Journal of Education and Practice
ISSN 2222-1735 (Paper) ISSN 2222-288X (Online)
Vol.7, No.28, 2016


# Public Enlightenment Education on the acceptance of Fingerprint Biometric Technology for administration in academic institutions and other organizations

Samuel Godwin Eze[1]* Edmond Ogochukwu Chijioke[2]

3. Department of Health and Physical Education, Faculty of Education, Enugu State University of Science and Technology, Agbani, Enugu, Nigeria

4. Department of Urban and Regional Planning, Faculty of Environmental Sciences, Enugu State University of Science and Technology, Agbani, Enugu, Nigeria

*The research is financed by Tenece Professional Services Ltd. Enugu, Nigeria*

**Abstract**

This research presents the overview of the origin of fingerprint biometric technology, the opinion of the public on the acceptance of fingerprint biometric technology and the means of instilling confidence on the public for the total acceptance of the technology. Data was collected with the aid of a lecture and structured questionnaires distributed to 50 respondents in NewLine Computer training Center Ltd. Abakpa. There were lectures and interviews conducted by the researcher and questionnaires completion by the selected population of 50 people comprising of age between 18 and 65 years. The 50 people consist of individuals from education, technology and government organisations. The organisation was done by the Researchers and three members of staff of NewLine Computer training Center Ltd. Abakpa Nike Enugu. The lectures enlightened the 50 participants/respondents that fingerprint is a discontinuous variation and that no two persons have exactly the same fingerprint. The study revealed that it is obvious that confidence will be instilled in the public if there is public enlightenment as the number of respondents who believe that fingerprint cannot be stolen or copied is 92% although 8% of the respondents is still biased after the lectures. The research will instil confidence in the use of fingerprint biometric technology and will break the shackles of currently being a misunderstood novelty to a widespread, mainstream personal identity authentication tool.

Keywords: Authentication, Biometric Technology, Chip Implantation, Fingerprint Acquisition, Identity Management.

## 1. Introduction

Fingerprint biometric technology is an emerging technology for secured identity management. The evolution of information technology is likely to result in intimate interdependence between humans and technology. This fusion has been characterized in popular science fiction as chip implantation. Some applications of biometric identification technology are now cost-effective, reliable and highly accurate and as a result, biometric systems are being developed in many countries for such purposes as social security entitlement, payments, immigration control and election management (Simon, G.D 1994).

According to Anil, K. J. (2007), whether in passports, credit cards, laptops or mobile phones, automated methods of identifying people through their anatomical features or behavioural traits are an increasing feature of modern life.

Biometrics is gaining increasing attention as organizations search for more secure authentication methods for user access, e-commerce and other security applications,. A company that adopts a biometric technology should choose the type of applications since different applications require different biometrics. One needs to navigate through some complex vendor products and keep an eye on future developments in technology and standards to select the right biometric for your situation (Liu S. and Silverman M. 2001).

### 1.1 Background of the study

The Automated fingerprint recognition was first developed by the FBI in the late 1960s and implemented in the early 1970s. The Federal Bureau of Investigation (FBI) moved to develop a system to automate its fingerprint identification process in 1969 and contracted the National Institute of Standards and Technology (NIST) to study

 

the process of automating fingerprint classification, searching, and matching. NIST identified two key challenges:

- scanning fingerprint cards and extracting minutiae from each fingerprint
- searching, comparing, and matching lists of minutiae against large repositories of fingerprints (John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, 2003).

### 1.2 Statement of the Problem

Unsecured identity management has resulted in:

- the breaking into the privacy of public through internet hacking in recent times,
- the deletion of important security information of a victim,
- the doctoring of personal details of students in academic institution, and
- the suspicion of the biometric data of a true passport holder.

### 1.3 Aim and Objectives of the Study

The study is aimed at understanding the perception of public on fingerprint biometric technology with the objective of instilling the public confidence on the acceptance of fingerprint biometric technology as the most secured form of identity protection information technology.

## 2. Literature Review

The literature review addresses three areas of the research problem:

i) social issues with respect to fingerprint biometric technology,

ii) Security concerns, and

iii) human factors (fingerprint individuality, age and gender)

### 2.1 Social Issues

Bolle et. al (2004) suggested that misconceptions, misunderstandings and false belief about the fingerprint biometric Technology are some social issues militating against its implementation and utilization worldwide. These are impediments to the technology's proliferation.

Any technology will likely be unaccepted if the user population has personal security uncertainties or believes the technology is intrusive in any way. Similarly, individuals' conceptions of what fingerprints in a fingerprint biometric system will be used for will greatly impact whether the system is accepted, and will ultimately determine the degree to which the technology will be embraced by the general public. In terms of social acceptance, fingerprint biometric technology ranks low to medium when compared to other biometric technologies. Acceptance is largely based on the ease of enrolment and is an obvious threat to personal privacy (Chirillo et. al. 2003).

The key to increasing the technology's acceptance is to figure out how such perceptions can be alleviated. According to some researchers, the best way to overcome a user's preconceived notions of a system is good communication. The user's concerns need to be addressed and the system's use and benefits needs to be enumerated. Before any type of education can be designed to effectively help users accept the technology, all potential concerns of the users must be understood (Ashbourn 2004).

### 2.2 Security Concerns

Lia B. and John D. W. (2003) stated that the right to privacy is one of our most cherished freedoms and as society has grown more complex and people have become more interconnected in every way, we have had to work even harder to respect privacy, the dignity, and the autonomy of each individual. Security and concerns over protecting personal identity are major issues to consider when implementing a fingerprint biometric system. Fingerprints are more difficult to steal and copy than a password, but the level of acceptance is low because most people have not understood that no two persons have got exactly the same fingerprints.

Chirillo et. al (2003) stated that it is important for the users to understand that "fingerprint templates are algorithmic representations of a fingerprint but cannot be used in reverse fashion to re-create the pattern of a fingerprint." Understanding this may help to reduce the level of perceived security risk and bolster the level of perceived security of fingerprint biometric systems.

### 2.3 Human Factors

Human factors refer to the age, gender and fingerprint individuality. Human factors have never been greatly recognized as factors affecting the acceptance of fingerprint biometric technology. However, human factors play a role in the accuracy of fingerprint biometric technology and consequently play a part in the level to which the technology is used in society and commerce.

#### 2.3.1 Fingerprint Individuality

Prindle (2005) asserted that all fingerprints are unique and no two are exactly identical and even identical twins have different fingerprint. However, this assertion does not prove 100% accuracy because of mutilation, damage and worn-out of fingerprints. Jain, A.K, Ross A, and Prabhakar, S. (2004) stated that it is generally conceded that a substitute to biometrics for positive identification in integrated security applications is non-existent. Cappelli, R. et. al. (2007) and Ross, A. et. al. (2007) affirmed that industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enroll a data subject cannot be reconstructed from stored templates.

#### 2.3.2 Gender Factors

Ashbourn (2004) observed that women generally tend to have smaller fingers and longer fingernails than men. It was also noted that certain fingerprint scanner may have difficulty obtaining a good sample of a fingerprint because of the size of the fingertip. However, this has not been proven conclusively and further research could be done to establish whether or not gender has an appreciable impact on the accuracy of fingerprint biometric systems.

#### 2.3.3 Age Factors

Ashbourn (2004) observed that age affects and denatures fingerprint. As people get old, their fingerprints becomes less pronounced due to the increased brittleness and decreased elasticity of the skin. Such degradation of the skin can result in poor fingerprint acquisition, template creation, and template matching from the original sample.

## 3. Study Area

The study was carried out at NewLine Computer Training Center Ltd. Abakpa Nike, Enugu. Lectures and interviews were conducted for population of 50 people (18 to 65 years). The questionnaires were distributed after the lectures to the population which consist of individuals from education, technology and government organisations. The organisation was done by the Researcher and three members of staff of management of NewLine Computer Training Center Ltd. Abakpa Nike, Enugu.

## 4. Research Methodology

Qualitative research approach which involves real-time survey was adopted for the purpose of this research in order to allow the full participation of the Researcher in the understanding of the perception of the participants to fingerprint biometric technology. There were 2 days Lectures on fingerprint biometric technology. 3 hours lectures with photographic illustrations were given to the 50 participants each day. Interviews were conducted and there were full time observations of the participants. Structured questionnaires relevant to the study were also distributed to the 50 participants selected.

 

## 5. Data Presentation and Analyses

The research questions and responses from the chosen population were presented in the tables below and analysed.

**Table 5.1: Research Question 1**

| *Question 1: To what level does the characteristics of fingerprint understood after the lecture.* | |
|---|---|
| Well Understood | 42 |
| Not Understood | 7 |
| Cannot say | 1 |
| No. of Respondents | 50 |

Source: Researchers field survey (2016)

From table 5.1, 84% of the chosen population understood the characteristics of fingerprint after the lecture, 14% of the participants did not understand the characteristics of fingerprint while 2% of the participants is biased about the understanding of the characteristics of fingerprint.

**Table 5.2: Research Question 2**

| *Question 2: To what level do the principles of the use of fingerprint biometric technology for identity management understood after the lecture?* | |
|---|---|
| Well Understood | 40 |
| Not Understood | 3 |
| Cannot say | 7 |
| No. of Respondents | 50 |

Source: Researchers field survey (2016)

From table 5.2, 80% of the chosen population understood well the principles on which the biometric technology operations lie. However, only 6% of the chosen population did not understand the principle and 14% is biased about the technology.

**Table 5.3: Research Question 3**

| *Question 3: How many times have you been a victim of identity theft in information technology?* | |
|---|---|
| Once | 10 |
| 3- 10 times | 4 |
| Uncountable times | 0 |
| None | 36 |
| No. of Respondents | 50 |

Source: Researchers field survey (2016)

From Table 5.3, greatest proportion of the chosen population (72%) confirmed that they were never victims of identity theft while 20% of the population said they experience identity theft once while 8% confirmed that they had been victims of identity theft about 3 to 10 times.

**Table 5.4: Research Question 4**

| *Question 4: To what degree do you consider security more important than convenience?* | |
|---|---|
| Highly Considered | 42 |
| Considered | 6 |
| Cannot say | 2 |
| No. of Respondents | 50 |

Source: Researchers field survey (2016)

From Table 5.4, 84% of the participants consider security highly important, 12% of the participants consider security more important than convenience while only 4% of the participant cannot say whether security is more important than convenience.

 

**Table 5.5: Research Question 5**

| *Question 5: How familiar are you with biometrics in general?* | |
|---|---|
| Very familiar | 28 |
| Familiar | 3 |
| Not Familiar | 19 |
| No. of Respondents | 50 |

Source: Researchers field survey (2016)

From Table 5.5, the study revealed that 56% of the chosen population is very familiar with the technology, 6% of the chosen population has a basic knowledge of biometrics, while 38% of the chosen population is not familiar with biometric technology.

**Table 5.6: Research Question 6**

| *Question 6: What level of consideration do you have about using your fingerprint for identification purposes after the lecture?* | |
|---|---|
| Highly Considered | 45 |
| Considered | 4 |
| Cannot say | 1 |
| No. of Respondents | 50 |

Source: Researchers field survey (2016)

Table 5.6 shows that the study has greatly changed the perception of the public and enlightened the public on the use of fingerprint biometric technology as 90% of the chosen population was convinced on the technology as a well-secured means of identity management while only 2% are still doubtful about fingerprint for the purpose of identification.

**Table 5.7: Research Question 7**

| *Question 7: After the lectures on fingerprint as a discontinuous variation, how easy do you think it is for fingerprints to be stolen or copied?* | |
|---|---|
| Very easy | 0 |
| Easy | 0 |
| Not easy | 46 |
| Cannot say | 4 |
| No. of Respondent | 50 |

Source: Researchers field survey (2016)

From table 5.7, it is obvious that confidence will be instilled on the public if there is public enlightenment as the number of people who believe that fingerprint cannot be stolen or copied is 92% although 8% is still biased after the lectures.

## 6. Conclusion and Recommendation

This chapter presents the conclusion drawn from the research and recommendation for further studies.

### 6.1 Conclusion

This research concludes that the level of user acceptance is the root cause of the lack of widespread recognition of fingerprint biometric technology throughout society and commerce. The organised lectures helped in giving the public in-depth knowledge on the fingerprint biometric technology and this if continues, will instil confidence on the use and acceptance of the technology all round the globe.

### 6.2 Recommendations

The following recommendations were made for further studies.

- Organisation of public enlightenment programme regularly on the use of fingerprint biometric technology as the most reliable means of identity management

 

- Dissemination of the vital information on the importance of identity management through advertising media such as television and newspapers
- Development of biometric system to replace password in personal data accessing in academic institutions since no two persons have the same fingerprints.
- Introduction of biometric technology in areas such as banking and industries where security is very important in order to instil confidence in the use of the technology.

## References

Anil, K.J. (2007), 'Technology: Biometric recognition', USA: Department of Computer Science and Engineering, Michigan State University, East Lansing Publications

Ashbourn, J. (2004), '*Practical Biometrics: From Aspiration to Implementation*', London: Springer Publications, Vol. 28, pp. 30-32, pp. 37-41, pg. 44.

Bolle, et. al (2004), *Guide to Biometrics,* New York: Springer-Verlag Publication, pp. (130, 139, 146, 153, 161, 212-218, 223, 241-242, 333)

Cappelli R, Lumini A, Maio D, Maltoni D (2007), 'Fingerprint image reconstruction from standard templates', *IEEE Trans Pattern Anal Mach Intell*, vol. 29, Issue 9, pp. 1489-1503.

Chirillo, et. al (2003), '*Implementing Biometric Security*', Indianapolis: Wiley Publishing, Inc. Pp. (16, 19, 20-22, 24-25)

Jain, A.K, Ross A, and Prabhakar, S. (2004), 'An introduction to biometric recognition', *IEEE Trans Circ Syst Video Technol* 2004, vol. 14, pp. 4-20.

John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins ( 2003), '*Biometrics*', New York: McGraw Publication.
Lia B. and John D. W. (2003), '*Biometrics: Identity Assurance in the Information Age'*, California: McGraw-Hill/Osborne Publications

Liu S. and Silverman M. (2001), 'A practical guide to biometric security technology', '*Information Technology Professional Journal , Vol. 3 issue 1, pp. 27 - 32*

Prindle, P. (2005) '*Twins and Fingerprints'*, Available www.multiples.about.com/cs/funfacts/a/twinfingerprint.htm [Assessed 15 April 2016]

Ross A, Shah J, Jain AK (2007), 'From template to image: reconstructing fingerprints from minutiae points', *IEEE Trans Pattern Anal Mach Intell*, vol. 29, Issue 4, pp. 544-560.

Simon, G.D, (1994), 'Touching Big Brother: How Biometric Technology Will Fuse Flesh & Machine', *Journal of Information Technology & People*, Vol. 7 Issue 4, pp.38 – 47