International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3362-3368 www.ijaem.net ISSN: 2395-5252

Application of Fingerprint Authentication on Household Appliances

Osodeke, Efe Charles[1], Joseph Ugochukwu[2], John Peace Chidimma[1]
Department of computer Science[1]
Department of Physics[2]
Michael Okpara University of Agriculture, Umudike

Submitted: 15-07-2021 Revised: 29-07-2021 Accepted: 31-07-2021

ABSTRACT
With the rapid advancement in technology, the need to apply fingerprint recognition in homes for security and others is highly needed. Password and identity cards or keys have been used as a traditional authentication mechanisms in home environments. However, the rise of misuse of these mechanisms are proving them to be less reliable. For instance ID cards can be misplaced, copied or counterfeited and being misused. Conversely, studies have shown that biometrics authentication systems particularly Iris Recognition Technology (IRT) and Fingerprint Recognition Technology (FRT) have the most reliable mechanism to date providing tremendous accuracy and speed. As the technology becomes less expensive, application of the IRT & the FRT in homes becomes more reliable and appropriate solution for security challenges. In this paper, I am going to describe a simple home security system that implemented using fingerprint biometrics technology. The system is known as Application of Fingerprint Authentication on Household Appliances. This system is demonstrated by using a prototype that consist of hardware and software components. The hardware includes fingerprint sensor, a micro controller, a wireless network router, an application server and a smartphone. For the software, a program is developed to record the fingerprint data and to verify the data on the remote server.

I. INTRODUCTION

Security is one of the most significant necessities for people at home. Here I will refer this home that will use a fingerprint authentications as a ‘’Smart Home’’. A smart home refers to a home that is combined with highly sophisticated automatic systems for monitoring doors, windows, alarms, alerts and various additional tasks monitored by computer systems.

The development of information and Communication Technology (ICT) currently offers convenience to the user and it improves various aspect of human life. The technology includes smart house or smart home authentication. The smart home had emerged and developed since 1960’s when the first homes automation processing device named ECO IV was designed. The machine, a private venture by a Westinghouse engineer, was designed to control home temperature and turn on the appliances at home (King 2015).

There exist several security and authentication Mechanisms that can be embedded in homes, these includes the use of numerical codes like passwords, Personal Identification Number (PIN) and passphrases, security tokens like smart card and biometrics authentication method, however, studies have shown that numerical codes, smart cards and physical keys mechanism have their associated drawbacks. Fingerprints have been accepted as the most common form of biometrics authentication today, the strong point about using fingerprint biometrics are that giving fingerprints is more widely accepted, convenient and reliable than other forms of physical identification system are gaining attractiveness as a way of providing access in different environment that needs security Fredrick (2011).

BIOMETRICS

Biometrics technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioural characteristics. Biometrics can provide very secure and convenient authentication for an individual since they cannot be stolen or forgotten and are very difficult to forget.

The term ‘’Biometrics’’ is derived from two Greek word ‘bios’ for life and ‘metric’ for measure. The area of biometrics can therefore be defined as the task of automatically recognizing a person using his/her distinguishing traits we will look into is the fingerprint. The idea of biometrics identification is not new, it have been around for centuries (Ahmed, 2017).

CLASSIFICATION OF BIOMETRICS

Biometrics can be broadly classified into two:

- Physiological Characteristic
- Behavioural Characteristics

Physiological Characteristic: This is a relatively stable physical characteristic such as an individual fingerprint, hand geometry, Iris pattern. This type of biometric measurement is usually unchanging and unalterable without significant clue to the individual.

Behavioural Characteristics: This is more a reflection of an individual psychological makeup. A signature is the most common behavioural biometrics used for identification. Because most behavioural character vary over time an identification system using these must allow updates to enrolled biometrics reference.

TYPES OF BIOMETRIC SYSTEM

There are two types of Biometrics System;

1. Recognition System: this simply mean the following

- Identifying a person among the whole group of users enrolled in the system
- It must be an online system
- Typical applications; Forensics

Identification (one to many comparison) varies if the individual exist within another identity card is not on a predetermined list of prohibited persons

2. Authentication System means the following

- Verifying the identity that user claims to have
- It can be offline
- Typical application; Access control, all kinds of application where cards are used.

Authentication (one to one comparison) confirms that the credential belong to the individual presenting it. In this case, the device that performs the authentication must have access only to the individual's enrolled biometric template, which may be stores locally or centrally.

Every human beings fingerprint is unique; each fingerprint has a unique characteristics and pattern that is made up of lines and space. The lines are called ridges while the space between the ridges are called valleys. These patterns of ridges and valleys are used to match the fingerprint for verification and authentication fingerprint is the oldest and the most used biometrics trait in identification problems, thanks to its wide user's acceptability, accuracy, security as well as to its relative inexpensive cost.

Fingerprint matching techniques can be placed in two categories; Minutiae base and correlation based.

Minutiae-based techniques first find minutiae point and then map their relative placement on the finger, however there are some difficulties when using the approach.

Correlation based method looks at the entire pattern of ridges and valleys in the fingerprint. The location of the whorls, loops and arches and the direction that they flow in are extracted and stores.

Fingerprint Authentication Technology

Fingerprint authentication technology is divided into two process identification and verification.

1. IDENTIFICATION PROCESS

In identification process, an individual present a sample to the biometrics system during enrolment. The biometric system then attempts to compare the sample with the database which has samples stored in it.

POSITIVE IDENTIFICATION; in a positive identification system users do not enter a pin number along with their fingerprint, but simply place their fingerprint on the capture device and their fingerprint is identified by matching the fingerprint in the database.

NEGATIVE IDENTIFICATION; in these system searching the database is done in the same fashion, comparing one template against many, but these systems are designed to ensure that a person is not present in the database.

2. VERIFICATION PROCESS

Verification is a one-to-one comparison in which the biometrics system attempts to verify an individual identity. In this case, a new biometric sample is captured and compares with the previously stored templates, if the two samples match, the biometrics system confirms that the applicant is who he/she claims to be.

Identification involves matching a sample against a database of many whereas verification involves matching a sample against a database of one. Table below shows the risk associated with using various security mechanism for homes.

Table1: List of Identification and related risk

SECURITY MEACHANISMS	RISK
Identity Cards (ID)	Lost, Stolen, Duplicated, Left
Physical Keys	Lost, Stolen, Duplicated, Left
Password	Forgotten, Shared, Observed
Magnetic Stripe Cards	Lost, Stolen, Duplicated, Left at home
Smart Cards	Lost, Stolen, Duplicated, Left at home
Signature	Imitated

Biometrics authentication system is going attractiveness as a way of providing access in different environment that needs security. Biometrics authentication system are classified in 2 group; physical based mechanism and behaviour based mechanisms.

Physical based mechanisms are the ones that emphases on observing the biological and the physiological characters of the human being. Example are the ones that involve giant and typing patterns biometrics.

Fingerprint Recognition Technology

This is the type of biometric security that uses the human fingerprint and compares its patterns for identifying a person. The recognition technology involves two steps; Enrolment steps, using fingerprint capturing device,

There are four steps in fingerprint recognition.

- Image Acquisition
- Location and determination of the fingerprints characteristics
- Template creation
- Template matching.

II. STATEMENT OF THE PROBLEM

With a growing range of features, smart locks are one of the most useful innovations in modern home security. When home access is in question, any measure that can increase security is significant and we know that individuals or people have concerns about device security. Strengthening the security of the device managing access to their front door, therefore, enhance both appeal of the smart lock. This is where biometrics fits in adding a trusted layer of security to device access to the front door, without compromising the convenience, unlike password protected smart locks.

Fingerprint/biometrics authentication uses personally identifiable information stored securely on-device (Weather the lock itself or a fingerprint – secured access card) for maximum privacy. This makes biometrics both difficult to hack and near-impossible to spoof, ensuring that homes stay considerably safer than with merely password secured, internet enables or traditional key locks.

Biometric technology not only ensures that convenience doesn't come at the cost of security, but can actively enhance convenience. In homes biometrics not only secure but enable a range of personalized access controls. For example access to potentially hazardous areas, such as medicine cabinets and kitchen drawers could be restricted to adults, similar in a shared house or flat personalized controls could give housemates greater privacy by controlling access to personal and shared areas.

Student accommodation is another interesting scenario. Typically, hundreds of student will not only share a front door, but access to the washing room, toilet, kitchen and many other community rooms. The specific combination of rooms and facilities student are permitted to access is likely to be individual to each student, creating an access controls headache. Biometric locks provide a sample and convenient solution, enabling the management team to ensure only the right students have access to certain rooms and areas of the building. Likewise students don't have to remember endless password or manage a set of keys.

Another notable example is the Inosmart solution, which was recently announced by Slovenian Smart door manufacturer inotherm. This adds fingerprint authentications to the doors smart keypad, enabling users to control access with fingerprints, ensuring significant potential for personalization, as well as convenience and security.

How Does Biometric Authentication Work?

Today's biometric authentication systems use the same forensic methods to compare and match two sets of biological characteristics. First, you register your information in a system and connect it to your profile. How the system matches your information to the stored records depends on the type of biometrics involved. For the system to work, there are three types of technologies involved:

- **Scanner or sensor** – A highly accurate scanning or sensing device used to capture your biometric information.

- **Computer or system** – The information system where you store the biometric information enabling you to retrieve it in the future for comparison with live data.
- **Software or application** – A program that manages the interface between the sensor and the computer system while carrying out a comparison.

The most common type of biometric authentication available today is fingerprint scanners. The scanners and software are becoming more common in laptops, mobile devices, or as a connected peripheral to improve your device security. Although voice and face recognition solutions exist, the technology is still prohibitively expensive and, in some cases, struggle with accuracy. Due to the years of research and the accuracy of the comparison methods, fingerprint scanners have become the preferred biometric authentication method for today's computer systems.

Benefits of biometric door system

Biometric provides better security and more suitable than other conventional methods of human recognition. Biometric refers to unique characteristics of an individual such as physiological or behavioural which doesn't change with time.

Fingerprint technology is more commonly used than any other biometric modality in residential security systems, fingerprint identification systems are quick and easy and also eliminates the conceptions required for a face or eye scan. In addition to these, there are numerous benefits of installing such mechanisms.

Key-less door lock

One of the primary reasons for adopting this system is that it completely eliminates the need of any key to operate door locks. This is a huge benefit for most people and especially those who are in the habit of misplacing or forgetting their keys, with this type of door lock, a big responsibility is removed from the users shoulder as keeping the key securely, is a must for every home owner. There always comes a time when someone loses a key no matter how careful they have been to keep all things at one place. These door locks are simply in execution and come in variety of shapes and sizes to fit any type of door, initially the designs were limited to residential security system but now there are numerous door-fingerprint combinations available in the market. These locks are mostly designed for the front doors or doors inside the building.

Other types also combine biometric identification and keypads for extra security. Depending on the number of security layers and how advance the system is the price can range from couple hundred to several hundreds of naira/dollars. The most expensive sensors have the capacity to hold many prints profiles for friends and family. Also the wide spread use of these device and latest innovations has made available variety of affordable scanners.

Convenience

This system makes it unnecessary to carry around numerous key for gaining access. A simple swipe of authorized fingerprint across the scanner is sufficient for gaining access. Owners no longer need to worry about the safety of their premises or valuables as their fingerprint is unique and virtually impossible to copy.

Quicker Access

It provides quicker access to individuals as it eliminates the need to manually lock and unlock doors with keys. Moreover, these systems usually slut doors automatically once the individual has entered his or her house thereby ensuring that only authorized persons can enter.

Advance Security Solution

Sometimes the traditional number lock on a home safe might not be sufficient, instead a biometric solution is a better option as it provides highly personalized safety by using fingerprint analysis scanner to protect the content. These systems can dissuade thieves who might steal an ordinary home safe with intention of breaking it later. Biometric solution also allows the owner to limit access of the safe to only one or two individuals. In addition to being highly useful for the key documents and jeweller, this is also a valued security features for firearm safes and gun cabinets where contents can be dangerous in the wrong hands.

Difficult to Override

Unlike door locks with keys, a biometric system cannot be overridden by any individual unless they have the home owner's fingers to prove to the system for authorized access. Conventional door locks are vulnerable to lock pickers but biometric system are impossible to break and provide effective defence against any kind of intrusion and is the best home security solution for areas that are prone to rubbers.

Cost-effective Solution

Although the system might be a bit expensive in terms of initial investment, it proves to be a cost-effective option in the long run. In comparison to other common types of locks, a fingerprint door lock does not easily especially the ones that are constructed from quality materials and manufactured by well-known companied.

User Friendly

This system does not need any complicated mechanism or things that might be discouraging to the new user as it is very intuitive and can be used in a simple manner.

III. LITERATURE REVIEW

In biometrics, human being needs to be identified based on some characteristic physiological parameters. A wide variety of recognition schemes are used to either confirm or determine the identity of an individual requesting their services. This Researcher has collected comprehensive information from various books, manuals, magazines, journals, articles and research websites.

Anil K.Jain (2007) focused on biometric template security which is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Protecting the template is a challenging task due to intra-user variability in the acquired biometric traits. He present an overview of various biometric template protection schemes and discuss their advantages and limitations in terms of security, revocability, and impact on matching accuracy.

Brindha, V.E. (2012) presented about protection of fingerprint template from creation of physical spoof and replacement by imposter's template to gain unauthorized access by transformation based approaches and biometric cryptosystems. The security of the fuzzy vault depends on the infeasibility of the polynomial reconstruction and the number of chaff points. In the proposed system an even more secured fuzzy vault is generated with combined features of fingerprint and palm print to enhance the security of the template stored.

Comesana, P (2006) in his paper proposed a new version of the sensitivity attack based on a general formulation; this method does not require any knowledge about the detection function nor any other system parameter, but just the binary output of the detector, being suitable for attacking most known watermarking methods.

Dacheng Xu and Bailiang Li (2009) presented a pseudo-random sequence fingerprint key algorithm based on fuzzy vault is proposed. It is usually difficult to transform template and generate cancellable fingerprint template. In this method, the distribution of the minutiae can be changed, which overcomes vulnerabilities. Further, a bounding box of variable size minutiae matcher during decoding to account for nonlinear distortion is used and this leads to find out reliable minutiae to improve the genuine accept rate.

Daesung et al (2006) presents an implementation to improve the security of the typical PKI-based authentication by protecting the private key with a fingerprint also the privacy issue of the fingerprint data by storing the fingerprint data not in a database, but in a user-carry device such as a smart card or a USB token. Furthermore, the fingerprint data stored in the user-carry device is conglomerated with the private key, and the private key is released only with the valid fingerprint

Fingerprint authentication or recognition is to distinguish between two human fingerprints. In order to match two fingerprints, several features of the print pattern are required including ridges and minutia points. Ridges contain three basic patterns which are arch, loop and whorl. Fingerprint recognition has become one of the most important and popular identification technique nowadays because of the accuracy of this technique is very high and the current fingerprint recognition system is sufficient for the identification and verification system that involve more than hundred users. (Anil et al, 2004)

In fingerprint recognition system, there are three sub-domains, which are enrolment, verification and identification. Enrolment is the process which the user's fingerprint data will be collected via a specific sensor and store into database after some processing. In verification mode, a captured fingerprint will be compared to the template stored in the database to validate a person's identify. This is so call one-to-one comparison. The purpose of verification is to prevent different person using the same identify. While for identification mode, the system will conduct a one-to-many

Mainstream Biometric Technologies

The function of a biometric technologies authentication system is to facilitate controlled access to applications, networks, personal computers (PCs), and physical facilities. A biometric authentication system is essentially a method of establishing a person's identity by comparing the binary code of a uniquely specific biological or physical characteristic to the binary code of an electronically stored characteristic called a biometric. The defining factor for implementing a biometric authentication system is that it cannot fall prey to hackers; it can't be shared, lost, or guessed. Simply put, a biometric authentication system is an efficient way to replace the traditional password based authentication system (Ashbourn, 2000).

Hand Geometry

The hand image is obtained using a camera capturing from the top when the user places his/her hand on a desired surface. User hand can be aligned using reference marks or pegs. Two views are usually taken in a single image, the side view and the top view. The side view is usually captured by the top camera, using a side mirror. From the hand image, the fingers are located and the width, length, thickness, curvatures and their relative geometry measured (Yun 2002).

In some cases the hand geometry template size can be very small. In that case it has acceptable accuracy for verification but not sufficient enough for best identification. The main advantage is that most people can use it with ease and the acceptance rate is good. However, the negative side is that the system is rather bulky and may face problems with users aging and health conditions such as arthritis (Yun 2002).

IV. CONCLUSION

It is clear that biometric is here to stay in the smart home ecosystem, it doesn't stop at the front door, either there's potential to add biometrics authentication to numerous devices throughout the smart homes itself. The primary as well as the most obvious benefits of this technology as compared to the conventional home security system such as keys or password is that it is inherently linked to home owners and therefore is much more difficult to compromise through theft, collusion or loss. The common perception that the incorporation of biometrics in home security systems will result in an expensive and sophisticated affair is in fact a myth. However the opposite is true. Integrating biometrics into security systems is not costly and home owners can affordably and easily use this technology to secure their property from theft and intruders. As a result more and more people/individuals are starting to use this technology because it is convenient and inexpensive. Therefore we can say that home security systems actually become less complicated with integration of this technology.

Using this system, home owners do not need to remember any password or their home keys, fingerprint also can neither be shared nor lost. This is the convenience that biometric technology brings to users along with improved reliability and security with traditional lock and key system cases where the owner forgets or loses his key are not unheard of. The owner and his family members might have to remain locked out of their own house while they are waiting for a professional locksmith to unlock their door. In addition to the inconvenience, the owner will also need to spend exorbitant amount to have a locksmith unlock the door and then get the door lock replaced.

Fingerprint door locks are the perfect solution for home owners, although this might sound like something out of a sci-fi movie, this technology is becoming more common and various fingerprint scan locks are now readily available.

Individuals can use their fingerprints to effortlessly identify and verify that they actually are who they claim to be. Such is the power of this technology and owners and their families will no longer have to worry about keys. A biometric home security system is definitely a better solution and has tremendous benefits when compared to the conventional key door locks, key-less keypad locks, combination doors locks or card reader locks. As these locks can only be opened by a specific person based on their unique fingerprint, they are therefore excellent for providing guaranteed security, speed and convenience. In addition to being the most accurate and cost effective home security system, duplication of this method is also virtually impossible. This system can also easily perform verification where it compares an input fingerprint to the enrolled

REFERENCES

[1]. Ahmed Abd Al Qawi (2017), The Possibility of Applying Biometric Safety Technology in Egyptian Hotels: "Evaluating Customer Experience Using the TAM Model" International Journal on Computer Science and Engineering 2(7)

[2]. Anil K. Jain, Arun Ross and SalilPrabhakar (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology

[3]. Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar (2007). Biometric Template Security; EURASIP Journal on Advances in Signal Processing.

[4]. Ashbourn, J. (2000) Biometrics: Advanced Identity Verification: The Complete Guide. Springer-Verlag, London, 1-6.

[5]. Brindha, V. E. (2012). Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. Journal of Biometrics.

[6]. Dacheng Xu; Bailiang Li (2009). A pseudo-random sequence fingerprint key algorithm based on Fuzzy vault. International

Conference on Mechatronics and Automation Mechatronics

[7]. Daesung Moon,Sungju Lee,Seunghwan Jung,Yonghwa Chung (2006) improve the security of the typical PKI-based authentication

[8]. Fredrick R. Ishengoma(2011). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies

[9]. Kensington News (2020). Biometric Authentication: Overview of the Advantages and Benefits

[10]. Leo King (2015). The evolution of the smart home - Raconteur

[11]. P Comesana, L Pérez-Freire, F Pérez-González (2006) The return of the sensitivity attack; International Workshop on Digital Watermarking

[12]. Wei-Yun Yau (2002), Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters