

# Evaluation of a Fingerprint Recognition Technology for a Biometric Security System

Chinedu Paschal Uchenna<sup>1</sup>, Adegher Pascal<sup>1</sup>, Ogundu Prince<sup>2</sup>

<sup>1</sup>Department of Information Technology, National Open University of Nigeria (NOUN), Abuja, Nigeria

<sup>2</sup>Department of Maths and Computer Science, National Open University of Nigeria (NOUN), Abuja, Nigeria

## Email address:

puchinedu@yahoo.com (C. P. Uchenna), padegher@gmail.com (A. Pascal), mcfredhprince@yahoo.com (O. Prince)

## To cite this article:

Chinedu Paschal Uchenna, Adegher Pascal, Ogundu Prince. Evaluation of a Fingerprint Recognition Technology for a Biometric Security System. *American Journal of Computer Science and Technology*. Vol. 1, No. 4, 2018, pp. 74-84. doi: 10.11648/j.ajcst.20180104.11

**Received:** November 5, 2018; **Accepted:** November 27, 2018; **Published:** December 26, 2018

---

**Abstract:** Authentication is a fundamental component of human interaction with computers. Traditional means of authentication, primarily password and personal identification numbers (PINs), have until recently dominated computing, and are likely to remain essential for the years to come. Over the years, passwords are kept simple to avoid them being easily forgotten. This has subjected them to higher vulnerability to much compromise by unauthorized persons. Thus, computers are forced to manage more and more passwords which imply that the likelihood of password being forgotten increases. Hence, biometrics is becoming more convenient and distinctly more precise than traditional methods such as passwords and PINs. Biometrics link the event to a particular individual, requires nothing to remember or carry, provides positive confirmation by verifying individuals are who they claim to be, and is becoming an inexpensive solution. This research work aims to evaluate fingerprint recognition technology for a biometric security system using the implementation at the Council for the Regulation of Engineering in Nigeria (COREN) as a case study; to reveal the enormous benefits of using or deploying biometrics which may include the increased security, increased convenience, reduce fraud, or delivery of enhanced services. An evaluation of the said system as deployed in COREN was advanced by the use of quantitative method which design administered a survey instrument in the form of a questionnaire among 20 employees of Council for Regulation of Engineering in Nigeria (COREN). Therefore, upon analyzing the responses from the field work conducted, it is evident that fingerprint recognition system is secured due to fingerprints uniqueness. The outcome of the system suggests that fingerprints, sensors and papillary line provide enough entropy on biometric security.

**Keywords:** Fingerprint Recognition Technology, Biometric Security System, Benefits of Biometric Security System

---

## 1. Introduction

Recent and rapid progress in electronics and computer science have transformed the nature of biometric data into digital form which are processed using computer technology so that an automatic comparison of such data can be made. This accelerated all the processes from the acquirement of biometric information to its evaluation. This progress was essential. Due to increase of Earth population, there was no other way which could be applied to practical processing of biometric data. At the moment, huge fingerprint database exists, which contain millions of fingerprints.

With the invention of letters and writing, the demand on information hiding started to grow constantly. The first

methods simple e.g. invisible ink, but better methods were developed with the improvement of theoretical knowledge, suitable not only for information hiding. These new methods included general algorithms for information encryption and decryption, using permutations and simple substitutions at the beginning, but later using keys as an important secret element to protect the information. The algorithm itself needs not be kept secret-in fact actual algorithm structures are publicly known.

The scientists discovered that biometric features could be used not only for criminal investigation but also for other purposes. That was the beginning of the era of access systems. Such access systems can control the access to physical or logical objectives. Users do not need to remember password or personal identification numbers PIN; they could

simply use their body attributes to get a granted access. With the increasing computational power and better theoretical basics, it has been possible to attack or deceive single cryptographic or biometric systems. This is therefore the reason for increasing use of the combination of both biometric and cryptography (data encryption and decryption).

### 1.1. Statement of the Problem

In the present system, the most frequently used authentication methods are passwords and PINs. They secure access to Personal Computers (PCs), networks, and applications; control entry to secure areas of a building; and authorize Automatic Teller Machine (ATM) and debit transactions. Handheld tokens (such as cards and key fobs) have replaced passwords in some higher-security applications. Physical authentication devices such as smart cards and password tokens were developed in order to eliminate certain weaknesses associated with passwords. However, passwords, PINs, and tokens or cards have a number of problems that call into question their suitability for modern applications, particularly high-security applications such as access to online financial accounts or medical data. The present system uses the *Traditional authentication methods*. *In theory*, a password is memorized by a single person, it's hard to guess, it's never written down, and it's never shared. *In practice*, however, people constantly violate these expectations. Password and PINs are easily guessed or compromised; tokens can be stolen. Many users select obvious words or numbers for password or PIN authentication, so that an unauthorized user may be able to break into an account with little effort. In addition, many users write password in conspicuous places, especially as the number of passwords users must manage continually increases. "Good password", i.e. long passwords with numbers and symbols, are too difficult to remember for most users and are rarely enforced.

Passwords, PINs and tokens can also be shared, which increases the likelihood of malicious or unaccountable use. In many enterprises, a common password is shared among administrators to facilitate system administration. Unfortunately, because there is no certainty as to who is using a shared password or token or whether the user is even authorized – security and accountability are greatly reduced.

In the present system, one of the reasons passwords are kept simple (and are then subject to compromise) is that they are easily forgotten. As computer are forced to manage more and more passwords, the likelihood of password being forgotten increases, unless users choose a universal password being forgotten increases, unless users choose a universal password, reducing security further. Tokens and cards can be forgotten as well. Biometrics are becoming more convenient and distinctly more precise than traditional methods such as passwords and PINs. Biometrics link the event to a particular

individual, requires nothing to remember or carry, provides positive confirmation by verifying individuals are who they claim to be, and is becoming an inexpensive solution.

### 1.2. Specific Objectives of the Study

This research focuses on evaluating fingerprint recognition technology for a biometric security system using the implementation at the Council for the Regulation of Engineering in Nigeria (COREN) as a case study. The specific objectives advanced in this study include, to:

1. Reveal the enormous benefits of using or deploying biometrics which may include the increased security, increased convenience, reduce fraud, or delivery of enhanced services.
2. Validate an efficient, accurate, consistent, and effective way of acquiring, processing, matching, storing and enhanced fingerprints image *acquisition*.
3. Unveil fingerprint Recognition Technology for Biometric Security System as a capable developed authentication technology that gained sufficient improvement on the existing traditional method
4. Determine the effects, uses, long term impact of the availability, accessibility and user-ability of fingerprint Recognition Technology for Biometric Security System.
5. Demonstrate how reliable, secure, fast and an efficient system the fingerprint biometric system is to replace the present traditional methods such as passwords and PINs

## 2. Biometrics Security System - Overview

According to Jain, Dass, and Nandakumar [1], authentication is a fundamental component of human interaction with computers. Traditional means of authentication, primarily password and personal identification numbers (PINs), have until recently dominated computing, and are likely to remain essential for the years to come. However, stronger authentication technologies, capable of providing higher degrees of certainty that a user really is who he or she claims to be, are becoming common. Biometrics is one of such strong authentication technologies.

Biometric technologies, as widely known today, have been made possible by explosive advances in computing power and have been made necessary by the near universal interconnection of computers around the world. If data is money, then server-based or local hard drives are the new vaults, and information-rich companies will be held responsible for their security. Because of this, password and PINs are nearing the end of their cycle for many applications. Figure 1 unveils the increase of security and comfort for three different authentication methods.

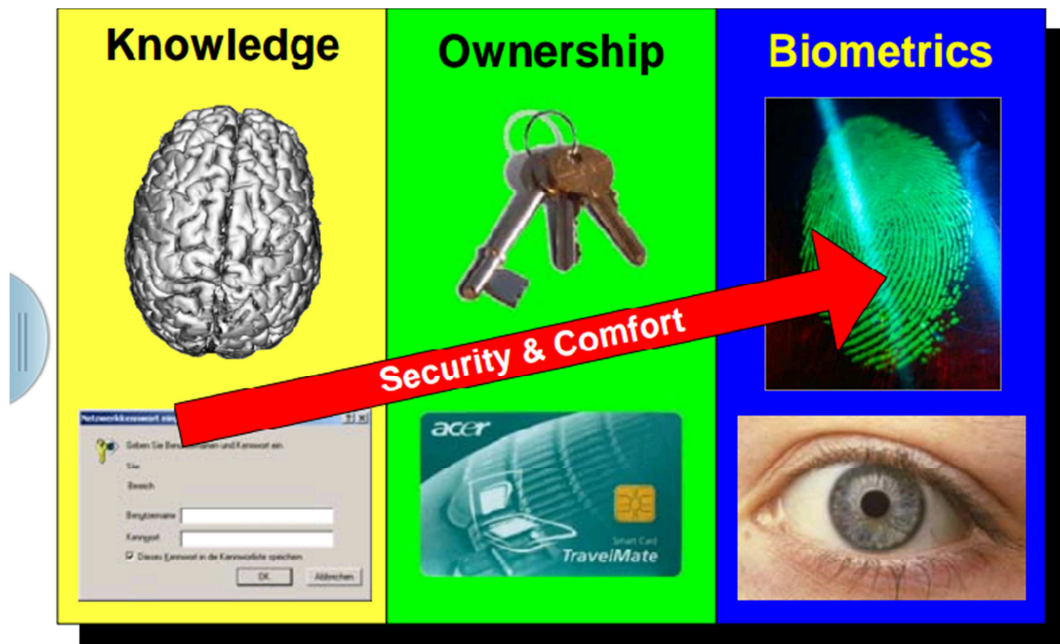


Figure 1. Increase in security and comfort.

In a paper, Opara, Rob and Etnyre [2] analyze biometrics technologies and describe techniques that can be utilized to decrease the probabilities of online attacks. The study showed that biometrics is the most accurate and secured representation of what an element is. Furthermore, it was submitted that Its technology can isolate false positive results, misrepresentation or creation of false identity during an identification process. As compared to other identification solutions packages, Biometrics systems are advanced and sophisticated since the technology would authenticates a person's identity base on a unique physical attribute rather than deploy some form of identification formula. Thus, it has been argued that though the visibility could become problematic to the industry in general, the exposure accorded biometric applications has enhanced its awareness [2].

But biometrics is more than a replacement for passwords

and PINs. Millions of people around the world use biometric technology in applications as varied as time and attendance, voter registration, internal travel, and benefit distribution. Depending on the application, biometric can be used for security, for convenience, for fraud reduction, even as an empowering technology [3]. A number of biometric attributes are in use in various applications. As indicated in Figure 2, the uniqueness of each biometric attribute is its benefit. Each biometric attribute has its strengths and weakness and the choice typically depends on the application. No single biometric attribute is expected to meet requirements of all applications effectively. The matching between a biometric attribute and an application is determined depending on the characteristics of the application and the properties of the biometric attribute.

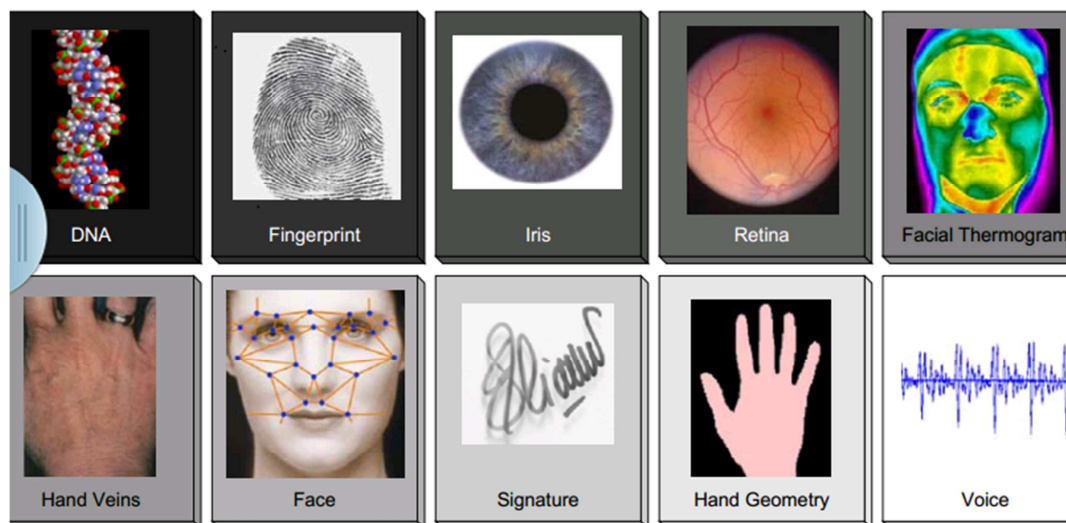


Figure 2. Different biometric attributes (ordered in accord with their uniqueness).

### 2.1. The Benefits of Biometrics Security System

1. Increased security. Biometrics can provide a greater degree of security than traditional authentication methods, meaning that resources are accessible only to authorized users and are kept protected from unauthorized users. In theory, a password is memorized by a single person, it's hard to guess, it's never written down, and it's never shared. In practice, however, people constantly violate these expectations. Password and PINs are easily guessed or compromised; tokens can be stolen. Many users select obvious words or numbers for password or PIN authentication, so that an unauthorized user may be able to break into an account with little effort. By contrast, biometric data cannot be guessed or stolen in the same fashion as password or token. Although some biometric system can be broken under certain conditions, today's biometric systems are highly unlikely to be fooled by a picture of a face, an impression of fingerprint, or a recording of a voice. This assumes, of course, that the impostor has been able to gather these physiological characteristics- what is unlikely in most cases.
2. Increased Convenience. One of the reasons passwords are kept simple (and are then subject to compromise) is that they are easily forgotten. Tokens and cards can be forgotten as well; though keeping them attached to keychain reduces this risk.
3. Because biometrics are difficult if not impossible to forget, they can offer much greater convenience than systems based on remembering multiple passwords or on keeping possession of an authentication token. For PC application in which a user must access multiple resources, biometrics can greatly simplify the authentication process – the biometrics replaces multiple passwords, in theory reducing the burden on both the user and the system administrator. Biometric authentication also allows for association of higher levels of rights and privileges with a successful authentication. Highly sensitive information can more readily be made available on a biometrically protected network than on one protected by passwords.
4. Increased Accountability. Using biometrics to secure computers and facilities eliminates phenomena such as buddy punching and provide a high degree of certainty as to what user accessed what computer at what time.
5. Multiple Identities. Some systems, particularly those that dispense a government's social services programme, are obligated to provide service to qualifying individual within their jurisdiction. These individuals generally show up in person and request services. For many reasons, however, some people have found it profitable to register two or more times for the same benefit.
6. Identity Theft. This is the extreme case of authentication risk- when an attacker establishes new accounts that are attributed to a particular victim but authenticated by the

attacker. In a simple masquerade, the attacker may assume the victim's identity temporary in the context of system the victims already use. In an identity theft, the attacker collects personal identification information for a victim (name, social security number, date of birth, mother's maiden name, etc.) and uses it to assume the victim's identity in a broad range of transactions.

7. Fraud Detection; identification system is deployed to determine whether a person's biometric information exists more than once in a database. By locating and identifying individuals who have already registered for a program or services, biometrics can reduce fraud. In a public benefit program, for instance, a person may be able to register under multiple identities using fraudulent document. A person can also obtain fraudulent identification such as a driver's license. Without biometrics, there is no way to be certain that a person is not electronically registered under a different identity.
8. Fraud Deterrence. Perhaps even more than fraud detection, fraud deterrence is a primary benefit in large scale identification systems. It can be difficult to return a highly certain match against millions of existing biometrics records; in some cases, the error rates in large scale identification systems can run into the single digits much higher than would be acceptable in verification applications. If the presence of biometric identification technology can deter individuals from attempting to enrol multiple times in a public benefit or driver's licenses system, then the public agency has saved money and ensured the integrity of its records. In the absence of biometrics, there is no effective way of identifying duplication application/registration and it is difficult to determine such applications.

Pierrard and Vetter, [4], said behavioural and physiological characteristics are regularly used to manually verify or determine identity- this is something that humans do every day when greeting friends or check an ID card. Biometric technologies, by contrast, are automated – computers or machines used to verify or determine identity through behavioural or physiological characteristics. Because the process is automated, biometric authentication generally requires only a few seconds, and biometric systems are able to compare thousands of records per seconds. A forensic investigator performing a visual match against an ink fingerprint is not performing biometric authentication. By contrast, a system wherein a user places his or her finger on a reader and a match/non-match decision is rendered in real time, is performing biometric authentication.

However, Faundez-Zanuy [5] highlights one of the main drawbacks to biometric security system by maintaining that although biometrics offers enormous benefits, yet its adoption has not been able to grow accordingly. The focus or critical issue is that biometric data is not secret and as such cannot be replaced after being compromised by a third party. This demerit was traceable to remote applications such as internet, some kind of liveness detection and as such anti-

replay attack mechanisms should be provided. According to the argument, this kind of deployment is an emerging research topic [5].

In a recent research the vulnerability of fingerprint recognition systems to dictionary attacks based on Master Prints has been demonstrated [6]. The report described Master Prints as real or synthetic fingerprints that can fortuitously match with a large number of fingerprints thereby undermining the security afforded by fingerprint systems. It generates complete image-level Master Prints known as Deep Master Prints, whose attack accuracy is found to be much superior than that of previous methods such as previous work by Roy et al. [7], which generated synthetic Master Prints at the feature-level.

## 2.2. Uniqueness of Fingerprints

The uniqueness and reliability of Fingerprints for biometric authentication has been submitted in Bose and Kabir [8] as such with the gold standard for personal identification within the forensic community for over one hundred years. Despite the discovery of DNA fingerprint, this concept has remained universal. The science of fingerprint identification has evolved over time spanning from the early use of finger prints to mark business transactions in ancient Babylonia to the modern use as core technology in biometric security devices and as scientific evidence in courts of law across the globe. The science of fingerprints, dactylography or dermatoglyphics, had long been widely accepted, and well acclaimed and reputed as panacea for individualization, particularly in forensic investigations [8, 9]. The report further appreciated human fingerprints as being detailed, unique, difficult to alter, and durable over the life of an individual, making them suitable as lifelong markers of human identity. Fingerprints can be readily used by police or other authorities to identify or unveil individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased, as in the aftermath of a natural disaster [8].

According to Hu, Li, Ma, and Zhang, [10], fingerprint based personal identification has been routinely used in forensic laboratories and identification units around the world and it has been generally accepted. The following five factors should be considered when assessing reliability:

1. Whether any particular technique or methodology in question has been subject to a statistical hypothesis testing.
2. Whether its error-rate has been established.
3. Whether the standards controlling the technique's operations exist and have been maintained.
4. Whether it has been peer reviewed, and published.
5. Whether it has a general widespread acceptance.

The two fundamental premises on which fingerprint identification is based are

- a. Fingerprint details are permanent.
- b. Fingerprints of an individual are unique.

The validity of the first premise has been established based on the anatomy and morphogenesis of friction ridge skin. The

second premise is debatable. The notion of fingerprint uniqueness has been widely accepted based on manual inspection (by dactyloscopic experts) of millions of fingers.

The degree of similarity depends on typical intra-class variations observed in multiple impressions of a finger.

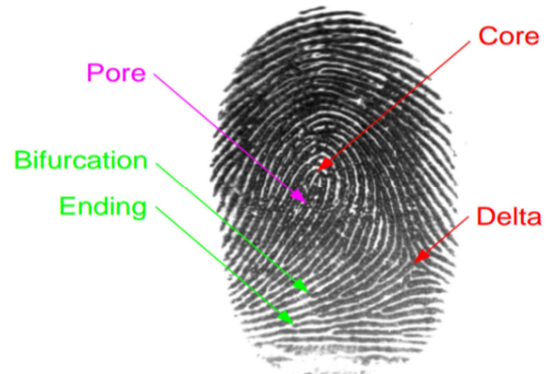


Figure 3. A fingerprint image with typical features.

In order to solve the problem of uniqueness, it is necessary to define the representation of a fingerprint pattern and the similarity metric. Fingerprints can be represented by a large number of features including the overall ridge flow pattern, ridge frequency, location and position of singular points-core(s) and delta(s), type, direction, and location of minutiae points and ridge counts between the pairs of minutiae. The representation of fingerprints minutiae, which is exploited by forensic experts, has been demonstrated to be relatively stable and has been adopted by the majority of automatic fingerprint matching systems. The similarity metric is the number of corresponding minutiae between two minutiae sets.

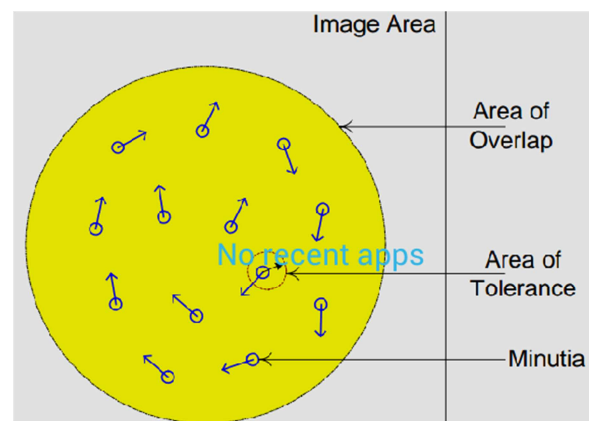


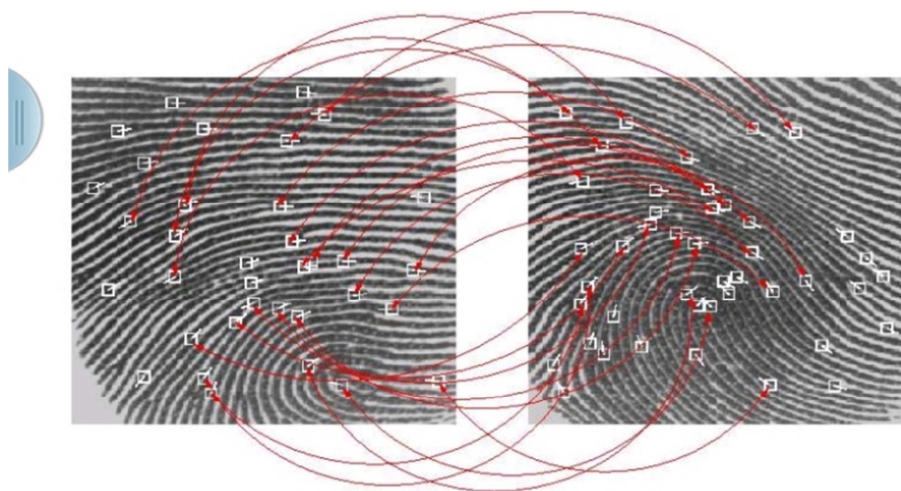
Figure 4. Fingerprint and its Minutiae.

There are two approaches for determining the uniqueness of the fingerprints. In the *empirical approach*, representative samples of fingerprints are collected and using a typical fingerprint matcher, the accuracy of the matcher on the samples provides an indication of the uniqueness of the fingerprint with respect to the matcher. In the *theoretical approach* to the estimation of uniqueness, all realistic phenomena affecting inter-class and intra-class pattern



variations are modelled. Given the similarity metric, it is then possible to estimate the probability of a false association. A theoretical formation of the fingerprint uniqueness model

based on a number of parameters derived from the database of fingerprint of fingerprint images has been proposed.



**Figure 5.** Automatic matching of minutiae.

### 2.2.1. Fingerprint Uniqueness (Background)

The problem of fingerprint uniqueness was first addressed by Galton in 1892, who considered a square region extending across six ridges in a given fingerprint. He assumed that a fingerprint can be covered by 24 on average such six-ridge wide independent square regions. Galton estimated that he could correctly reconstruct any of the regions with a probability of  $\frac{1}{2}$ , by looking at the surrounding ridges. According, the probability of a specific fingerprint configuration, based on the surrounding ridges, is  $(\frac{1}{2})^{24}$ . He multiplied this conditional probability with the probability of finding the surrounding ridges to obtain the probability of occurrence of a fingerprint.

Pearson argued that there could be 36 ( $6 \times 6$ ) possible minutiae locations within one of Galton's six-ridge-square regions, and replaced Galton's probability of a six-ridge-square region of by  $\frac{1}{36}$ . Several subsequent models are interrelated and are based on a fixed probability,  $p$ , for the occurrence of a minutia. Such models compute the probability of a particular  $N$ -minutiae fingerprint configuration as  $p$  (Fingerprint Configuration) =  $p^N$ , where  $p$  is a fixed probability for the occurrence of a minutia.

Osterburg divided fingerprints into discrete cells with the size  $1 \text{ mm} \times 1 \text{ mm}$ . He computed the frequencies of 13 types of minutiae events (including an empty cell) from 39 fingerprints (8,591 cells) and estimated that 12 ridge ending will match between two fingerprints based on an average fingerprint area of  $72 \text{ mm}^2$  with the probability  $1, 25.10^{-20}$ .

Stoney and Thirnton critically reviewed earlier fingerprint uniqueness models and attempted to characterize pairwise minutiae dependence. They proposed a linear ordering of minutiae and recursively estimated the probability of an  $n$ -minutiae configuration from the probability of a  $(n - 1)$ -minutiae configuration and the occurrence of a new minutiae of certain type/orientation at a particular distance/ridge counts from its nearest minutiae configuration from different

models are compared thus, an average size fingerprint has 24 regions ( $R = 24$ ) as defined by Galton, 72 regions ( $M = 72$ ) as defined by Osterburg, and has 36 minutiae on average ( $N = 36$ ).

### 2.2.2. Fingerprint Uniqueness Model

A model for obtaining a realistic and accurate probability of correspondence, the following assumptions should be made:

- Only two types of minutiae details will be considered: ridge endings and ridge bifurcations. The model does not distinguish between the two types of minutiae because it cannot accurately discriminate between each other. Since minutiae can reside only on ridges which follow certain "flow" pattern, the model evaluates the statistical dependence between minutiae directions and locations.
- Correspondence of a minutiae pair is an independent event and each correspondence is equally important.
- The fingerprint image quality is not taken into account since it is very difficult assign reliably a quality index to a fingerprint.

The fingerprint correspondence problem involves the process of matching a template fingerprint with an input fingerprint. It is assumed that a reasonable alignment can be established between the template and the input. The alignment of the input minutiae set with the template minutiae set is done under the condition that respective minutiae correspondence can be determined within a small tolerance.

### 2.2.3. Strength of Information from Fingerprint

In a technical report to the European Commission, Beslay, Galbally, and Haraksim [11] proposed experiments which was aimed to deepen the understanding regarding the physiological development of the fingertip ridge structure over time and its impact on automated fingerprint recognition. The experiments explore three biometric

processes in the light of age, ageing and growth effects. These effects are demonstrated and validated, resulting in a growth model which is developed and validated. From a quality point of view, it was concluded that children fingerprints show better quality than those of elderly. However, from a matching perspective, elderly fingerprints result in either as good as or even higher matching scores than children fingerprints ones. Both from a quality and a matching perspective, adult's fingerprints are clearly those that present the highest matching score.

In a paper, Muchtar et al. [12] appreciate that the fingerprint sensor can only identify the user's fingerprint registered in the sensor. This approach makes fingerprint recognition using a fingerprint sensor but from a centralized system. Therefore, with the aid of Arduino and Raspberry Pi, supporting data could be centralized to identify the user's fingerprint entirely and could perform fingerprint recognition in different fingerprint sensors. WebSocket is used to makes it possible to provision a variety of interactions between browsers and websites. With this method, two-way continuous conversations can be made between browsers and servers

The uniqueness of fingerprints was established only on the basis of experience and observation. Choi, Yang, Ro, and Plataniotis, [13] argued that three dactyloscopic axioms have been defined thus:

- There are no such two people in the world which would have an identical pattern structure of papillary lines.
- The pattern of papillary lines of any person remains relatively stable or unchanged for his or her whole life.
- The papillary lines regenerate with the growth of the skin. The papillary lines cannot be destroyed, only when very removal of the skin occurs.

The second dactyloscopic axiom has been proven by the medical science and has been examined, e.g., within the project BioFinger. The third dactyloscopic axiom has also been explained by the medical science.

However, the first dactyloscopic axiom is subject of ambiguity. The first obvious method how to prove the validity of the first axiom would be to compare all available

fingerprints in the world. But this is impossible. This axiom says that not only all people living in the world have different fingerprints, but that each human has the fingerprint which is at least a little bit different from some other fingerprint. Most fingerprints are not likely to be compared, although there are huge amounts of fingerprints saved in criminal police database. These fingerprints are mostly rolled inked fingerprints or latent fingerprints, i.e. they contain more information than live-scan fingerprints. The second method would be to find some theoretical model, which describes the uniqueness of the fingerprint, so that it would be possible to determine the validity of the first dactyloscopic axiom. Another type of uniqueness is needed for cryptographic tasks, namely the uniqueness for random sequence, or more precisely for cryptographic key generation. The main question which should be answered is: is there enough usable information hidden in a biometric pattern and is such information suitable for cryptographic purpose? It is well established that random information can be used as the cryptographic key data as long as it is unpredictable and unguessable.

### 2.3. Biometric Security System

Jaewon, Takeo, and Daijin [14] have maintained that the Biometric Security System consists of a general Biometric System (based on fingerprints in the case) and a general cryptographic system. A new special step, an art of pipe through both systems, has been developed and tested. This connecting step corresponds to the key generation from the fingerprint. The Biometric System acquires and processes biometric data (fingerprint images). Then a key is generated in an intermediate step and such key is delivered to the cryptographic module at the end. These three main steps are schematically shown in Figure 6. Any biometric attributes can be used as the input biometric information, as it has been said in the general introduction of the selected biometric attribute. If there is not enough entropy information, it is impossible to generate strong cryptographic keys, even if the process of key generation is realizable.



Figure 6. Three main phase of the Biometric Security System.

Besides, the individual phases shown above can be described in a more detailed way. In the first phase, called Acquirement, not only fingerprint scanning, but also all image processing algorithms are applied with the aim to extract the minutiae points with their characteristic's information data (position, gradient and type). The second phase called Key Generation is dedicated to biometric key generation. The minutiae from the previous phase are taken as an input and some mathematical operations are done with them. These mathematical operations generate sub-vectors from the set of minutiae points and these sub-vectors can be considered as keys. Although it is not absolutely necessary to generate more sub-vectors, as a single vector representing the whole minutiae set would be theoretically sufficient, it is not recommendable to be limited to such single vector. As the output of the second phase, the set of sub-vectors is processed by a cryptographic module. Well-tried cryptographic modules exist and therefore is not necessary to develop an own cryptomodule. That is why some common cryptographic algorithm can be used, such as DES or 3DES (only symmetric cryptography is considered further).

In order to make it more complicated, the whole Biometric Security System must be divided into two separate concepts. The first one is the Certificate Creation concept, and the second one is the Certificate Usage concept. Both concepts have some common steps, but there are some differences in these two main parts of the Biometric Security System. Both concepts consist of the same phases as discussed above (i.e. Acquirement, Key Generation and Cryptomodule). But the difference is visible in each phase, and indeed, the execution and handling modes are not identical.

#### **2.4. System Design Consideration (Present/Existing System)**

The most frequently used authentication methods are passwords and PINs. They secure access to personal computers (PCs), networks, and applications; control entry to secure areas of a building; and authorize automatic teller machine (ATM) and debit transactions. Handheld tokens (such as cards and key fobs) have replaced passwords in some higher-security applications. Physical authentication devices such as smart cards and password tokens were developed in order to eliminate certain weaknesses associated with passwords. However, passwords, PINs, and tokens or cards have a number of problems that call into question their suitability for modern applications, particularly high-security applications such as access to online financial accounts or medical data. What benefits does the biometrics provide compared to these authentication methods?

All data inputs from the user for the existing system are in (hard) paper forms and they all contain written inputs from the user and the system. For instance, a person needs to access a system, the person or user is given a check-in form tagged AS FORM UFP-11F as a case may be; this is a paper form stored in file and folders.

##### **2.4.1. Digital Enhancement Biometrics**

The performance of currently available minutiae extraction algorithms depends heavily on the quality of input images. In an ideal fingerprint image, ridges can be easily detected and minutiae can be precisely located from the thinned ridges. However, in practice, due to the factors of sensor environment and the state of human finger, a significant percentage of acquired fingerprint images (approximately 10%) are of poor quality. The ridges structures in poor-quality fingerprint images are not always well-defined and hence they cannot be correctly detected. It is therefore necessary to use a digital image enhancement algorithm which can improve the clarity of the ridge structures of input fingerprint images.

##### **2.4.2. Storage**

For the existing system, storage is entirely by memorizing Password, PIN and Token by using figure, letters, symbols, and numbers that is remarkable to the user such as birthday, wedding day etc which is easily compromised and sometimes they are stored in diaries, phones, other devices, files and folders in physical storage cabinets.

One of the reasons passwords are kept simple (and are then subject to compromise) is that they are easily forgotten. Tokens and cards can be forgotten as well.

##### **2.4.3. Outputs of the Existing System.**

The Output of the Existing System includes;

- a. Create password.
- b. Create and Change PIN and Token.
- c. Generate authentication.

##### **2.4.4. Analysis of the Anticipated System**

The anticipated system is a Biometric Security System is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and/or behavioural characteristics possessed by the person, an important issue in designing a practical biometric system is to determine how an individual is recognized. Depending on the application context, a biometric system may be called either a verification or identification system.

##### **2.4.5. Strength of Fingerprint Information**

Although the word fingerprint is popularly perceived as a synonym for individuality, the uniqueness of fingerprint is not a proven fact but an empirical observation. With the accepted widespread use of fingerprints, however, there is a rightfully growing public concern about the scientific basis associated with the uniqueness of fingerprints. Widespread doubts of general public in this regard would have disastrous consequences, especially if fingerprints are to be commonly used for unambiguous identification of a person due to their efficiency, convenience and reliability in fighting constantly increasing identity fraud in the society. Furthermore, automated fingerprint matching systems do not use the whole differentiating information contained in the fingerprints, but only sectional representation extracted by a machine unsupervised by human fingerprint experts.



#### 2.4.6. Weakness of the Existing System

The most frequently used authentication methods are passwords and PINs in the present system. They secure access to personal computers (PCs), networks, and applications; control entry to secure areas of a building; and authorize automatic teller machine (ATM) and debit transactions. Handheld tokens (such as cards and key fobs) have replaced passwords in some higher-security applications. Physical authentication devices such as smart cards and password tokens were developed in order to eliminate certain weaknesses associated with passwords. However, passwords, PINs, and tokens or cards have a number of problems that call into question their suitability for modern applications, particularly high-security applications such as access to online financial accounts or medical data. The present system uses the *Traditional authentication methods, in theory*, a password is memorized by a single person, it's hard to guess, it's never written down, and it's never shared. *In practice*, however, people constantly violate these expectations. Password and PINs are easily guessed or compromised; tokens can be stolen. Many users select obvious words or numbers for password or PIN authentication, so that an unauthorized user may be able to break into an account with little effort. In addition, many users write password in conspicuous places, especially as the number of passwords users must manage continually increases. "Good password", i.e. long passwords with numbers and symbols, are too difficult to remember for most users and are rarely enforced.

Passwords, PINs and tokens can also be shared, which increases the likelihood of malicious or unaccountable use. In many enterprises, a common password is shared among administrators to facilitate system administration. Unfortunately, because there is no certainty as to who is using a shared password or token or whether the user is even authorized – security and accountability are greatly reduced.

In the present system, one of the reasons passwords are kept simple (and are then subject to compromise) is that they are easily forgotten. Tokens and cards can be forgotten as well; though keeping them attached to keychain reduces this risk.

#### 2.5. Uses of Biometric Security System

Biometric Systems have been specially applied in three different aspects [15]. These are:

- a. Commercial uses: Application include authentication in online banking services or ATM, credit card usage, e-commerce, mobile phone, distance learning, access to health care systems, etc.
- b. Government purposes: Typically, in issuing Official ID cards, driver's licenses, social benefits, National ID cards, homeland security.
- c. Forensic uses: Including body identification, criminal purposes, parenting determination and lost persons [15, 8].

### 3. Method

This research work was carried out by reviewing relevant literatures on Fingerprint biometric security system. Then a survey, using questionnaire, interview and observation techniques was carried out, to assess the implementation of the fingerprint recognition technology for a biometric security system at the Council for the Regulation of Engineering in Nigeria (COREN). The interview and observation techniques were used as tools to verify and validate the responses obtained from the administration of questionnaire. Questionnaires were collected from the respondents, after the validation and coding. The research questionnaires were administered to 20 employees of Council for Regulation of Engineering in Nigeria (COREN).

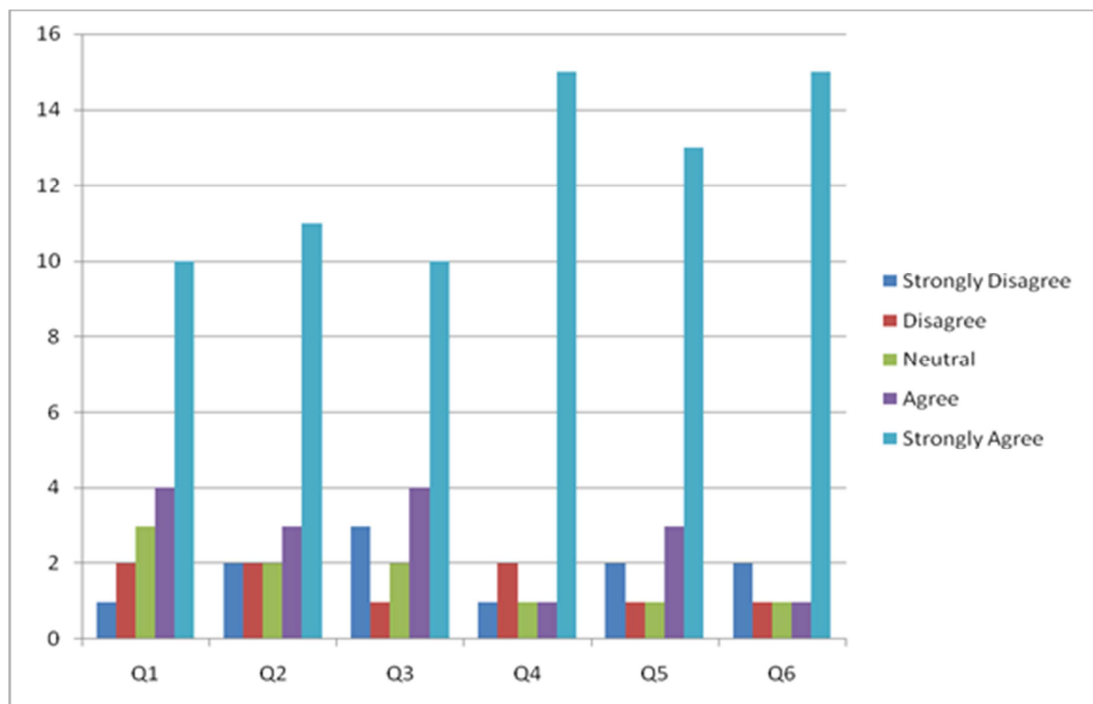
The Likert items (i.e. each question asked in the questionnaires) provided metrics on which the performance parameters for the evaluation of this model were formulated. Data from the dully filled questionnaire were captured, compiled and analysed using Microsoft Excel. Descriptive statistics (such as frequency distribution, and percentages) was used to determine the relationship between the variables.

### 4. Result and Discussion

The developed system was tested for 20 employees of Council for Regulation of Engineering in Nigeria (COREN). There were six (6) closed questions. The Likert items (i.e. each question asked in the questionnaires) provided metrics on which the performance parameters for the evaluation of this model were formulated. Survey targets were set for each evaluation parameter of the developed model. The respondents gave objective measure of the adequacy of the model based on the parameters. Twenty (20) responses were received from the respondents and data from the dully filled questionnaire were captured, compiled and analysed using Microsoft Excel. The result of data analysis of individual Likert items is as presented in Table 1. The first column of each table represents the question number of an item on the questionnaire. For example, Q1, Q2, Q3, Q4, Q5 and Q6 represent questions one, two, three, four, five and six respectively, while data in the split cells represent the frequency of the responses in number and its equivalent percentage. The response means and response mode depicts the overall user's satisfaction with most of the features of the developed model. The mean and modal values of response are in the upper classes of the rating scale. In general, responses showed that the model is acceptable by COREN staff because of its efficiency, increased security, increased convenience, reduce fraud, or delivery of enhanced services as shown by response of item 1, 2, 3, 4, 5 and 6 respectively. The data of the Likert item of Table 1 was subjected to statistical analysis using column chart as shown in Figure 7.

**Table 1.** Data Analysis of the Administered Questionnaire.

Q	Likert Items	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Response Mean	Response Mode
Q1	Do demographic factors (e.g. age, sex, marital status) have impacts on user preferences for fingerprint Recognition Technology for Biometric Security System?	1	2	3	4	10	4.00	5
Q2	There are more limitations to the traditional authentication method (such as Password, PIN, and Token) than the fingerprint Recognition Technology for Biometric Security System?	2	2	2	3	11	3.95	5
Q3	The capacity of developed authentication technology using fingerprint Recognition Technology for Biometric Security System gained sufficient improvement on the existing traditional method?	3	1	2	4	10	3.85	5
Q4	Fingerprint Recognition Technology is the best form of Biometric Security System	1	2	1	1	15	3.75	5
Q5	The fingerprint Recognition Technology for Biometric Security System has significant impact on corporate image, infrastructural and resource management to justify initial cost of deployment?	2	1	1	3	13	3.25	5
Q6	Do you think the use of fingerprint Recognition Technology for Biometric Security System will solve security and privacy issues?	2	1	1	1	15	3.75	5



**Figure 7.** Representation of Numeric Frequency of Response of Table 1.

In a nutshell, it can be inferred that a reliable, secure, fast and an efficient system had been successfully developed. It is a system that could replace the present traditional methods such as passwords and PINs as can be shown by the bars of the chart in Figure 7.

## 5. Conclusion

### 5.1. Concluding Statements

The biometric technologies are at the beginning of their

broad practical application. There are many biometric attributes, such as fingerprint, face, retina, iris, voice etc., which can be used for the verification of systems (access systems). At the moment, it seems that the most required systems based on such biometric verification method relates to personal document applications allowing a person to be verified or identified (in this case, its identity is unknown at the beginning), e.g. for border control purposes. However, the limitations are not only to verification or identification systems: an integration is possible of a biometric system into

a cryptographic system (or otherwise) and thus obtain a biometric security system.

### 5.2. Recommendations

It is recommended that:

- a. For this system and any other further system related to this should be maintained and managed by a System Engineer in other to maintain proper Biometric data integrity.
- b. Every sensor technology should maintain standard in acquiring, matching, enrollment and minutiae extraction to enable effective input processing.
- c. Every related system maintains and share Biometric information for inter-organization data sharing; for referential purposes, to increase security, and reduce time wasted.
- d. More work should be done on the aspect of signatures, certificate creation and fingerprints in the form of referential integrity and identification and verification of system user.
- e. Moves should be made to establish and solidify the national Biometric Security System database for comprehensive database of all Biometric of citizen in the country for referencing, security purposes and easy identification.
- f. It strongly recommended that all five listed above should be implemented to establish more trust worthy Biometric Security System in the Nigeria.

### 5.3. Direction for Future Studies

Based on the contributions of this paper, the following research directions appear promising. Additional features such as Car Ignition System, Security Doors of the fingerprint-based matching should be considered. This will improve the matching accuracy with fingerprints and enable more reliable fingerprint image retrieval. The fingerprint image retrieval system can be combined with other robust fingerprint matchers for faster search. Since each fingerprint is locally defined, minutiae can be easily used in matching and retrieval given partial fingerprint. The deployed fingerprint detection and matching system should be evaluated in an image-based recognition system. The fingerprint-based matching techniques can be combined to build a unified system for video and signature-based fingerprint recognition.

## References

- [1] Jain, A., Dass, S. C. & Nandakumar, K. (2004). "Soft biometric traits for personal recognition system," in Proc. ICBA, 2004, vol. 3072, LNCS, pp. 731-738.
- [2] Opara, E. U., Rob, M. & Etnyre, V. (2016). Biometric and Systems Security: An Overview of End-To-End Security System. *Communications of the IIMA* Vol. 6, no. 2, pp. 53-57.
- [3] Kumar, A., Berg, A. C., Belhumeur, P. N. & Nayar, S. K. (2009). "Attribute and simile classifiers for face verification," in IEEE Int. Conf. Computer Vision (ICCV), 2009, pp. 1-8.
- [4] Pierrard, B. S. & Vetter, T. (2007). "Skin detail analysis for face recognition," in Proc. CVPR, 2007, pp. 1-8.
- [5] Faundez-Zanuy, M. (2016). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, Vol. 21 no 6, pp. 15-26, ISSN: 0885-8985. June 2006.
- [6] Bontrager, P., Roy, A., Togelius, J., Memon, N. & Ross, A. (2018). DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. Retrieved November 23, 2018 from <https://arxiv.org/pdf/1705.07386.pdf>
- [7] Roy, A., Memon, N., Togelius, J., & Ross, A. (2018). Evolutionary methods for generating synthetic masterprint templates: Dictionary attack in fingerprint recognition. In International Conference on Biometrics, pages 1-8, 2018.
- [8] Bose, P. K. & Kabir, M. J. (2017). Fingerprint: A Unique and Reliable Method for Identification. *Journal of Enam Medical College* Vol 7 No 1 January 2017. Retrieved November 23, 2018 from doi: <http://dx.doi.org/10.3329/jemc.v7i1.30748>
- [9] Thompson, W. C., Vuille, J., Taroni, F. & Biedermann, A. (2018). After Uniqueness: The Evolution of Forensic-Science Opinions. *Judicature*. Vol. 102 No 1 Spring 2018. Retrieved November 23, 2018 from <https://judicialstudies.duke.edu/wp-content/uploads/2018/04/JUDICATURE102.1-THOMPSON-et-al-1.pdf>
- [10] Hu, Y., Li, M., Ma, W. & Zhang, H. (2004). "Efficient propagation for face annotation in family albums," in Proc. ACM Int. Conf. Multimedia, 2004, pp. 716-723.
- [11] Beslay, L. Galbally, J. & Haraksim, R. (2018). Automatic fingerprint recognition: from children to elderly. Ageing and age effects. JRC Technical Report, the European Commission's science and knowledge service. ISBN 978-92-79-87179-5 ISSN 1831-9424. Retrieved November 23, 2018 from doi: 10.2760/809183.
- [12] Muchtar, M. A., Seniman, D Arisandi, D. & Hasanah, S. (2018). Attendance fingerprint identification system using arduino and single board computer. *IOP Conf. Series: Journal of Physics: Conf. Series* 978 (2018) 012060 doi : 10.1088/1742-6596/978/1/012060.
- [13] Choi, J. Y., Yang, S., Ro, Y. M. & Plataniotis, K. N. (2008). "Face annotation for personal photos using context-assisted face recognition," in Proc.ACM Int. Conf. Multimedia Information Retrieval, 2008, pp. 44-51.
- [14] Jaewon- Sung, T. Takeo, K., & Daijin, K. (2007). "A Unified Gradient-Based Approach for Combining ASM into AAM" *International Journal of Computer Vision* 75 (2), 297-309, 2007.
- [15] ŐSZI, A. & RUIZ, L. S. (2016). Biometric Uses in Occupational Safety and Health. Vol. 11 no 4, December 2016. Retrieved November 23, 2018 from [http://hadmernok.hu/164\\_01\\_arnold.pdf](http://hadmernok.hu/164_01_arnold.pdf)