



# INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES



## Effect of Ease of Use and Fallibility of Biometric Fingerprint Technology in Criminal Identification in Kenya

Monica Mwashumbe Tangai, Joyce Kaguta, Yongho Yi

To Link this Article: <http://dx.doi.org/10.6007/IJARBSS/v9-i3/5750>

DOI: 10.6007/IJARBSS/v9-i3/5750

*Received: 02 Feb 2019, Revised: 17 Feb 2019, Accepted: 30 Feb 2019*

Published Online: 03 March 2019

**In-Text Citation:** (Tangai, Kaguta, & Yi, 2019)

**To Cite this Article:** Tangai, M. M., Kaguta, J., & Yi, Y. (2019). Effect of Ease of Use and Fallibility of Biometric Fingerprint Technology in Criminal Identification in Kenya. *International Journal of Academic Research in Business and Social Sciences*, 9(3), 842–859.

**Copyright:** © 2019 The Author(s)

Published by Human Resource Management Academic Research Society ([www.hrmars.com](http://www.hrmars.com))

This article is published under the Creative Commons Attribution (CC BY 4.0) license. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this license may be seen at: <http://creativecommons.org/licenses/by/4.0/legalcode>

Vol. 9, No. 3, 2019, Pg. 842 - 859

<http://hrmars.com/index.php/pages/detail/IJARBSS>

JOURNAL HOMEPAGE

Full Terms & Conditions of access and use can be found at  
<http://hrmars.com/index.php/pages/detail/publication-ethics>



# INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES



## Effect of Ease of Use and Fallibility of Biometric Fingerprint Technology in Criminal Identification in Kenya

Monica Mwashumbe Tangai  
Dedan Kimathi University of Technology  
Email wawudatangai@gmail.com

Dr. Joyce Kaguta  
Institute of Criminology, Forensics and Security Studies  
Dedan Kimathi University of Technology

Prof. Yongho Yi  
Institute of Criminology, Forensics and Security Studies  
Dedan Kimathi University of Technology

### Abstract

The aim of this study was to assess the factors influencing the use of Biometric Fingerprint Technology in criminal identification in Kenya. The specific objectives for the study were to assess the effect of Ease of use and fallibility of biometric fingerprint technology on Criminal Identification in Kenya. The study was grounded on probability theory and technology acceptance model. The study used a census. The study targeted 140 fingerprint officers working at the National Registration Bureau at the Huduma Centers, National Registration Bureau headquarters, and Langata, Kariakor, Pumwani and Makadara stations. Primary data was collected using a self-administered semi-structured questionnaire. SPSS software version 22 was used to analyze the data. Descriptive and regression analysis were used. Multiple linear regressions were used to examine the effect of the variables on criminal identification. All the statistical tests were carried out at 5% level of significance. Correlation results revealed that Ease of use and fallibility of BFT positively and significantly influence criminal identification. Regression results showed that Ease of use of BFT positively and significantly influences Criminal Identification ( $\beta = 0.296$ , Sig = 0.000). Moreover, regression results revealed that Fallibility of biometric fingerprint technology had a positive and significant influence on Criminal Identification ( $\beta = 0.226$ , Sig = 0.000). The study recommends the management of National Registration Bureau to ensure that their fingerprint officers capture quality level fingerprint

impressions during the registration process using BFT in order to ensure that individuals are accurately authenticated thereby preventing and detecting criminal activities. Other means identification such as DNA should be incorporated as a change in environmental conditions causes fingerprints to be unrecognizable and in cases of cuts or burns or extreme weight gain or loss, higher level of deformity of fingers.

**Keywords:** *Ease of Use, Fallibility, Fingerprint Biometric Technology, Criminal Identification*

## Introduction

The realization of governments' efforts towards fighting fraud or providing civic services prudently depends on the affirmative and correct identification of their people and the capacity to infer and compare with the databases and material across government units and agencies. This is only probable if there is a general structure that lets people to be distinctively identified, (Saini & Kapoor, 2016). For the last one and a half decade, the integration of biometric technologies in regulating crimes has been rising continuously. From the year 2008, the Next Generation Identification (NGI) method was adopted and integrated by the Federal Bureau of Investigation (FBI).

Biometric tools can be used in different forms and in various areas of practice, (Peter *et al* (2011). Biometric technology has been employed at the various entry points for instance airports and the border to verify the identity of beings. Biometric technology is very fundamental in monitoring individuals coming in and leaving the state. This permits for the classification of criminals, terrorists or militants. In residential areas, biometric voice technology is applied in validating the individualities of authorized people, home owners or family members. The significance of Biometric technology is not limited to the provision of security but it also can be applied in other key areas of life for instance in the commercial industry like e-commerce and naval shipping segments. 2-D barcode biometrics technology has enabled the hypermarkets and stores keep track of their inventories by keeping the information of the specific items. The use of Biometrics technologies like 2-D barcode systems has tremendously simplified our life. In business, 2-D barcode systems have enabled the taking of stock inventories much simpler. Similarly, in learning institutions (libraries), 2-D barcode systems are useful in taking book inventories for issuing to the learners.

In today's world, institutions are using Biometric technologies to monitor work schedules of their staff especially their arrival and departure times. For instance, biometrics has been integrated in hourly and turnout processes to manage staffs who work on hourly shifts from logging in on behalf of their colleagues who have absconded. This has helped companies save costs in millions of dollars yearly. The use of biometrics to manage workers duty roster is widely used in casinos across states in North America to detect frauds.

The use of Biometric technologies for instance DNA matches and fingerprints have led to a very significant impact especially with regard to the regulating fraud over the past few years. Biometric technologies such as the ones engineered to battle the challenges brought about by terrorism related threats have been adopted nationally to ensure that implementation of the law, (Robyn *et al*, 2015). Moreover, developments in computing have resulted in broader forms of portable DNA and other biometric information gathering systems besides additional cost-effective solutions for keeping and distributing biometric information among state organizations. This speedy uptake in the advancement and application of biometric technological applications in policing devoid of monitoring

or control has led to anxieties about probable misapplications or abuses of such data. As the particulars of persons are put into the national and government biometric databases whether they have had an experience with the criminal justice system or not the massive growth of biometric databases have also led to suspicions on the simplicity with which any person can secure the backing of the United States criminal justice system, (Robyn *et al*, 2015).

The ease of use of biometric technology in Kenya has increased sharply. An example on the use of biometric technology in Kenya is UAP insurance, the first medical insurance to use Biometric technology but as at now more than 70% of the medical insurance companies have adopted the technology. The perceived ease of use of biometric technology in healthcare has a significant effect on the plan to use. Biometric technological systems are cheaper to maintain, self-efficient, smaller in size, have low power consumption capacity, easy to use and are non-intrusive. This increases the organizations intention to adopt Biometric technologies for authentication, (Malla, 2018).

### **National Registration Bureau of Kenya (NRB)**

According to the Directorate of Immigration and Registration of persons, The National Registration Bureau became a completely operational unit in 1978. It was empowered through the Registration of Persons Act (Cap.107) Laws of Kenya to classify, index and provide Identity cards to all the citizens of Kenya irrespective of sex given that they have attained the mandatory age of sixteen (16) years. The National Registration Bureau of Kenya (NRB) is one of the agencies under the Ministry of Interior and Co-ordination of National Government. The NRB is divided into four broad divisions which are; Training and Quality Assurance, Registration and Field Services, Production Services, Fingerprint Services and Administrative Services. The objective of the National Registration Bureau is to augment the National Security, Social and Political growth of the state by detecting, processing, giving identity cards to the citizens of Kenya with a mandatory age of eighteen (18) years and above, and maintaining an all-inclusive database for use by the government and authorized agencies, (<http://www.immigration.go.ke>)

The role of National Registration Bureau is to ascertain and document Kenyan citizens aged 18 years and above, generation and Issuance of valid ID cards, control of an all-inclusive database of all recorded people as well as recognition and deterrence of unlawful registration. The National Registration Bureau has a staff complement of about 4,800 officers of various professional cadres and educational qualifications. The two technical cadres are Registration Officers and Fingerprint officers. The Registration Officers deal mainly with the initial identification and registration of citizens through documentation at the initial stages in the field, whereas the Fingerprint Officers deal with the analysis and verification of the fingerprint data.

The Registration of Persons Act (Cap. 107) mandates NRB under the Fingerprint Services Function to carry out fingerprint identification creation, classification and maintenance of automated and manual fingerprint records. The NRB Fingerprint Services is mandated to prepare and present fingerprint marks for individual identification, detection of double or illegal registration through fingerprint search, analysis of documents and / or exhibits for fingerprint identification and other related documentary evidence for court proceedings. From the foregoing, it is clear that fingerprint biometric Technology plays a fundamental part in the identification of individuals and criminals in the National Registration Bureau.

### Statement of the Problem

The upsurge in the adoption of biometric technologies in combating fraud in various institutions such as banks, learning institutions and Directorate of criminal investigation calls into question the effectiveness of these technologies. Even though literary studies on biometric fingerprint technology are scanty and far-fetched, this study sought to assess the factors influencing the use of Biometric Fingerprint Technology in criminal identification in Kenya. The acceptance of Biometric applications for instance the matching of fingerprint and DNA have contributed significantly in monitoring and supervision over the recent past, and biometric equipment such as the ones aimed at combating extremist related dangers, are applied nationally solely with an aim of maintaining law and order, (Robyn *et al*, 2015). However, their implementation has had some challenges such as ease of use of biometric systems and fallibility of biometric technology. This swift increase in the generation and application of biometric applications in policing with no monitoring or control has greatly raised some worries on the possible manipulations or exploitations of such data.

Reviewed literature studies indicate few studies have focused on factors influencing biometric fingerprint technology in Kenya. The reviewed literature studies also showed mixed results. Studies such as by Al-Raisi and Al-Khoury (2008) sought to determine the fallibility of fingerprinting, iris, facial, and retinal recognition and revealed that bad ecological situations and lack of hygiene can unfavorably influence the collected sample from every person resulting in biometric fingerprint failure, Bustard *et al* (2013) looked at the effect of targeted impersonation as an instrument for uncovering the weaknesses of biometric applications and revealed that the verification algorithm has a very high possibility of failing if subjected with 800 potential targets. Similarly Kwakye *et al* (2013) carried out a study to ascertain the effect of the adoption of crypto-bio verification processes in Automated Teller Machines of the financial institutions while Adel *et al* (2016) carried out a study to evaluate the efficiency of biometric systems in regulating the Border Ports of the State of Kuwait and found that the use of biometric fingerprint systems decreased the number of unlawful entry of deportees who may want to re-enter the state. The studies present a contextual and conceptual knowledge gaps that this study sought to bridge.

Despite NRB using Biometric Fingerprint technology since its inception, no research study has been carried out to determine the factors that influence the use of BFT in criminal identification in Kenya. Hence, carrying out this study would-be significant in bridging this research gap.

### Research Objectives

- i. To assess how Ease of use influences the use of Biometric Fingerprint Technology in criminal identification in Kenya
- ii. To evaluate effect of the fallibility of Fingerprint Biometric Technology on the use of Biometric Fingerprint Technology in criminal identification in Kenya

### Theoretical Literature Review

#### ***Probability Theory (Mathematical Theory of Probability)***

The theory was proposed by Gerolamo Cardano in 1657. Probability is the measure of the likelihood that an event will occur. It is the likelihood of something to occur. The theory can be applied to fingerprint technology which holds that when two fingerprints are similar, there is no probability that



they are identical. This can only be disproved by the use of fingerprint technology through use of a database. The proponents of probability theory hold that the certainty of fingerprint identification is founded on calculations based on the theory of probability which states that "If events are independent of each other the probability of their concurrence is the product of their separate probabilities". Simply put, this calculation predicts odds of astronomic proportions against two different fingers having the same coincident sequence of ridge characteristic or Galton details. The axiom *nature never repeats herself* is aptly demonstrated by the fact that distribution of the minute ridge details on the palmer surface is never the same in different persons or even different fingers on the same hand. The theory can be practical to fingerprint identification in various forms depending on the direction of what needs to be studied. This theory has been widely used by forensic experts to give evidence in courts of law and issues dealing with commercial transactions. In fingerprint studies, the use of pattern identification has been widely adopted by studying fingerprint characteristics such as ridge endings, bifurcations or variations of other features. A spur for example, consists of a bifurcation where one arm forms a ridge ending. On examining fingerprints, it can be noticed that these characteristics may occur in different directions; they may occur upwards or downwards or horizontally to the left or to the right. Thus a particular characteristic can take four possible directions in a fingerprint and the probability of it having a particular direction is one in four

### ***Technology Acceptance Model (TAM)***

The proponent of this theory was Davis in 1986. Technology Acceptance Model is widely employed to comprehend the behaviour of people and their views to technology and innovation. It is concentrated towards demonstrating how people view and use technology and aspects concerning it to exactly how and when they will apply technology (Davis, 1989). According to Davis (1989), the supposed simplicity of usage is the extent to which an individual considers that application of a certain technology would be effortless, and supposed applicability is the extent to which an individual trusts that usage of a certain method would improve the efficiency of his or her work. According to the Model, the conduct of an individual is influenced by the perceived ease of use which is an outcome of the desire to and need with respect to the usage of technology. Attitudes associated with the application of a certain system are influenced by the supposed ease of usage and apparent effectiveness. Furthermore, perceptions have immediate influence on the purpose to which one plans to apply technology. Perceived simplicity of application and applicability has been shown to be influenced by outside aspects like individual preferences, technology or system characteristics, and business setting (Chen & Shen, 2005). There is no official study providing more of the application of and acceptance technology has been published, and however, the most concerned scholars apply the generic TAM and prolonged TAM to comprehend client acceptance of biometrics in the hospitality industry (Murphy & Rottet, 2007). In TAM 3 model, the perceived ease of use to perceived usefulness, computer anxiety to perceived ease of use and perceived ease of use to behavioural intention were moderated by experiences. TAM3 model of research is more applicable in the application of Biometric Fingerprint Technology in criminal identification. The model is as indicated in figure 1 below.

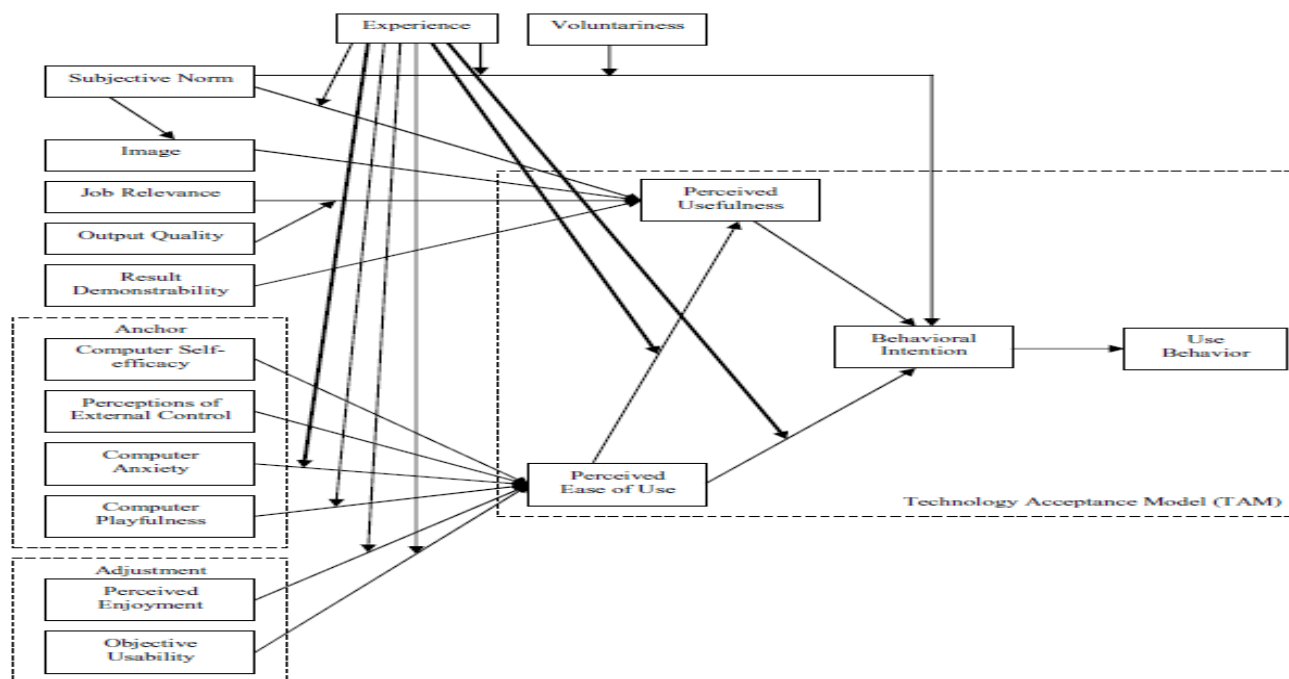


Figure 1 Technology Acceptance Model 3 (Venkatesh and Bala, 2008)

## Empirical Literature Review

### *Ease of Use*

Malla (2018) sought to determine the ease of use of Gaze-Based biometric Authentication System in verification and intrusion detection. The study used census design. The findings of the study revealed that the ease of use and superior functionality of Gaze-Based biometric Authentication System has increased significantly as a result of higher ability to protect users' confidential and private information. The results of the study showed that the use of gaze-based authentication system helps tackle with the challenges such as spoofing, video analysis and shoulder surfing attacks.

Indrayani (2014) carried out a study in Bandung to ascertain the effectiveness and the efficiency of the use of biometric systems in supporting national database. The study employed a descriptive research design. Both qualitative and quantitative research methods were used. The findings of the study showed that the use of the biometric system is quite efficient as it makes it easy to review recorded results in a more quick and automatic way thereby raising productivity. The study concluded that the effectiveness of the use of biometric systems in Bandung is classified according to quality systems indicators for instance capacity, timeliness, convenience, flexibility, cost-effectiveness, accuracy, consistency, security and ease.

Amin (2007) carried out a study to find out how the perceived ease of use of biometric technology in healthcare in Labuan and Sabah areas in Malaysia. The findings of the study showed that the perceived ease of use of biometric technology in healthcare has a significant effect on the plan to use. The study findings indicated that biometric technological systems are cheaper to maintain, self-efficient, smaller in size, have low power consumption capacity, easy to use and are non-intrusive. This increases the organizations intention to adopt Biometric technologies for authentication.

**Fallibility of fingerprint Biometric Technology**

A study by Al-Raisi and Al-Khourri (2008) to determine the fallibility of fingerprinting, iris, facial, and retinal verification/matching revealed that bad ecological settings can poorly influence the process of gathering fingerprint samples. The findings of the study also revealed that the failure of biometric fingerprint identification systems was linked to poor sanitization.

Bustard *et al* (2013) carried out a research to determine the impact of targeted impersonation as an instrument for the recognition of biometric technology weaknesses. The study specifically sought to determine the influence of targeted crimes, which can lessen the usefulness of biometric identity authentication. The study revealed that the verification algorithm has a very high possibility of failing if subjected with 800 prospective targets. This is due to the fact that such assaults can lead to a rise in the number of incorrect approval proportions by a factor of three; plummeting security to the extent that they are no longer be trusted for scientific verification. Additionally, the evaluation indicates that wrong approval proportions can be determined with the help of modest approach that is relative to the logarithm of the quantity of registered samples/people.

**Conceptual Framework**

According to Mugenda and Mugenda (2003), a conceptual framework denotes a component of the methodical examination practice in which a particular idea is defined as a quantifiable event or in quantifiable approaches that essentially provide a perfect implication of the idea. Simply put, a conceptual framework refers to a diagrammatic demonstration of the association among the predictor variable and the dependent variables. In this study, the dependent variable is criminal identification while predictor variables (independent variables) include Ease of use and fallibility of biometric fingerprint technology.

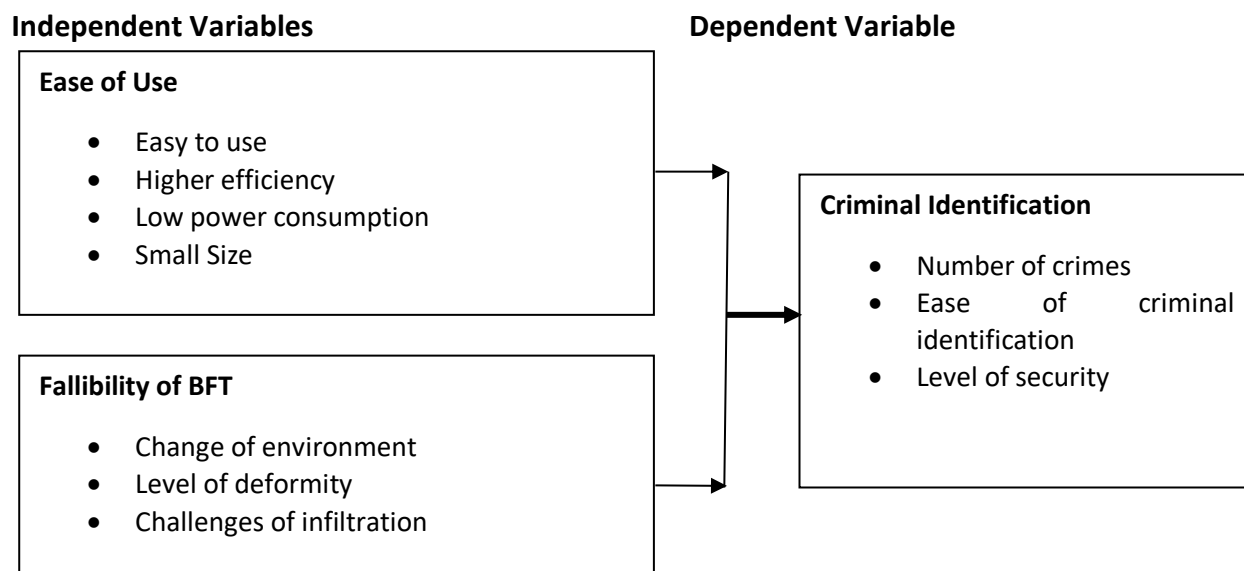


Figure 2 Conceptual framework for Criminal Identification



### Research Methodology

The study used census design. Kothari (2013) asserts that the use of census allows for reporting on things as they actually are. The study targeted staff involved with fingerprint identification. The target population comprised of the entire 140 fingerprint personnel based at the NRB Nairobi headquarters, Langata, Kariakor, Pumwani and Makadara stations and Huduma Centres within Nairobi County. The unit of analysis for the study was the National Registration Bureau head office, Langata, Kariakor, Pumwani and Makadara stations and Huduma Centres within Nairobi. The unit of observation was fingerprint officers. The sampling frame of the study was a list of all the fingerprint officers in Nairobi County. This consisted of 140 fingerprint officers who were included in the study. The study used semi structured questionnaires to capture quantitative and qualitative data. The structured questionnaires were quantified using a 5-point Likert scale type. Questionnaires were dropped and picked after one week to enable the respondent's ample time to respond to the questionnaires. The study pilot tested the questionnaire on 8 fingerprint officers working at NRB Headquarter in Nairobi. The study used Cronbach's alpha coefficient to check for the internal consistency of the questionnaire items. The results indicate that all the constructs had a Cronbach alpha confident value above 0.7 was implying that the questionnaire was reliable.

Before data analysis was carried out, diagnostic tests regarding multicollinearity, normality, linearity and autocorrelation were carried out in order to ensure proper specification of the models. Variance Inflation Factor was used to check for multicollinearity, Kolmogorov-Smirnov test was used to check for normality while Durbin-Watson t-test was used to check Autocorrelation.

Both bi-variate and multiple linear regression models were used. The multiple linear regression equation for this study was of the following form;

$$\text{Criminal Identification} = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \epsilon$$

Y=Criminal Identification,  $\beta_0$ =Constant,  $X_1$ = Ease of use,  $X_2$ =Fallibility of BFT,  $\epsilon$  = Error term. The statistical tests were tested at 5% level of significance.

### Results of Analysis

Out of 132 questionnaires that were distributed, a total of 117 questionnaires were duly filled and returned representing 88.6% response rate. According to Dixon (2012), a response ratio of 50% is satisfactory while a response ratio higher than 70% is excellent. Thus a response ratio of 88.6% is very good for this study.

### Descriptive Analysis for Criminal Identification

The study asked the respondents to indicate the extent to which they agree or disagree with the statements on Criminal Identification. The findings of the study are as presented in table 1 below. The findings showed that most officers agreed with the statement that the use of biometric technology has led to a decrease in the number of crimes to a very high extent (mean=4.64). The findings revealed that majority of the participants agreed with the statement that the use of biometric technology has led to an increase in the level of security (mean=4.62). Moreover, the results of the study revealed that most of the respondents indicated that they agree with the statement that the use of biometric fingerprint technology by the criminal identification agencies

have made it easy to identify criminals to a high extent (mean=3.62). Finally, the results of the study showed that majority of the respondents agreed with the statement that the use of biometric fingerprint technologies have decreased the number of illegal entry for expellees who tried to re-enter the country to a high extent (mean=4.07). On average, the findings of the study indicated that most of the respondents agreed with the statements on criminal identification to a high extent as shown by a mean of 4.24. The results of the study also revealed that the responses given by the respondents were less varied (standard deviation=0.80).

**Table 1 Descriptive Analysis Results for Criminal Identification**

Statement	Mean	SD
The use of biometric technology has led to a decrease in the number of crimes	4.64	0.77
The use of biometric technology has led to an increase in the level of security	4.62	0.57
The use of biometric fingerprint technology by the criminal identification agencies have made it easy to identify criminals	3.62	1.50
The use of biometric fingerprint technologies have decreased the number of illegal entry from expellees who tried to re-enter the country	4.07	0.36
Average	4.24	0.80

### Regression Test Results

#### Normality Tests Results

The test for normality was examined using One-Sample Kolmogorov-Smirnov Test. The results indicate that the residuals are normally distributed. The rule of thumb states that the data-set are normally distributed if  $K-S >$  level of significance ( $K-S > 0.05$ ). The Kolmogorov-Smirnov test results indicate that K-S values are insignificant implying that the data-set are normally distributed.

**Table 2 Normality Test Results**

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	Df	Sig.
Criminal Identification	.208	117	.203*	.588	117	.271

a. Lilliefors Significance Correction

\* This is a lower bound of a true significance

#### Test for Multicollinearity

The study used variance inflation factor to test whether multicollinearity is present. Multicollinearity is said to be absent if VIF is between 1 and 10. Moreover, multicollinearity is said to be absent if the tolerance values are higher than 0.8. The results presented in table 2 below. Based on the Coefficients Output of multicollinearity Statistics the VIF values are between 1.202 and 1.277, meaning that the VIF value obtained is between 1 and 10. This means that there is no multicollinearity.

**Table 2 Test of Multicollinearity Results**

Variable	Tolerance	VIF
Ease of use	0.812	1.232
Fallibility Fingerprint Biometric Technology	0.803	1.277

a Dependent Variable: Criminal Identification

**Autocorrelation Test**

Durbin-Watson test was used to check for the association between the error terms of the regression model. The rule of thumb is that Durbin Watson t-test value of between 1.5 and 2.5 indicates absence of autocorrelation. The results of the test showed that the error terms (residuals) for the study variables were not auto correlated.

**Table 3 Results for Tests for Independence**

Variable	Test	Statistic
Ease of use	Durbin Watson	1.797
Fallibility of BFT	Durbin Watson	2.111
Criminal Identification	Durbin Watson	1.813

**Linearity Tests for the Study Variables**

Correlation coefficient (r) was used to assess linearity between the ease of use, fallibility of BFT and Criminal identification. Pearson correlation value indicates a positive correlation. The strength of the association increases as the value approaches either -1 or +1. The correlation findings are presented in Table 5. The results show that both ease of use and Fallibility of BFT had a correlation with criminal identification at a coefficient of .261 and .459 respectively. The findings of the study showed that both regressors are linear to the dependent variable.

**Table 4 Linearity Results**

Variable		Ease of Use	Fallibility of BFT
Ease of use			
Fallibility of BFT	Pearson Correlation	.261**	.459**
	Sig. (2-tailed)	0.005	0.000

**Ease of Use and Criminal Identification**

The respondents were asked to indicate the extent to which they agree or disagree with the statements Ease of use of biometric fingerprint technology at the National Registration Bureau. Results of the study showed that majority of the respondents agreed that **Automated Fingerprint Registration System are smaller in size and easy to use** to a very high extent (mean=4.64). The findings of the study also showed that the respondents agreed to a very high extent that Ease of use **determines the quality level of fingerprint impressions acquisitions** (mean=4.68). Moreover, the results of the study revealed that the respondents agreed with the statement that **the use of Biometric Fingerprint Technology is non-intrusive** to a moderate extent (mean=3.26). Additionally, the respondents indicated that they agree with the statement that Ease of use **of BFT at the National**

**Registration Bureau leads to higher efficiency in fingerprint impressions collection** to a moderate extent (mean=3.02). Further, the results of the study showed that the respondents agreed with the statement that the use of AFIS is more efficient and cost saving to a moderate extent (mean=3.33). These results imply that majority of the respondents agreed with the statements on Ease of use to a high extent as indicated by a mean of 3.79. The responses given by the respondents had a small variation as shown by a standard deviation of 1.04. The results are consistent with the findings of a study by Indrayani (2014) which indicated that the use of the biometric system is quite efficient as it makes it easy to review recorded results in a more quick and automatic way thereby raising productivity.

**Table 5 Descriptive statistics for Ease of Use**

Statement	Mean	SD
Automated Fingerprint acquisition system are portable and easy to use	4.64	0.77
Ease of Use determines the quality level of fingerprint impressions acquisitions	4.68	0.60
The use of Biometric Fingerprint Technology is Non-intrusive	3.26	1.16
Ease of Use at the National Registration Bureau leads to higher efficiency in fingerprint impressions collection	3.02	1.28
The use of AFIS is more efficient and cost saving	3.33	1.37
Average	3.79	1.04

#### **Relationship between Ease of Use and Criminal Identification**

The bivariate linear regression model between ease of use and criminal identification shows that there is a relationship,  $R = 0.261$  and  $R^2 = 0.068$  which means that approximately 26.1% of the resultant changes in Ease of Use leads to 0.261 unit variation in criminal identification. The model summary results are presented in table 6 below.

**Table 6 Model Summary for Ease of Use**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.261	0.068	0.06	0.394721

a Predictors: (Constant), Ease of use

The bivariate linear model significance was determined using ANOVA. Regression results indicate that the linear relationship between Ease of use and criminal identification has an F value of  $F = 8.381$  with F critical value of 3.923. This shows that F calculated is greater than the F critical ( $8.381 > 3.923$ ) implying that the overall model is statistically significant at 5% significance level. The findings of the study are presented in Table 7.

**Table 7 ANOVA Results for Ease of Use**

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	1.306	1	1.306	8.381	.005
	Residual	17.918	115	0.156		
	Total	19.223	116			

a Dependent Variable: Criminal Identification

b Predictors: (Constant), Ease of use

The regression coefficient test results showed that the beta coefficient of the resulting regression model, the constant  $\beta_0 = 3.771$  is significant with p value  $p = 0.000 < p = 0.05$ . The coefficient  $\beta = 0.16$ , has a p value,  $p = .005 < 0.05$ . This implies that the effect of Ease of use on criminal identification is significant in the regression model. The findings of the study are in agreement with the findings of a study by Malla (2018) which indicated that the that the Ease of use and superior functionality of Gaze-Based biometric Authentication System has increased significantly as a result of its higher ability to protect users' confidential and private information.

**Table 7 Regression Coefficients for Ease of Use**

Coefficients	B	Std. Error	Beta	T	Sig.
(Constant)	3.771	0.216		17.443	0.000
Ease of use	0.16	0.055	0.261	2.895	0.005

a Dependent Variable: Criminal Identification

#### **Fallibility of BFT and Criminal Identification**

The study sought to extent to which fallibility of fingerprint biometric technology influences Criminal Identification. The results of the study were as presented in table 8. The results of the study revealed that majority of the respondents with the statement that a change in environmental conditions can adversely affect the collection sample from any individual to a high extent (mean=3.96). Moreover, the results of the study indicated that the respondents agreed with the statement that the fingerprints can be unrecognizable due to cuts or burns or extreme weight gain or loss to a high extent (mean=4.43). In addition, the finding of the study showed that the respondents agreed with the statement that Higher level of deformity of fingers leads to fallibility Fingerprint Biometric Technology to a high extent (mean=3.70). The results of the study also showed that the respondents agreed with the statement that Biometric fingerprint technology are susceptible to challenges of infiltration such as the use of artificial fingers made with candle wax or gelatin to a high extent (mean=3.96). These results imply that most of the respondents agreed with the statements on fallibility of BFT as indicated by a mean of 4.01. The responses given by the respondents were less varied as shown by a standard deviation of 1.12. The findings agree with the results of a study by Al-Raisi and Al-Khouri (2008) which revealed that bad environmental settings can poorly influence the process of gathering fingerprints samples while the failure of biometric fingerprint identification systems was linked to poor sanitization.

**Table 8 Descriptive Results for Fallibility of BFT**

Statements	Mean	Std
A change in environmental conditions can adversely affect the collection sample from any individual	3.96	1.32
Fingerprints can be unrecognizable due to cuts or burns or extreme weight gain or loss	4.43	0.94
Higher level of deformity of fingers leads to fallibility Fingerprint Biometric Technology	3.70	1.06
Biometric fingerprint technology are susceptible to challenges of infiltration such as the use of artificial fingers made with candle wax or gelatin	3.96	1.16
<b>Average</b>	<b>4.01</b>	<b>1.12</b>

**Relationship between Fallibility of BFT and Criminal Identification**

The bivariate linear regression model between fallibility of BFT and criminal identification shows that there is a relationship,  $R = 0.459$  and  $R^2 = 0.211$  which means that approximately 21.1% of the resultant changes in the fallibility of BFT leads to 0.211 unit variation in criminal identification. The model summary results are presented in table 9 below.

**Table 9 Summary for Fallibility of BFT**

R	R Square	Adjusted R Square	Std. Error of the Estimate
.459	0.211	0.204	0.363262

a Predictors: (Constant), Fallibility of BFT

The bivariate linear model significance was determined using ANOVA. Regression results indicate that the linear relationship between Fallibility of BFT and criminal identification has an F value of  $F = 30.676$  with F critical value of 3.923. This shows that F calculated is greater than the F critical ( $30.676 > 3.923$ ) implying that the overall model is statistically significant at 5% significance level. The findings of the study are presented in Table 10.

**Table 10 ANOVA Results for Fallibility of BFT**

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	4.048	1	4.048	30.676	.000
	Residual	15.175	115	0.132		
	Total	19.223	116			

a Dependent Variable: Criminal Identification

b Predictors: (Constant), Fallibility of BFT

The regression coefficient test results showed that the beta coefficient of the resulting regression model, the constant  $\beta_0 = 3.618$  is significant with p value  $p = 0.000 < p = 0.05$ . The coefficient  $\beta = 0.192$ , has a  $p = 0.000 < 0.05$ . This implies that the effect of fallibility of BFT on criminal identification is significant in the regression model. The study findings are consistent with the findings of a study by Al-Raisi and Al-Khouri (2008) which revealed that bad environmental settings can poorly influence the process of gathering fingerprints samples while the failure of biometric fingerprint identification



systems was linked to poor sanitization. Another study by Bustard *et al* (2013) revealed that the verification algorithm has a very high possibility of failing if subjected with 800 potential targets. This is because attacks can increase false acceptance rates by a factor of three; reducing security to the point that it is no longer reliable for forensic identification. Further analysis suggests that the false acceptance rate can be estimated using a simple model that is proportional to the logarithm of the number of enrolled subjects.

**Table 11 Regression Coefficients for Fallibility of BFT**

Variables	B	Std. Error	Beta	t	Sig.
(Constant)	3.618	0.143		25.313	0.000
Fallibility of BFT	0.192	0.035	0.459	5.539	0.000

a Dependent Variable: Criminal Identification

### Regression Analysis

The study used a multivariate regression model to evaluate the effect of ease of use and fallibility of biometric fingerprint technology on criminal identification in Kenya. The overall regression model of the study was  $Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \epsilon$  Where; Y= criminal identification,  $X_1$  = Ease of use,  $X_2$ =Fallibility Fingerprint Biometric Technology and  $\epsilon$  = Error term. The model summary results for the study variables are presented in Table 12. The results of the study indicated that Accuracy Ease of use and Fallibility Fingerprint Biometric Technology account for 59.3% of the variation in criminal identification. This is indicated by an R-square value of 0.593. The regression results show that R was 0.770 which means that the relationship between the independent variables and the dependent variable is positive.

**Table 12 Model Summary for the Study Variables**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.770	0.593	0.579	0.264162

a Predictors: (Constant), Ease of use, Fallibility Fingerprint Biometric Technology

The results of the analysis of variance for the study variables showed that the overall regression model linking Ease of use and Fallibility Fingerprint Biometric Technology and their influence on criminal identification was significant as indicated by F (4,112) statistic at 0.000 level of significance which is < than 0.05 significance level. F calculated is 40.869 while f critical is 2.453. F calculated is greater than the F critical (40.869 > 2.453), this showed that the overall model was statistically significant at 5% significance level. The results of the study are as shown in table 13.

**Table 13 Analysis of Variance for the Study Variables**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.408	4	2.852	40.869	.000
	Residual	7.816	112	0.07		
	Total	19.223	116			

a Dependent Variable: Criminal Identification

b Predictors: (Constant), Ease of use, Fallibility Fingerprint Biometric Technology

To determine the connection involving the dependent variables and the dependent variable, regression coefficients were generated as shown in table 4.26 below.

**Table 14 Regression coefficients for the Study Variables**

Variables	Unstandardized Coefficients		Standardized Coefficients			
	B	Std. Error	Beta	t	Sig.	
(Constant)	0.481	0.359		1.34	0.183	
Ease of use	0.296	0.041	0.482	7.207	0.000	
Fallibility Technology	Fingerprint Biometric	0.226	0.029	0.54	7.93	0.000

a Dependent Variable: Criminal Identification

Therefore, optimal multivariate Regression Model for the study is as shown below

**Criminal Identification = 0.481 + 0.296 Ease of use + 0.226 Fallibility Fingerprint Biometric Technology**  
Regression coefficients for the study variables showed that Ease of use of BFT had a positive and significant effect on Criminal Identification ( $\beta = 0.296$ , Sig = 0.000). This implies that the Ease of use of BFT, non-intrusiveness of AFIS, higher efficiency and quality level of fingerprint impressions acquisition leads to 0.296 unit effects on Criminal Identification. The findings are in agreement with the results of a study by Indrayani (2014) which indicated that the use of the biometric system is quite efficient as it makes it easy to review recorded results in a more quick and automatic way thereby raising productivity.

Moreover, the findings of the study also showed that fallibility of biometric fingerprint technology had a positive and significant influence on Criminal Identification ( $\beta = 0.226$ , Sig = 0.000). This implies that a change in environmental conditions, unrecognizable fingerprints due to cuts or burns or extreme weight gain or loss, higher level of deformity of fingers, susceptibility of BFT to challenges of infiltration leads to 0.226 unit effect on Criminal Identification. The findings agree with the findings of a study by Al-Raisi and Al-Khoury (2008) which revealed that bad environmental settings can poorly influence the process of gathering fingerprints samples while the failure of biometric fingerprint identification systems was linked to poor sanitization. Another study by Bustard *et al* (2013) revealed that the verification algorithm has a very high possibility of failing if subjected with 800 potential targets. This is because attacks can increase false acceptance rates by a factor of three; reducing security to the point that it is no longer reliable for forensic identification. Further analysis suggests that the false acceptance rate can be estimated using a simple model that is proportional to the logarithm of the number of enrolled subjects.

## Conclusion

The study established that Ease of use Biometric Fingerprint Technology leads to the acquisition of more efficient and quality level of fingerprint impressions. Higher quality fingerprint impression significantly influences criminal identification. Moreover, the study established that the fallibility of biometric fingerprint technology has a positive and significant effect on criminal identification. The

study concluded that a change in environmental conditions, unrecognizable fingerprints due to cuts or burns or extreme weight gain or loss, higher level of deformity of fingers, susceptibility of BFT to challenges of infiltration positively influences criminal identification.

### Recommendations

The study recommends the management of National Registration Bureau to ensure that their fingerprint officers capture quality level fingerprint impressions during the registration process using BFT. This is because quality biometric data helps to accurately authenticate individuals thereby preventing and detecting criminal activities. The study also recommends the management of National Registration Bureau to incorporate other means of biometric identification such as DNA, as a change in environmental conditions causes fingerprints to be unrecognizable and in cases of cuts or burns or extreme weight gain or loss, higher level of deformity of fingers.

### References

- Al-Raisi, A and Al-Khouri, A. (2008). Iris recognition and the challenge of homeland and border control security in UAE. *Journal of Telematics and Informatics*, 25(2): 117-132.
- Burns, N., & Grove, S. K. (2010). *Understanding Nursing Research-eBook: Building an Evidence-Based Practice*. Elsevier Health Sciences.
- Bustard, J. D., Carter, J. N., & Nixon, M. S. (2013). Targeted impersonation as a tool for the detection of biometric system vulnerabilities. In *Biometrics: Theory, Applications and Systems (BTAS)*, 2013 IEEE Sixth International Conference. IEEE.
- Creswell, J. W., & Poth, C. N. (2017). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-339.
- Giné, X., Goldberg, J., & Yang, D. (2010). *Identification strategy: A field experiment on dynamic incentives in rural credit markets*.
- Indrayani E. (2014). The Effectiveness and the Efficiency of the Use of Biometric Systems in Supporting National Database Based on Single ID Card Number. The Implementation of Elektronik ID Card in Bandung. *Journal of Information Technology & Software Engineering*. Vol. 4: 129. doi:10.4172/2165-7866.1000129
- Kothari C.R. (2004). *Research Methodology, Methods and Techniques*. New Delhi New Age International publishers.
- Kothari, C. (2013). *Research Methods & Techniques*. New Delhi: New Age Publications.
- Kowalczyk, S., & Shankar, K. (2011). Data sharing in the sciences. *Annual review of information science and technology*, 45(1), 247-294.
- Kwakye, M. M., Boforo, H. Y., & Badzongoly, E. L. *Adoption of Biometric Fingerprint Identification an Accessible, Secured form of ATM Transaction Authentication*.
- Malla, A. H. (2018). *A Gaze-Based Authentication System: From Authentication to Intrusion Detection*. (Doctoral dissertation).

- Mugenda, O., & Mugenda, A. (2003). Research methods: Quantitative and Qualitative methods. *Revised in Nairobi*.
- Mulumba, M. (2012). *Biometric authentication systems and service delivery in healthcare sector in Kenya*.
- Murphy, C. H., & Rottet, D. (2009). An exploration of the key hotel processes implicated in biometric adoption. *International Journal of Contemporary Hospitality Management*, 21(2), 201–212.
- National Institute of Standards and Technology, (2009). *Accuracy of Computerized Fingerprint Matching*.
- National Registration Bureau 2010 operational manual
- National Registration Bureau 2016. *Unpublished manuals*.
- Saini, M., Kapoor, A.K. (2016). Biometrics in Forensic Identification: Applications and Challenges. *Journal of Forensic Med* 1: 108. Do. ISSN: 2472-1026. Volume 1 • Issue 2 • 1000108
- Saunders, M. L., & Lewis, P. and Thornhill, A. (2009). *Research methods for business students*, Saunders. (2003). *Research methods for business students (3rd edition)* . New York : Prentice Hall.
- Upagade, V., & Shende, A. (2012). Research methodology. *S. Chand & Company Ltd. New Delhi, India*.
- Venkatesh, V. & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Science*, 39 (2), 273-312.
- Venkatesh, V. (2000). Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, 11(4), 342-365.
- Zuniga, A.E., Win, K.T., & Susilo, W. (2010). Biometrics for electronic health records. *Journal of Medical Systems*, 34(5).