Proper Accountability**: In other verification methods, anybody can use your password or security number to hack your personal information, which is highly risky and we are suffering from this

problem continuously. But, in the case of biometric security, it needs our direct interactions to login or pass the security system which allows 100% accountability for all activities.

4. **Convenience**: Imagine all the times when you forgot your passwords. We all have gone through this process where it is hard to memorize or note down each and every password and we are more than likely to forget it at some situations. There are some handy tools to do the job, but none of these can beat the convenience of biometric solutions which stands to be the most convenient solution ever. Your credentials are with you forever, so it doesn't require you to memorize or note down anything.
5. **Scalability**: Unlike other solutions, biometrics is highly scalable solutions for all types of projects. Biometric technologies are used in many government projects, banking security systems, workforce management, etc. It is possible because of the scalability of its solutions.
6. **Flexibility**: Definitely biometric systems are the most flexible security solution. You have your own security credentials with you so you don't need to bother memorizing awkward alphabets, numbers and symbols required for creating a complex password.
7. **Save Time**: Biometric solutions are highly time conserving. In most cases, you just need to look at the camera for access authentication.

1.4 Theoretical Background

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society, in which questions related to identity of an individual such as "Is this the person who he or she claims to be?", "Has this applicant been here before?", "Should this individual be given access to our system?" "Does this employee have authorization to perform this transaction?", etc are asked millions of times every day by hundreds of thousands of organizations, in schools, financial services, healthcare, electronic commerce, telecommunication, government, etc. With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming more critical.

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. The major advantages of this traditional personal identification are that: They are very simple; and they can be easily integrated into different systems with a low cost. However these approaches are not based on any inherent attributes of an individual to make a personal identification thus having number of disadvantages like tokens may be lost, stolen, forgotten, or misplaced; PIN may be forgotten or guessed by impostors. Security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor; further, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user).Therefore they are unable to satisfy the security requirements of our electronically interconnected information society. The emergence of biometrics has addressed the problems that plague traditional verification. Meanwhile, Biometric is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured in Biometrics are face geometry, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice, (Brostoff and Sasse, 2000).

Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face geometry, fingerprint, hand geometry, iris, retinal, signature, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, schools, in the military, and in commercial applications, (Bours and Barghoutti, 2009).

The security field uses three different types of authentication:

1. **Something you know** — a password, PIN, or piece of personal information (such as your mother's maiden name)
2. **Something you have** — a card key, smart card, or token (like a Secure ID card)
3. **Something you are** — a biometric.

Of these, a biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible.

1.4.1 Biometric Technologies

Face Recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. This technique has attracted considerable interest, although many people don't completely understand its capabilities. Some vendors have made extravagant claims, which are very difficult, if not impossible, to substantiate in practice, for facial recognition devices. Because facial scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel, (Kelly, 2011).

Fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiré-fringe patterns (large-scale interference patterns that can be produced when an opaque ruled pattern with transparent gaps is overlaid on another similar pattern) and ultrasonic. Some verification approaches can detect when a live finger is presented; some cannot. A greater variety of fingerprint devices is available than for any other biometric. As the prices of these devices and processing costs fall, using fingerprints for user verification is gaining acceptance. Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices, (Prabhakar, et al, 2003).

Hand Geometry involves analyzing and measuring the shape of the hand. This biometric offer a good balances of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system. Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular. Ease of integration into other systems and processes, coupled with ease of use, and makes hand geometry an obvious first step for many biometric projects.

Iris based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration has not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge, (Tieniu, et al, 2013).

Retina-based Biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.

Signature Verification analyzes the way a user signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Surprisingly, relatively few significant signature applications have emerged compared with other biometric methodologies. But if your application fits, it is a technology worth considering, (Simske, 2009).

Voice Authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware, most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.

1.4.2 Computer Vision

Computer vision is an interdisciplinary scientific field that deals with how computers can be made to gain high-level understanding from digital images or videos. From the perspective of engineering, it seeks to automate tasks that the human visual system can do. Computer vision tasks include methods for acquiring, processing, analyzing and understanding digital images, and extraction of high-dimensional data from the real world in order to produce numerical or symbolic information, e.g., in the forms of decisions. Understanding in this context means the transformation of visual images into descriptions of the world that can interface with other thought processes and elicit appropriate action. This image understanding can be seen as the disentangling of symbolic information from image data using models constructed with the aid of geometry, physics, statistics, and learning theory.

As a scientific discipline, computer vision is concerned with the theory behind artificial systems that extract information from images. The image data can take many forms, such as video sequences, views from multiple cameras, or multi-dimensional data from a medical scanner. As a technological discipline, computer vision seeks to apply its theories and models for the construction of computer vision systems, (William, et al 2008).

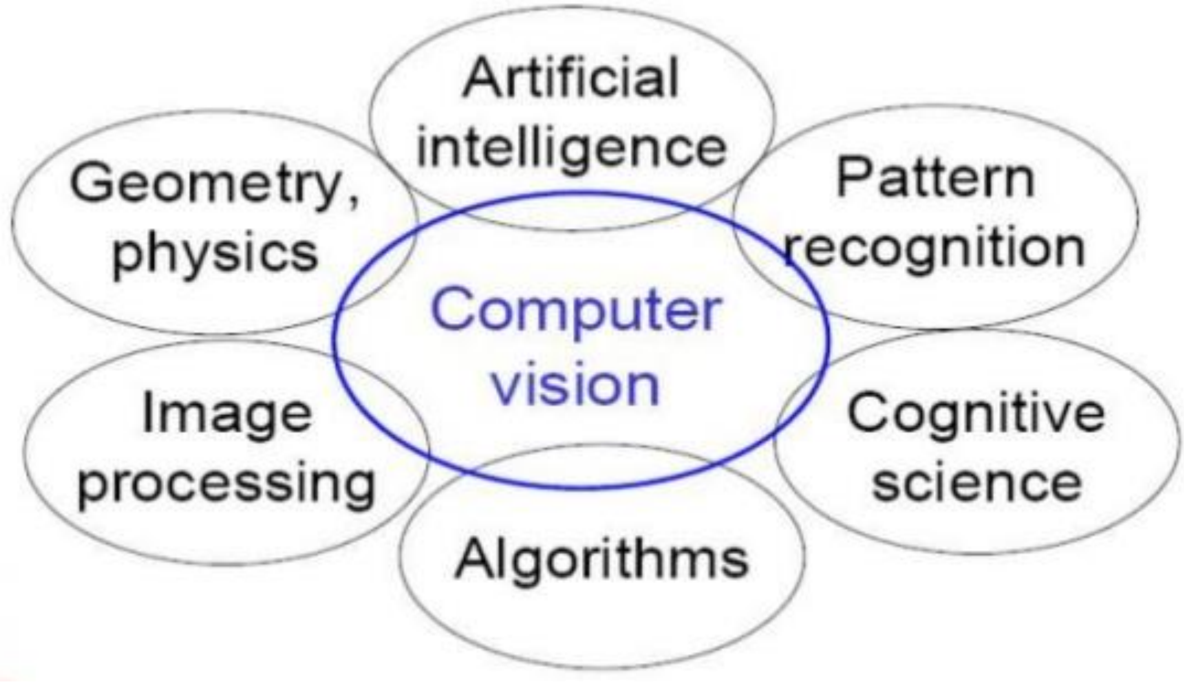

Figure 1.3.2 Computer Vision

1.5 Thodology

This paragraph deals with the methodology adopted in the course of the study. The type of methodology adopted is the Structured System Analysis and Design Methodology (SSADM). This methodology involves the analysis of the old and new system under study. It gives an orderly approach to system design and development. This structured methodology uses modules, stages, steps and tasks to improve project management and control; this invariably helps to produce a higher quality system. The SSADM adopts the waterfall model where each phase is completed, tested and approved before subsequent phase can begin. The waterfall model is also a sequential development process, in which development is seen as flowing steadily downwards (like a waterfall) through the phase of requirements analysis, design, implementation, testing (validation), integration, and maintenance.

SSADM divides an application development project into modules, stages, steps, and tasks, and provides a framework for describing projects in a fashion suited to managing the project. SSADM's objectives are to:

1. Improve project management & control
2. Make more effective use of experienced and inexperienced development staff
3. Develop better quality systems
4. Make projects resilient to the loss of staff
5. Enable projects to be supported by computer-based tools such as computer-aided software engineering systems
6. Establish a framework for good communications between participants in a project

In detail, SSADM sets out a cascade or waterfall view of systems development, in which there are a series of steps, each of which leads to the next step. SSADM's steps, or stages, are:

1. Feasibility
2. Investigation of the current environment
3. Business systems options
4. Definition of requirements
5. Technical system options
6. Logical design
7. Physical design

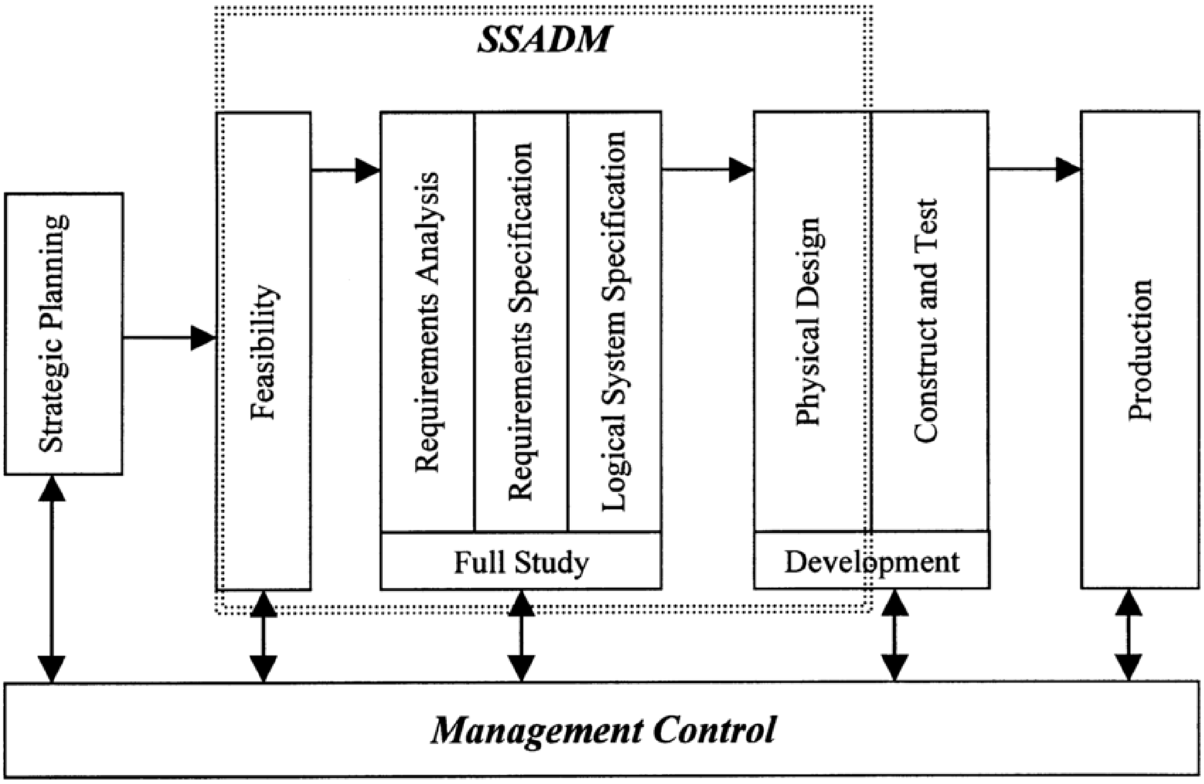

Figure 3.4 *Structured Systems Analysis and Design Method (SSADM)*

Stage 1 → Feasibility Study

Investigation of the economic, and technical feasibility. The problems are defined and the project identified.

Stage 1 → Investigation of the Current Environment

Definition of broad requirements, investigation of current data, and processes involved. The project is being identified and costs calculated. This stage is especially important as any omissions will have a bad effect on the whole project.

Stage 2 → Business Systems Options

Evaluation of the implication and benefit of each proposed option.

Stage 3 → Requirements Specification

Having selected a specific BSO a detailed specification of requirements now begins. The emphasis is on determining the desired system data, functions and events. Prototyping techniques are also suggests for the development of the system.

Stage 4 → Technical Systems Options

This assesses the different options for implementing the specification and describes the costs, benefits and constraints. Factors include internal and external constraints. External constraints consist of, for example, time, cost, business performance and any hardware or software constraints set in the feasibility study. The procedure for producing and selecting Technical System Options (TSOs) is very similar to that for BSOs.

Stage 5 → Logical Designs

The Logical Dialogue of the system is defined. This does not include the physical dialogues (menu structures, form designs etc.). Neither is this the stage at which the physical screen characteristics are defined. At this stage the logical exchange of data is defined.

Stage 6 → Physical Design

The Physical Environment the system will operate in is considered. After producing a physical design, creating a function and data design, the SSADM cycle is completed and the application is now ready for deployment.

1.6 System Analysis

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society, in which questions related to identity of an individual such as *"Is this the person who he or she claims to be?", "Has this student been here before?", "Should this student be given access…?", "Does this student have authorization to perform this action?",* etcetera are asked millions of times every day as a means of identification which is not trusted or reliable. By asking questions and physical observations, a lot of errors can be encountered during the course of identification. Developing a fingerprint biometric system will curb these problems of individual identification.

How Authentication Works Using Face Geometry

Face recognition uses the spatial geometry of distinguishing features of the face. It is a form of computer vision that uses the face to identify or to authenticate a person.

Every face recognition system is accomplished as follows:

1. A digital camera acquires an image of the face.
2. Software locates the face in the image bank; this is also called face detection.
3. When a face has been selected in the image bank, the software analyzes the spatial geometry.
4. The generated template is then compared with a set of known templates in the database (identification) or with one specific template (authentication).
5. The software generates a score which indicates how well two templates match.

Difficulties that often arise with face recognition are:

1. Variable image lighting and background make it more difficult to locate the face in the image.
2. Parts of the face are covered, e.g. long hair, and make it more difficult to locate the face in the image and to recognize the face.
3. Subject does not look directly into the camera, when the face is not held in the same angle the software might not recognize the face.

4. Using different types of cameras (with different lighting, resolution, etc.) makes it more difficult to recognize the face.
5. The face of a subject changes with ageing.

But all these stated above have remedy to each and every one listed.

Conclusion

User authentication is to associate a person with an identity. This process plays a serious role in our modern society, in which questions related to the identity of a person is being asked. Such questions include: “Is this the person who he or she claims to be?”, “Has this candidate been here before?”, “Should this fellow be granted access?” “Does this worker have authorization to perform this action?” are asked several times daily. The problems of user identification can be easily solved using Face Geometry Recognition technology; this technology can be categorized as a subdomain of Computer Vision; and Computer Vision can be seen as an interdisciplinary scientific field that deals with how computers are made to gain high-level understanding from real-time images or video streams. This technology has come a long way in the past years. Nowadays, through the help of Object Recognition technology, computers can identify, and verify details for highly secured environments, such as login authentications, surveillance, and access control to secured structures. Computer Vision applications like Face Geometry Recognition systems usually work well in controlled environs. Nevertheless, some next generation Face Geometry Recognition systems will be having widespread applications in smart environs where computers are more likely helpful aides. To accomplish this aim, computers must be capable to dependably recognize close objects (like a person), in a way that fits naturally within the form of human communications. These machines (computers) must not need distinct interactions, and must adapt to human perceptions about when recognition is likely. This implies that future smart environs should use the same modalities as humans, and have almost the same restrictions. The aim now appears in reach; however extensive research is to be furthered in making Face Geometry Recognition systems work reliably, in broadly changing environments.

References

[1] Bours, P. and H. Barghouthi. Continuous authentication using biometric keystroke dynamics. In The Norwegian Information Security Conference (NISK) 2009, 2009.

[2] Brostoff S. and Sasse, M. A. (2000), "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[3] William Freeman; Pietro Perona; Bernhard Scholkopf (2008), "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[4] Kelly A. G. (2011), Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (New York, 2011), p. 100.

[5] Prabhakar, S. Pankanti, S. and Jain, A. K. (2003). Biometric recognition: security and privacy concerns. IEEE Journals on Security & Privacy, 1(2):33–42, 2003.

[6] Simske. S. J (2009). Dynamic biometrics: The case for a real-time solution to the problem of access control, privacy and security. In Paper presented at IEEE BIdS Conference, Tampa, Florida, Sept 22-23 2009.

[7] Tieniu, Y. W., Wang, Y., Tan, T. and Jain, A. K. (2013). “Combining face and iris biometrics for identity verification,” pp. 805-813