REVIEWED JOURNAL of INTERNATIONAL SOCIAL SCIENCE & HUMANITIES [ISSN 2663-127X]

Vol. 4, Iss. 1 (2023), pp 611 – 638, November 4, 2023. www.reviewedjournals.com, ©Reviewed Journals

INNOVATIVE USE OF EMERGING BIOMETRIC TECHNOLOGY IN ENHANCING AIRPORT SECURITY AT JOMO KENYATTA INTERNATIONAL AIRPORT IN NAIROBI, KENYA

[1] Nzioka Trizah Nzisa & [2] Dr. Duncan O. Ochieng, PhD, MBS

[1] Master of Arts in Security Management and Policing Studies Student, Department Security, Diplomacy and Peace Studies, School of Law, Arts and Social Sciences, Kenyatta University, Kenya

[2] Department of Security, Diplomacy and Peace Studies, Kenyatta University, Kenya

Accepted: October 9, 2023

ABSTRACT

Airports are becoming increasingly vulnerable to impersonation and unauthorized access to designated areas by various cadres of employees due to the diversity of numbers and roles of airport employees. Unauthorized individuals can approach an aircraft or gain access to the airside by exploiting flaws in airport access control methods. Airport employee entry points are perhaps the weakest and most complex to access control. The study's problem is that many authorities have long attempted to improve security standards in the aviation industry through various means. While maintaining a secure aviation industry has always been a top priority, there has been a renewed focus on aviation security and safety since September 11, 2001. More than 77 percent of airports and 71 percent of airline security use biometric technology. In 2018, global biometric systems generated around $21.8 billion in revenue, which was used to advance airlines and airports. As a result, the goal of this study was to explore and implement the utilization of emerging biometric technology as a means to enhance the airport security measures at Jomo Kenyatta International Airport in Nairobi, Kenya. The specific objectives were to assess the effectiveness of biometric face recognition, evaluate the adoption and applications of biometric fingerprint identification system and examine the adoption and applications of automated passport control systems in enhancing Airport security in JKIA, Kenya. The study adopted a descriptive survey research approach with a target population of 1000 airport employees from various departments. Questionnaires were administered to a statistically meaningful sample size of 230 respondents and analyzed using descriptive and inferential statistics. Key informant interviews were also carried out to corroborate the findings from the questionnaires. The study findings reveal that biometric facial recognition technology is considered to have a significant effect on airport security with correlation of 0.569. Further, biometric fingerprint recognition is highly correlated to airport security with a coefficient of 0.541. Automated passport control had a significant effect on airport security with a correlation coefficient of 0.541. Moreover, the findings concluded that adopting both biometric fingerprint and automated passport control technologies would boost airport security. The study recommended that more efforts should be put on facial recognition technology as it is efficient in enhancing airport security. Further, the study recommended that the three technologies should be put together for better results.

Key Words: *Unauthorized Access, Airport Security, Aviation, Biometric Recognition and Identification*

CITATION: Nzioka, T. N., & [2] Ochieng, D. O. (2023). Innovative use of emerging biometric technology in enhancing airport security at Jomo Kenyatta International Airport in Nairobi, Kenya. *Reviewed Journal of Social Science & Humanities*, 4 (1), 611 – 638.

INTRODUCTION

Biometric technology is crucial for information technology progress as well as boosting the security of numerous systems that require user authentication (Mohsin et al., 2018). Its use ensures a person's accurate identification and protects material objects and data from unauthorized access. Long-term studies use multimodal biometric technologies to improve identification; as a result, control is based on multiple biometric features, preventing unauthorized access (Jain et al., 2016).

Non-identification access control methods pose a security risk, and biometric technologies may be a viable solution (Perry, 2014). Card swipe systems, keys, PINs, and other non-identification techniques are inherently insecure because anyone having them can get access, even if they are not the authorized holder. Since the first photograph of a traveler was included in a passport over a century ago, border controls have relied on biometric features (Del Rio et al., 2016).

Authorities can build a highly accurate and dependable method of identifying visitors and employees by integrating biometric technology into airport security measures. This not only aids in preventing unwanted access to restricted locations but also makes screening processes faster and more effective. Due to their difficulty in forging or duplicating, biometric systems offer a higher level of security than conventional identifying techniques like ID cards or passwords. Additionally, real-time identification verification made possible by biometrics enables law enforcement to quickly identify people of interest or potential threats. As a result, biometric technology integration into airport security has grown in popularity as airports work to improve security, streamline processes, and give passengers a smooth and secure travel experience.

Airport security is a multifaceted discipline that addresses the complex challenges faced by airports in maintaining a safe and secure environment (Kirschenbaum, 2013). It involves the deployment of a layered approach, integrating various security measures to create multiple lines of defense and increase the probability of threat detection and prevention. Access control measures, such as identification checks and restricted areas, ensure that only authorized individuals have access to sensitive airport locations. Passenger and baggage screening processes, which utilize technologies like X-ray scanners and metal detectors, aim to identify prohibited items and potential threats. Surveillance systems, including CCTV cameras and video analytics, enhance situational awareness by monitoring airport premises and identifying suspicious activities (Sagawa et al., 2016). Perimeter security measures, such as fencing, intrusion detection systems, and vehicle barriers, protect the airport's outer boundaries. The presence of well-trained security personnel acts as a visible deterrent and enables prompt response in case of security incidents (Dubey et al., 2018).

Biometric technologies are used in developed countries to provide reliable passenger verification at state borders, as well as to strengthen passport and visa regulations, as well as the control of other identification documents. The Federal Bureau of Investigation (FBI) of the United States of America (USA) uses biometric technology in criminal records and data on tens of millions of Americans in its database. The Next Generation Identification (NGF) system of the FBI collects and processes data, as well as identifying eyes, fingerprints, and iris patterns (Lyamin and Cherepovskaya, 2016).

The importance of security challenges in airports is critical for this research. As a result, a background investigation is required. To begin with, traditional city issues such as homelessness, mental illness, drug addiction, pathetic and complicated violence, and civil disobedience are increasingly being addressed in airports. Performing first-responder duties while also recognizing high-risk threats to aircraft operations is difficult for law enforcement and security services. Both of these responsibilities necessitate distinct skill sets. To mitigate both public disorder and homeland security vulnerabilities, security directors must manage assets, employees, and operations.

Second, militant groups and extremists continue to see commercial aviation as a lucrative target. Active shooters, bomb-laden bags, armed drones, and vehicle ramming are all plausible terrorist attacks on the public side of airports, from curbside to security screening. Thousands of fighters who defected from the collapsing ISIS caliphate have the option of forming new organizations, joining al Qaeda affiliates, or acting alone.

Third, on a monthly basis, media stories and Internet videos document the newest upheaval in aircraft cabins fighting, drunken outbursts, sexual assaults, and disobedience by flight attendants. The present tendency of in-flight squabbles and violence is potentially lethal at 35,000 feet. Making institutional adjustments in the flight crew-to-passenger contact is one alternative to boarding a security officer. Commercial airlines, for example, are increasingly being used by human traffickers, and flight crews are being educated to spot and respond to warning indicators. Another illustration of the flight crew's transformation from comforter to enforcer may be seen in this scene.

To get through security systems, terrorist groups may enlist the assistance of airport staff, particularly those with direct access to flights. Employees have also been busted for transporting drugs, firearms, and other illegal items. Because it only takes one radicalized or dissatisfied employee to produce a catastrophic disaster, insider threats are a major issue. Airports and airlines are adopting their own tactics to address this issue. All employees or a subset of them have been subjected to security screening prior to accessing restricted zones. Technology could help with this endeavor. Video and access control systems now have analytics capabilities that can be used to create a sophisticated surveillance tool. Internal self-policing is necessary, as is a "See Something, Say Something" effort (Kamau and Mireri, 2016).

The government hopes to make Kenya the African region's aviation hub, with an annual capacity of 45 million passengers, through the construction and modernization of aviation facilities. JKIA's Green Field Terminal, a second runway, and related facilities; Kisumu International Airport's increased terminal and airside capacity; Moi International Airport's improved safety and support operations; and the construction, rehabilitation, and maintenance of airstrips and airports are just a few of the major projects (Kenya Vision 2030 Blueprint, 2009).

The following issues regarding biometric technology therefore need to be addressed. Evaluating the effectiveness of the biometric technology being used at the airport, assessing its accuracy, reliability, and ability to identify potential security threats, investigating the level of acceptance among passengers, airline personnel, and airport staff regarding the use of biometric technology, Explore the challenges and potential benefits of integrating biometric systems with other existing airport security systems and Identify potential security vulnerabilities and threats related to the use of biometrics, and propose mitigation strategies.

Statement of the Problem

Biometric technologies are now used in almost every aspect of life, including access to work places and network resources, information security, granting access to specific resources, and airport security, to name a few examples (Mohsin et al., 2018). They have become indispensable in society, with applications such as identity management, surveillance, access control, social and welfare management, and automatic border control being used by billions of people either directly or indirectly. Biometric technologies can be used to verify a person's identity and differentiate them based on biological and behavioral characteristics (For example, face and voice respectively).

Enhancing security in borders of countries, and even within countries has been a great challenge despite the implementation of biometric technologies in major institutions, airports and within the land itself. Terror attacks are still evident in many developing and developed countries, Kenya not being an exception. Cases of drug trafficking, illegal trade in wild animal body parts, human trafficking and attempted smuggling of weapons into the airports and aircraft are still evident. These criminal activities especially drug and human trafficking keep happening despite the tight security measures put in place by the various authorities.

The airport is a perfect example of how security has become a more important part of our everyday lives. For the majority of travelers, the line at the security checkpoint is the most over indication, as more thorough checks on passengers and their bags produce bottlenecks. While passenger and baggage screening are clearly crucial to airports, a more holistic strategy is typically adopted, which brings together diverse security issues and handles them through interoperable solutions and fully integrated systems.

Airport safety is a top priority for everyone in Kenya, including passengers and employees. Despite the fact that biometric technologies are used in many countries, there are concerns about their effectiveness. With the outbreak of COVID – 19, biometric technologies have become increasingly important. In order to combat the health disaster, health-related measures were implemented in 2020. One of the major issues is allowing new approaches and principles to be used in the development of various systems to prevent smuggling and terrorist attacks, as well as the establishment of national security centers and international integration. All of these factors combined, this study aimed to innovate uses of emerging biometric technology in enhancing airport security in Kenya.

Objective of the Study

The study's overall objective was to examine the application of emerging biometric technology in enhancing airport security in JKIA, Kenya. The study was guided by the following specific objectives
The specific objectives were to;

- Assess the effectiveness of biometric face recognition in enhancing airport security in JKIA, Kenya.
- Evaluate the adoption and applications of biometric fingerprint identification system in enhancing airport security in JKIA, Kenya.
- Examine the adoption and applications of automated passport control system in enhancing airport security in JKIA, Kenya.

LITERATURE REVIEW

Empirical Literature Review

Effectiveness of Biometric Face Recognition System

Face recognition is a biometric approach that use computer algorithms to verify or identify the identification of a living individual using physiological signs. A biometric identification system, in general, identifies a person by using physiological (fingerprint, iris pattern, or face) or behavioral (handwriting, voice, or keyboard pattern) traits. Because of their natural need to protect their eyes, some people are hesitant to employ eye identification equipment. Face recognition has the benefit of being a non-intrusive, passive technique of validating personal identity in a "natural" and welcome manner.

In the previous few years, facial recognition technology has advanced significantly. The top face identification algorithm has an error rate of only 0.08 percent in the most recent round of testing by the National Institute of Standards and Technology (NIST) in March 2020. The most commonly used algorithm in 2014 had a 4.1 percent error rate. NIST determined that more than 30 algorithms exceeded the best results from 2014 during the 2018 tests. Face recognition research and development is helping to improve overall accuracy and extend use cases at a time when we're moving toward a more contactless society, especially in light of the COVID-19 epidemic.

In ideal settings, facial recognition systems, according to Crumpler (2020), have practically absolute precision, reaching a recognition accuracy level of 99.97 percent. In day-to-day operations, perfect conditions are rare, and algorithms are subjected to a range of factors that impair their accuracy. Face recognition technology has been used in a variety of settings, including airport security. In a study conducted in Europe, Lombardi et al. (2018) discovered that humans have been utilizing face recognition to identify one another as a part of daily life for centuries. Face recognition can be divided into two categories: facial appearance and facial geometry. The Eigen face method was named after a group of face photos that were combined to make a two-dimensional gray-scale image that was then used to construct a biometric template (Black & Daéid, 2018).

Adoption of Biometric Fingerprint Identification System

In research done in the United Kingdom to assess the fallibility of fingerprinting, Al-Raisi & Al-Khouri (2008) revealed that poor environmental conditions might impair the collecting of fingerprint samples. According to the findings of the study, poor sanitization was also linked to the failure of biometric fingerprint identification devices. The impact of targeted impersonation as a tool for finding biometric technology vulnerabilities was investigated by Bustard et al., (2013). The study's purpose was to see what impact targeted crimes have on the utility of biometric finger printing. When evaluated with 800 potential targets, the verification algorithm had a very high likelihood of failing, according to the report. Because such attacks can result in a threefold rise in the number of false approval proportions, security can be compromised to the point where scientific verification can no longer be trusted. Furthermore, the analysis reveals that incorrect approval proportions can be calculated using a straightforward method based on the logarithm of the number of registered samples or people.

Several issues have been raised in studies on the adoption of biometrics. An obstacle to wider use of biometric technology has been noted as the lack of a generic evaluation technique that includes performance, user acceptability and satisfaction, data quality, and security considerations when evaluating biometric systems (El-Abed et al., 2010). Tassabehji &Kamala, (2009) extended the traditional technology acceptance model (TAM) to see if users' attitudes and intentions to use biometric banking were influenced by their perceptions of biometric security. (Kant & Nath, 2009) proposed a model for reducing fingerprint identification system process time. Abdelbary (2011) investigated the factors that influence the acceptance of biometrics technology in Egyptian hotels. (Patel & Asrodia, 2012) proposed fingerprint matching methods. Fingerprint imaging was studied by (Maheswari & Chandra, 2013).

One of several solutions to the banking industry's security concerns has been to use biometric technologies to identify and verify people (Kwakye et al., 2015). The authors employed fingerprint identification as one type of biometric authentication in their study to address the ATM transaction authentication difficulty. According to the findings of the study, the average reaction times of each of the operations (and their sub processes) were remarkably short. Fingerprint scanning using a scanner, completing the enrollment procedure, and completing online off-card verification were among the methods employed. Some areas of the design and implementation, according to the writers, needed to be improved.

Adoption of Automated Passport Control System

Through CBP's Main Observation Division, Automated Passport Control (APC) automates the entry procedure for US citizens, legal residents, Canadians, Visa Requirements participants, and certain tourists with a US visa. Self-service kiosks are used by travelers to answer CBP inspectors' questions and provide biographical information. It is a free service that requires no preregistration or membership and ensures the highest level of security when dealing with personal data or information. APC users benefit from shorter lines, less traffic, and faster processing (Schwarz, et al., 2021).

The United States Customs and Border Protection (US CBP) is a significant law enforcement agency tasked with "protecting the public from harmful individuals and goods by defending America's borders." The four points of entry into a country are airlines, harbors, protected land terminals and coastlines (Riley, 2006). Customs is known as a 'gatekeeper,' a checkpoint where foreign trade must pass to protect the country's interests (Widdowson, 2007). On an average day, CBP processes around 340,000 international airline passengers and crew, encountering 592 inadmissible at US ports of entry, identifying 1607 people with national security concerns, and intercepting 12 fake documents (Khan & Efthymiou, 2021).

Theoretical Framework

Routine Activity Theory

The routine activity theory was used in this research. Lawrence E. Cohen and Marcus Felson proposed routine activity theory in 1979, and it was later developed by Felson. They claimed that indicators of well-being and socioeconomic conditions – Poverty, a lack of education, and unemployment are just a few examples– were the primary causes of crime in this theory (Cohen and Felson, 1979). It emphasizes the coming together of three different elements: (1) a driven assaulter, (2) a victim, and (3) a caregiver who is incapable. It includes the usual tasks of both the claimant and the defendant. An offender may go through a neighborhood on a frequent basis, seeking for residences that appear to be ideal targets for burglary or enter business premises looking for opportunities to steal. Access restrictions and other security measures are typically lacking in commercial buildings, making them attractive targets. Guardianship can be provided by ordinary people who can intervene or serve as witnesses, as well as police or security professionals.

Coupe and Blake (2006) looked at daytime and nighttime house burglary targeting methods based on everyday activities, and discovered that the relative security of potential target residences, as well as the victim's work and lifestyle, all had an impact on burglary possibilities. Smith et al., (2000) discovered that an offender's familiarity with a potential crime scene influenced their criminal behavior choices; street robbers committed crimes within their "awareness zone." Using a routine activities approach, Weisburd et al. (2004) discovered frequent criminal "hot spots," as well as the effect of commercial enterprises (bar violence) on domestic crime, using a routine activities approach (Roncek and Maier, 1991). In Israel and Germany, this argument has been used to explain automobile theft (Aleksander et al., 1994).

In this study, the theory was used by Airport security to detect crimes and criminal activities at JKIA. Moreover, the theory can be used in this study to assess security breach and ways of preventing it and enhancing the security. The theory is important for the study since it describes how to employ biometric patterns with particular properties such as ridge ends, bifurcations, and other variations. A spur is a bifurcation with one arm terminating in a ridge, for example. The theory was vital in meeting the study's first specific objectives on the effectiveness and use of biometric face recognition technology at the airport.

Situational Crime Prevention Theory

Situational crime prevention, according to Clarke (2017), is a major topic in criminology, criminal justice, and security studies that is extensively employed in crime prevention. It promotes environmental and administrative measures targeted at lowering the likelihood of crime and the accompanying rewards. It focuses on proactive tactics and approaches against crime, according to Freilich & Newman (2017), by using a preventive approach to remove crime opportunities. Situational crime prevention focuses on the existing environmental variables that make a crime conceivable, and then creates methods to decrease these scenarios through in-depth investigation. The techniques are designed to reduce crime's possibilities and rewards. It is one of the few ideas that can be applied to improve corporate and personal security initiatives outside of the current criminal justice system.

According to Smith & Clarke (2012), it is frequently used in law enforcement practice, administration, and management. Problem-solving policing employs situational crime prevention, which is one of the most widely employed policing tactics globally. It concentrates on a specific criminal concern and offers preventative measures. It emerged 45 years ago, according to Huisman & Van (2013), by merging concepts from other key theories such as rational choice and opportunity structure theories. According to Gruenewald et al. (2015), it produces the best results since it focuses on situational variables, making the criminal act difficult to carry out regardless of the offender's motivation by removing any situations that might spark the offender's interest.

Conceptual Framework

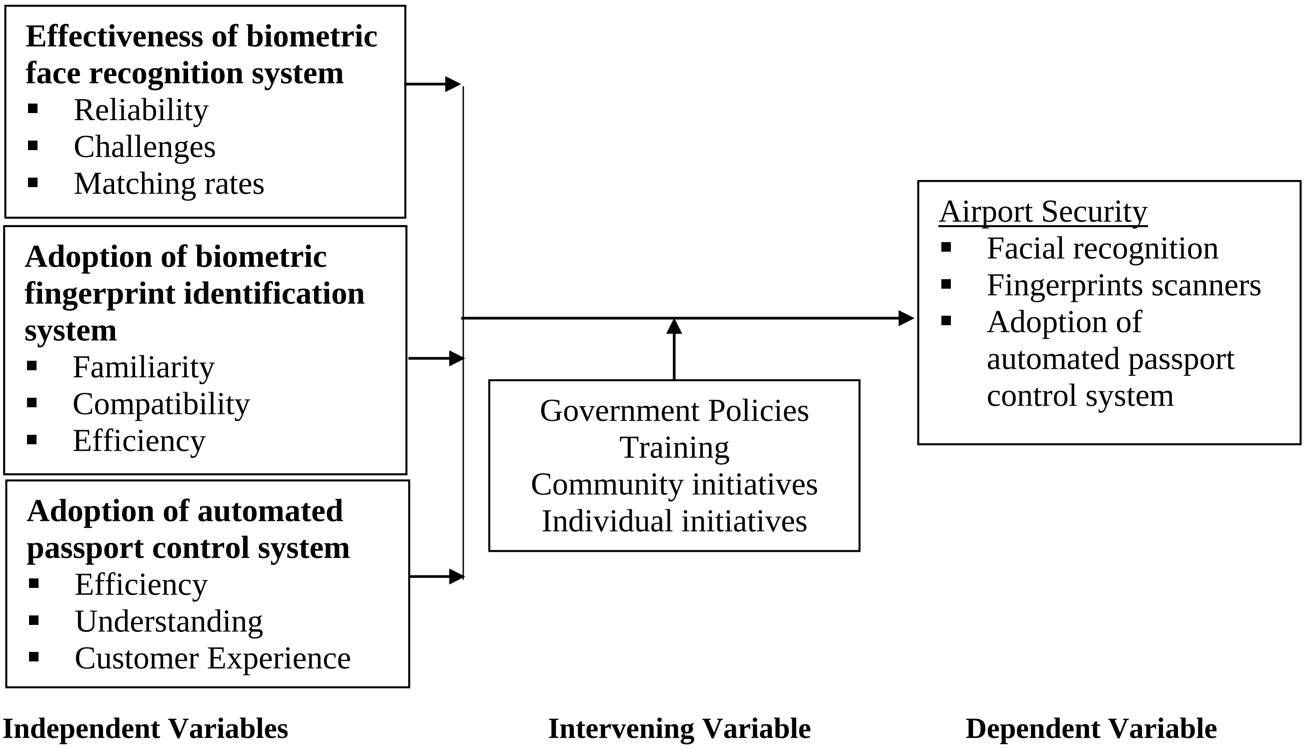

Figure 1: Conceptual Framework

METHODOLOGY

A descriptive research design was adopted in the study. The study took place at Jomo Kenyatta International Airport in Nairobi. The JKIA is a Nairobi-based international airport in Kenya. A total of 1000 people from JKIA security departments were enrolled in the study. These individuals were chosen because they were familiar with various biometric aspects and their applications at the airport. Sampling frame refers to the set of units used to calculate sample size. The sample size was determined using simple random sampling from the stratum specified. This approach was acceptable since the sample size chosen is a representative sample of the population. The sample size of 286 was calculated using Yamane's method (Adam, 2020). The number of participants in each stratum was determined using proportionate sampling, which was based on the ratio of employees in the establishments. Then, until the appropriate sample size is obtained, a simple random selection procedure was employed to choose research volunteers in each stratum.

The major source of data for this study was self-administered questionnaires delivered to JKIA management and workers. Questionnaires were used to collect data for the study. There were closed-ended questions in the questionnaires. Closed-ended questions aided in providing structural responses, allowing a viable proposal to be presented. Closed-ended items were used to examine ratings on various attributes, as this is critical for minimizing related responses and obtaining a diverse response. To enhance the questionnaires, they were carefully prepared and evaluated on a small sample of the population. Questions were divided into groups. A key informant interview with two employees from each institution (KCAA, KRA, and Kenya Airways ((KQ)) was also be conducted as part of the study.

A computer software program was used to clean, analyze, and assess the data collected in the field. The statistical tool Statistical Package for Social Sciences (SPSS) version 22 was used to analyze quantitative data using inferential and descriptive statistics. The raw data went through a data preparation procedure before being evaluated. After the quantitative data has been examined, data preparation was performed, including instrument inspection, data editing, data coding, data entering, and data cleaning, as well as diagnostic testing

(Bager et al., 2018). The study used content analysis to analyze qualitative data, identify major themes, and present excerpts verbatim. Descriptive statistics were utilized to describe the responses in connection to the dependent, independent, and demographic information from the respondents. Frequency distribution, mean (measure of dispersion), standard deviation (measure of dispersion), and percentages are examples of descriptive statistics. Inferential statistics including Pearson correlation analysis and multivariate regression analysis were used in this research. The following is the regression model:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

where;

Y = Airport Security

β_0 = Constant

$\beta_1, \beta_2, \beta_3, \beta_4$ = Coefficients of determination

X_1 = Effectiveness of Biometric Face Recognition

X_2 = Adoption of Biometric Fingerprint recognition

X_3 = Adoption of Automated Passport Control

ε = Error term

RESULTS

Effectiveness of Biometric Facial Recognition

The first specific objective of the study was to assess the effectiveness of biometric face recognition in enhancing airport security in Kenya. This specific objective was achieved by use of both open and close ended questions.

Biometric Facial Recognition Rating

The respondents were asked to rate the biometric facial recognition technology at JKIA and the study findings presented in Table 1. To accomplish this, a five-point Likert scale comprising of two items was used. The scale rating ranged from 0 to 4 with 0 denoting very high, 1 representing high, 2 minimal, 3 low and 4 very low. The midpoint of the scale was a score of 2. From the study findings, majority (42.1%) indicated high, 37 per cent minimal, while 20.9 per cent indicated very high.

Table 1

Biometric Facial Recognition

Facial Recognition Technology	**0**	**1**	**2**	**Mean**	**Std. Dev**
	%	**%**	**%**		
How would you rate the effectiveness of biometric facial recognition technology at JKIA?	20.9	42.1	37.0	1.16	0.745

Source: Field Data (2022).

The effectiveness of biometric facial recognition at JKIA was rated to be high as visualized in Table 1. This was clearly indicated by a 42.1 per cent response rate. Furthermore, 37.0 per cent and 20.9 per cent effectiveness were evident for minimal and very highly effective respectively. According to Sumner (2007), facial recognition technology is considered to be effective to the airport. One interviewee from Kenya Airports Authority noted that the technology is highly effective despite challenges that it may encounter. Clearly, as seen from the mean response of 1.16 with a standard deviation of 0.745, its effectiveness was rated to be high.

One of the key informants said,

> Facial recognition technology has the potential to make travel both more convenient and more secure because it creates a digital template that's unique to you. Machines are getting faster at matching faces

> and do a better job than humans do. I would say that biometric facial recognition technology is effective at the airport. There is no perfection of a technology that is why facial recognition encounters challenges here and there but with advances and improvements, it can be considered to be highly effective to aid in airport security (Respondent 01).

Technology Response Time in Detecting Crime

To determine whether the technology used at the airport was effective in detecting crime. based on the response time, the respondents were asked to rate the technology response time and from the study findings presented in Table 2, majority (37.4%) of the respondents indicated minimum, 34.5 per cent very high, 15.3 per cent low while 12.8 per cent indicated high. Clearly, the technology was rated to be minimal effective in detecting crimes as seen from the mean response of 1.34 with a standard deviation of 1.106. Therefore, there was a need in improving the airport security by either improving the standards of the technology or adoption of other technologies. According to Sumner (2007), the technology is considered to have challenges in detecting crimes.

Table 2

Response in Detecting Crimes

Response time in detecting crimes	**1**	**2**	**3**	**4**	**Mean**	**Std. Dev**
	%	**%**	**%**	**%**		
How would you rate the technology response time in detecting crimes at JKIA?	34.5	12.8	37.4	15.3	1.34	1.106

Source: Field Data (2022).

One of the key informants said,

> Detecting a crime with only facial recognition faces several challenges. Clarity of images as well as CCTV cameras may fail. This aspect makes the technology to become less effective in response time in detecting crimes (Respondent 02).

Perception of Facial Recognition

The perception of the respondents was important in determining the effectiveness of the technology and the respondents were asked to indicate their perception of the facial recognition technology at the airport and from the study findings, majority (82.2%) indicated good while 17.8 per cent indicated not good. According to Lai and Rau (2021), facial recognition is perceived to be a good technology for use at the airport.

From the key informants, one said,

> Biometric facial recognition is good. It allows for efficient security process implementation, incident prevention. Travelers present themselves and their documentation and pose for a quick photo in seconds. The officer has the data they need based on a discussion with the traveler about the purpose of the trip and ultimately can decide about whether further examination is needed (Respondent 03).

Facial Recognition Technology

The respondents were asked to indicate their level of agreement with statements regarding facial technology recognition using a scale of 1 to 5 where 1 = strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = strongly agree and the study findings presented in Table 3.

Table 3

Facial Recognition Technology

Facial Recognition Technology	1	2	3	4	5
	%	%	%	%	%
The Airport has enough personnel to handle biometric technology	10.4	41.3	4.8	30.9	12.6
Biometric technology has helped the airport to main security	0.0	0.0	25.7	41.3	33.0
The biometric technology at the airport meets technical satisfaction	0.0	22.6	11.7	65.7	0.0

Source: Field Data (2022).

From the findings presented in Table 3 above, it was clear that 41.3 per cent noted that the airport lacked enough personnel to handle biometric technology. Moreover, 30.9 per cent agreed that the airport had enough personnel to handle biometric technology. 12.6 per cent also indicated that they were in strong agreement on the statement that the airport had enough personnel to handle biometric technology. According to Lazarick (1998), there is need for enough personnel to handle biometric technology at the airport.

On whether the technology has helped the airport maintain security, majority of the respondents agreed to the statement (41.3%). Moreover, 33.0 per cent strongly agreed towards the statement. This implies that the technology has really helped the airport maintain security. According to Sumner (2007), facial recognition technology helps in maintaining airport security.

Approximately 65.7 per cent agreed that the technology at the airport meets technical satisfaction. However, 22.6 per cent disagreed to the statement that the technology at the airport met technical satisfaction. Moreover, 11.7 per cent had a neutral opinion towards the same. From the findings, it is appropriate to mention that the technology met technical satisfaction. According to Lazarick (1998), technical satisfaction is crucial for a technology to be applied for security purposes.

Biometric Facial Recognition and Reduction in Crimes and Insecurity

It was important to determine if biometric facial recognition technology has led to reduced cases of crimes and insecurity and from the study findings, majority (71.7%) of the respondents indicated that the use of biometric facial recognition technology has led to reduced crimes and insecurity at the airport. The study findings were consistent with a study by Sumner (2007) in which, the technology helped in reduction in crimes and insecurity at the airport.

Extent to which Biometric Facial Recognition Affects Airport Security

The respondents were further asked to indicate the extent to which biometric facial recognition technology affects the Airport security and a scale of 1-5 where 1= very great extent, 2=great extent, 3=Moderate extent, 4=minimal extent and 5= Not at all and from the study findings, majority (66.1%) of the respondents indicated that the technology affected the security at the airport to a great extent. According to Lazarick (1998), facial technology greatly affects airport security.

Challenges Facing Facial Recognition at JKIA

The respondents were further asked to indicate if there are challenges facing facial recognition at JKIA and the study findings showed that majority (77.0%) of the respondents indicated that the technology faced challenges whereas 23 per cent noted that the technology did not face any challenges. According to Dillingham (2003), facial technology faces quite a number of challenges that need to be looked into.

Challenges of Biometric Facial Recognition Technology

It was important to determine the challenges facing biometric facial recognition technology at the airport and the respondents were asked to indicate their level of agreements on a scale of 1 to 5 where 1 = strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = strongly agree. Table 4 shows the percentages obtained for the challenges of biometric facial recognition technology. The first challenge under study was the inconsistency of matching rates. From Table 4 above, majority (49.4%) had a neutral opinion. Moreover, a substantial number (20%) of respondents strongly agreed that biometric facial recognition faced inconsistent matching rates.

Table 4

Challenges of Biometric Facial Recognition

Challenge	**2**	**3**	**4**	**5**	**Mean**	**Std. Dev**
	%	**%**	**%**	**%**		
Biometric Facial Recognition faces inconsistent matching rates	13.6	49.4	17.0	20.0	3.43	0.960
Biometric Facial Recognition faces low matching rates during pilot trials	0.0	28.1	49.4	22.6	3.94	0.711
Biometric Facial Recognition faces network availability issues	27.7	44.3	11.9	16.2	3.17	1.010
Biometric Facial Recognition is time consuming	0.0	26.0	43.4	30.6	4.05	0.752
Biometric Facial Recognition cannot be considered reliable	17.9	51.5	8.9	21.7	3.34	1.011
Biometric Facial Recognition needs to be bypassed	8.1	17.0	49.4	25.5	3.92	0.864

Source: Field Data (2022).

Furthermore, this was closely followed by a response rate of 17.0 per cent on agreement that the technology faced inconsistent matching rates while 13.6 per cent of the respondents indicated that they disagreed with the statement and therefore, according to their response, the technology does not face inconsistent matching rates. In general, there was a 50-50 per cent response on whether the technology faced inconsistency of matching rates.

One of the key informants said;

> From my honest opinion, the biometric facial recognition technology faces inconsistent matching rates and many a times, the users of this technology are left wondering what they can do to salvage the situation especially whenever this involves passengers of a scheduled flight (Respondent 04).

Additionally, Spreeuwers et al (2012) argue that 5 percent of European passports have insufficient quality photos, which can also contribute to issues in identity verification. A mean response rate of 3.43 with a standard deviation of 0.960 was observed imply that most of the respondents had a neutral opinion on whether the technology faces inconsistent matching rates.

On matching low rates, 49.4 per cent agree with the statement that biometric facial recognition technology faced low matching rates during the pilot trials. As a result, the high response rate needed to be considered by attempting to solve the problem. Furthermore, 28.1 per cent responded neutral. They neither agreed or disagreed with the statement. 22.6 per cent of the respondents claimed to strongly agree to the statement implying that low matching rates was a challenge in applying biometric facial recognition technology.

One of the key informants said;

> In the pilot tests, the technology has poor matching rates. False rejections must also be decreased in order to improve the effectiveness of the facial recognition process. (Respondent 05).

According to Labati et al., (2016), several factors can contribute to the quality deterioration of a biometric sample. Therefore, the technology faces low matching rates during the pilot phase as realized by a mean of 3.94 with a standard deviation of 0.711.

For the technology to be of efficiency, there has to be an availability of network and internet devices. This challenge was addressed and from the findings, 44.3 per cent neither agreed nor disagreed to the challenge of network availability issues. Approximately 27.7 per cent had a disagreement on the availability of network which indicated that network issues were minor to the implementation of the technology. Moreover, 16.2 per cent strongly agreed to the statement on availability of network issues. Lastly, the number of respondents who agreed to the statement amounted to 11.9 per cent posing as the minimum response rate achieved from the challenge.

One of the key informants also said;

> Network availability may at times become an issue. Electricity shortages which are backed up with automatic generators cause the internet to buffer. As a result, some communications may be cut short or even some may cause loss of data which could not have been saved (Respondent 06).

This study’s findings are consistent with Khan and Efthymiou, (2021) which indicated that biometric facial technology faced network availability issues during the pretesting period. Therefore, the technology was neither perceived to face network availability issues or not since the mean response rate was seen to be 3.17 with a standard deviation of 1.010.

During identification of individuals in the system, there are procedures that are usually undertaken so that an output is enabled. This process may be time consuming. This challenge was therefore put under study and the findings were as follows. 43.4 per cent of the respondents agreed that the technology is time consuming while 30.6 per cent strongly agreed that the technology was time consuming. However, 26.0 per cent had a neutral response implying that they were neither in disagreement nor in agreement on whether the technology was time consuming or not. Two interviewees indicated that the technology was time consuming which is in collaboration with Khan and Efthymiou, (2021) study which gave similar results. Therefore, there was need to review the technology for fast detection since majority agreed to the technology being time consuming with a mean response of 4.05 with a standard deviation of 0.752.

On reliability of biometric facial recognition, 51.5 per cent were undecided. They were neither in disagreement nor in agreement on whether the technology was reliable or not. Furthermore, 21.7 per cent strongly agreed that one could not rely on the technology. Moreover, 17.9 per cent disagreed as 8.9 per cent agreed to the statement. From the findings, it implied that this technology could not be relied on to curb security challenges that may occur. One interviewee responded that the technology would be considered unreliable. The findings of the study were consistent with Spreeuwers et al. (2012) study on reliability since due to clarity of pictures taken or quality of pictures. This arises an alarm on the technology since airport security is crucial. Moreover, the technology could not be perceived as reliable or not since the mean response rate was seen to be 3.34 with a standard deviation of 1.011.

Since the challenges of the technology were put under study and findings showed that biometric facial recognition technology faces several challenges, there was need to examine on whether to bypass the technology or not. Therefore, of the respondents, 49.4 per cent claimed to agree on bypassing the technology. In addition, 25.5 per cent strongly agree to bypass the technology. 17.0 per cent of the respondents were undecided on whether to bypass or not while only 8.1 per cent disagree.

One of the key informants said;

> It would be more effective to combine other technologies with biometric facial recognition than to bypass the technology. Further, incorporating facial recognition CCTV systems can improve performance in carrying public security missions (Respondent 07).

According to Spreeuwers et al (2012), it is efficient to incorporate other technologies with biometric facial recognition in order to enhance airport security. With majority of the respondents agreeing to bypass the technology, as evident with a mean response of 3.92 with a standard deviation of 0.864, the study therefore analyzed on whether two other technologies can be adopted namely biometric fingerprint technology and automated passport control technology in enhancing Airport Security.

Biometric Facial Recognition and Airport Security

To determine the influence of biometric facial recognition on airport security, the researcher conducted Analysis of Variance (ANOVA). The independent variables of the study were factors that were studied under effectiveness of biometric facial recognition while the dependent variable of the study was airport security. Tables 5 shows results of this analysis.

Table 5

ANOVA for Biometric Facial Recognition and Airport Security

ANOVA

Source of Variation	Sum of Squares	DF	Mean Square	F	Sig.
Regression	3.861	1	3.861	109.326	.000*
Residual	8.053	228	0.035		
Total	11.914	229			

*Significant at *p*<0.05 level

ANOVA statistics test revealed that biometric facial recognition had a significant influence on airport security. This implies that the technology has a positive impact on the state of security at the airports. From the findings, it was also clear that the technology had played a vital role in enhancing airport security. A sum of square due to regression of 3.861 was observed which imply that there was low variation of data points from the mean.

Further, correlation statistics were conducted to determine whether there was any relationship between biometric facial recognition and airport security. The results are shown in the Table 6 below. Findings in Table 6 above indicate a positive correlation of 0.569 between biometric facial recognition and airport security. This implies that biometric facial recognition is significant to airport security.

Table 6

Correlation between Biometric Facial Recognition and Airport Security

Correlations

		facial	Airport security
Facial	Pearson Correlation	1	.569**
	Sig. (2-tailed)		.000
Airport security	Pearson Correlation	.569**	1
	Sig. (2-tailed)	.000	

**. Correlation is significant at the 0.01 level (2-tailed).

Adoption of Biometric Fingerprint Recognition

On whether to accept or reject biometric fingerprint recognition technology, this study looked into a number of factors. The researcher sought to bring to understanding as well as have concrete reasons to why this technology would be much preferred to facial recognition technology.

Training to use Biometric Fingerprint Technology

The study sought to understand whether the respondents had received training on biometric fingerprint technology. Table 7 showed the findings of the study.

Table 7

Training on Biometric Fingerprint Recognition

Training	Frequency	Percentage
Yes	152	66.1
No	78	33.9
Total	**230**	**100.0**

Source: Field Data (2022)

From the findings of the study, majority (66.1%) had been trained on how to use biometric fingerprint technology whereas 33.9 per cent responded that they had not received any training on the technology. This is crucial in determining on whether to adopt a technology or not. According to Miltgen et al (2013), training on a technology is essential on whether or not to adopt the technology.

Institutional Support of Biometric Fingerprint Technology

It was crucial to determine whether the respondents' institutions supported biometric fingerprint technology. The findings are presented in Table 8 below.

Table 8

Support of Biometric Fingerprint Recognition

Support	Frequency	Percentage
Yes	158	68.7
No	72	31.3
Total	**230**	**100.0**

From the findings in Table 8 above, majority (68.7%) noted that their institutions supported biometric fingerprint technology. Moreover, it was noted that there were some institutions that did not support the technology in their operations (31.3%). These findings are in line with Miltgen et al., (2013) study where institutional support is key to adopting a technology.

Biometric Fingerprint Recognition Variables

The variables under study for the technology were whether the technology was familiar, whether the staff understood the technology before adoption, compatibility with operations at the airport and its efficiency. Table 9 gives an output of the respondents' responses.

The responses were measured using a five-point Likert scale. The scale rating ranged from 1 to 5 with 1 denoting strongly disagree, 2 representing disagree, 3 neutral, 4 agree and 5 strongly agree. The midpoint of the scale was a score of 3. On whether the staff was familiar with biometric fingerprint recognition technology, 40.4 per cent were in strong agreement that the technology was familiar to them. Moreover, 32.6 per cent agreed to the same. At the same time, 17.8 per cent were neither in agreement nor in disagreement on the same. However, 9.1 per cent disagreed to the familiarity of the technology. From the findings, it is evident that the technology was familiar to most of the staff in the airport. Two interviewees noted that the technology was familiar to them and for operations at the airport. These results were in line with Sumner (2007) study which noted that familiarity is key to adoption of a technology in enhancing airport security. Moreover, there was a mean response rate of 4.04 with a standard deviation of 0.975 which suggested that most of the respondents agreed to the question.

Table 9

Adoption of Biometric Fingerprint Recognition Factors

Variable under study	2	3	4	5	Mean	Std. Dev
	%	%	%	%		
Biometric Fingerprint recognition is familiar to every staff	9.1	17.8	32.6	40.4	4.04	0.975
Every staff has an overall understanding of Biometric Fingerprint Recognition when considering it for airport security	0.0	19.6	53.9	26.5	4.07	0.677
There is enough information available to make an informed decision on whether or not to incorporate Biometric Fingerprint Recognition	7.4	23.9	28.7	40.0	4.01	0.969
Biometric Fingerprint Recognition is compatible with current airport security operations	0.0	34.3	60.9	4.8	3.70	0.552

Source: Field Data (2022).

It is usually of much importance that the staff have an overall understanding of the technology before considering for adoption or not. This was also aired to the respondents and 53.9 per cent agreed that they understood the technology. 26.5 per cent were in strong agreement that they understood the technology while 19.6 per cent had no clue on whether they agreed or not. One interviewee noted that there was an overall understanding of how the technology works. These results were in line with Sumner (2007) study which noted that overall understanding is key to adoption of a technology in enhancing airport security. The mean response rate was 4.07 with a standard deviation of 0.677 which implied that majority of the respondents understood the technology.

Before incorporating a technology, one has to know the advantages and disadvantages of the same. Therefore, the study sough to know whether there was enough information available to make an informed decision on whether or not to incorporate the technology. The respondents generally agreed to the statement implying that there was enough information available to make an informed decision on whether to incorporate the technology or not as it is depicted with a mean response rate of 4.01 with a standard deviation of 0.969. Further, two interviewees noted that there was enough information available to make an informed decision on whether or not to incorporate the technology. These results were in line with Sumner (2007) study which noted that availability of information to make an informed decision is key to adoption of a technology in enhancing airport security. By distribution, 40.0 per cent strongly agree, 28.7 per cent agreed, 23.9 per cent were neutral and 7.4 per cent disagree.

The study also sought to know whether the technology was compatible with the current airport security operations. Compatibility is the degree to which an innovation is perceived as being consistent with the existing values and needs of the potential adopter. From an interview conducted, one noted that the technology was compatible with the current airport security operations. The findings of the study showed that 60.9 per cent agreed that the technology was compatible with the current airport security operations. In addition, 34.3 per cent had a neutral response to the statement. Further, 4.8 per cent strongly agreed to the statement of compatibility with operations. These results were in line with Sumner (2007) study which noted that compatibility with current airport security operations is key to adoption of a technology in enhancing airport security. The mean response rate was at 3.70 with a standard deviation of 0.552 indicating that majority agree of compatibility with operations.

Efficiency of Biometric Fingerprint Recognition

This study further sought to determine the efficiency of biometric fingerprint recognition in the airport. To determine whether the technology is efficient, several variables were put under study among them security level, increase in speed of procedures. Here, a five-point Likert scale was applied with ranged from 1 to 5 with 1 denoting strongly disagree, 2 representing disagree, 3 neutral, 4 agree and 5 strongly agree. The midpoint of the scale was a score of 3. The results were tabulated in Table 10 below.

On the aspect of increase in security level, 44.8 per cent had a neutral opinion. Further, 30.0 per cent agreed that adopting the technology could increase the level of security at the airport. Moreover, 25.2 per cent strongly agreed to the same. One interviewee noted that adopting the technology would increase the level of security at the airport. Further, a mean of 3.80 with a standard deviation of 0.815 was registered by the respondents. This implies that, in general, adopting the technology would increase the level of security at the airport. At the airport, there are several procedures that one usually undergoes. These were also put under study and aimed to know whether adopting this technology would improve the speed of the security procedures.

Table 10

Efficiency of Biometric Fingerprint Recognition

Efficiency	**2**	**3**	**4**	**5**	**Mean**	**Std. Dev**
	%	**%**	**%**	**%**		
Biometric Fingerprint recognition can increase the level of security	0.0	44.8	30.0	25.2	3.80	0.815
Biometric Fingerprint Recognition can speed up the security procedures	7.8	23.9	53.9	14.3	3.75	0.797
Biometric Fingerprint Recognition can speed up immigration	0.0	34.8	53.0	12.2	3.77	0.648
Biometric Fingerprint Recognition can speed up the boarding procedures	0.0	37.0	37.8	25.2	3.88	0.781
Biometric Fingerprint Recognition can speed up the check in procedures	0.0	33.0	59.1	7.8	3.75	0.589

Source: Field Data (2022).

One of the key informants also said;

> Adopting this technology would improve the speed of the security procedures. The biometric technology will replace passport checks by border guards, with the goal of increasing security and the ease of border crossing for travelers. Moreover, at the boarding places, the technology would replace manual passport checks (Respondent 08).

From the findings, 53.9 per cent agreed while 23.9 per cent had a neutral opinion. Furthermore, 14.3 per cent strongly agreed to the statement which implied that adoption of the technology would speed up the security procedures. However, only 7.8 per cent disagreed on the same. Generally, it would be advisable to adopt the technology since it would speed up the security procedures at the airport as evident from the mean response of 3.75 with a standard deviation of 0.797.

When asked whether the technology would speed up immigration, 53.0 per cent agreed to the statement. Further, 34.8 had a neutral opinion on the same. Only 12.2 per cent of the respondents strongly agreed to the aspect of speeding up immigration. One interviewee was neither in agreement nor disagreement that adopting the technology would speed up immigration. On average, 3.77 with a standard deviation of 0.648 had their response that the technology would speed up immigration. Therefore, from the findings, it would be sufficient to state that adopting biometric fingerprint recognition technology would speed up immigration.

Approximately 37.8 per cent agreed to the statement that adopting biometric fingerprint recognition would increase the speed of boarding processes at the gate, 37.0 per cent had a neutral opinion on whether or not to agree or disagree. About 25.2 per cent had a strong agreement on the same.

One of the key informants said;

> Adopting biometric fingerprint recognition would increase the speed of boarding processes at the gate. The technology would provide a touchless and seamless flow of passengers through a checkpoint, being suitable in a pandemic world and suitable for CBP, who envisage numerous passengers daily (Respondent 09).

It is clearly evident from the findings; it would be appropriate to state that adoption of the technology would speed up the boarding process at the gate as it is evident from the mean response of 3.88 with a standard deviation of 0.781.

The check-in procedures were also examined on whether adopting the technology would speed them up. Two interviewees noted that adopting the technology would speed up check-in procedures. From the results above, 59.1 per cent agreed to the statement while 33.0 per cent had a neutral opinion. However, only 7.8 per cent strongly agreed to the statement. On average, it would be appropriate to state that adopting the technology would speed up the check-in procedures as it is evident from the mean response rate of 3.75 with a standard deviation of 0.589.

Biometric Fingerprint Recognition and Airport Security

To determine whether biometric fingerprint recognition could have an influence on airport security, the researcher conducted Analysis of Variance (ANOVA). The independent variables of the study were factors that would be considered on whether to adopt biometric fingerprint recognition while the dependent variable of the study was airport security. Table 11 shows results of this analysis. ANOVA statistics test revealed that biometric fingerprint recognition had a significant influence on airport security. This implies that the technology has a positive impact on the state of security at the airports. From the findings, it was also clear that the technology had played a vital role in enhancing airport security. A sum of square due to regression of 3.486 was observed which imply that there was low variation of data points from the mean.

Table 11

ANOVA for Biometric Fingerprint Recognition and Airport Security

ANOVA

Source of Variation	Sum of Squares	DF	Mean Square	F	Sig.
Regression	3.486	1	3.486	94.316	.000*
Residual	8.428	228	0.037		
Total	11.914	229			

*Significant at *p*<0.05 level

Further, correlation statistics were conducted to determine whether there was any relationship between biometric fingerprint recognition and airport security. The results are shown in the Table 12 below.

Table 12

Correlation between Biometric Fingerprint Recognition and Airport Security

Correlations

		fingerprint	Airport security
Fingerprint	Pearson Correlation	1	.541**
	Sig. (2-tailed)		.000
Airport security	Pearson Correlation	.541**	1
	Sig. (2-tailed)	.000	

**. Correlation is significant at the 0.01 level (2-tailed).

Findings in Table 12 indicate a positive correlation of 0.541 between biometric fingerprint recognition and airport security. This implies that biometric fingerprint recognition is significant to airport security.

Adoption of Automated Passport Control

The third objective of the study was to examine the adoption of automated passport control. The study sought to determine a number of factors to consider before adopting the technology.

Training on Automated Passport Control

Before adopting a technology, it is crucial to understand whether the staff has received adequate training or not. Table 13 below shows the findings.

Table 13

Training on Automated Passport Control

Training	Frequency	Percentage
Yes	17	7.4
No	213	92.6
Total	**230**	**100.0**

Source: Field Data (2022)

From the findings presented in Table 13 above, majority (92.6%) indicated that they had not received training on Automated Passport Control technology. Moreover, 7.4 per cent indicated that they had received the training. According to Premkumar et al (1994), training on a technology is essential on whether or not to adopt the technology.

Support of Automated Passport Control

The study further sought to know whether the technology was supported by the respondents' organizations. Table 14 below shoe the results obtained.

Table 14

Support of Automated Passport Control

Support	Frequency	Percentage
Yes	87	37.8
No	143	62.2
Total	**230**	**100.0**

Source: Field Data (2022)

Results in Table 13 above indicate that majority (62.2%) of the respondents' organizations did not support the APC technology. However, 37.8 per cent indicated that their organization supported the technology. These findings are in line with Miltgen et al (2013) study where institutional support is key to adopting a technology

Automated Passport Control Variables

Similarly, whether or not to adopt biometric fingerprint recognition technology, this study took in to account factors that would be appropriate for making the decision. They include; familiarity, overall understanding, availability of information, compatibility with operations, customer experience and efficiency. Table 15 below shows a summary of the findings of the study.

Table 15

Adoption of Automated Passport Control factors

Variable under study	2	3	4	5	Mean	Std Dev
	%	%	%	%		
Automated Passport Control is familiar to every staff	16.5	5.2	48.7	29.6	3.91	1.003
Every staff has an overall understanding of Automated Passport Control when considering it for airport security	0.0	73.8	27.0	0.0	3.27	0.445
There is enough information available to make an informed decision on whether or not to incorporate Automated Passport Control	29.6	30.4	20.9	19.1	3.30	1.090
Automated Passport Control is compatible with current airport security operations	13.9	37.4	48.7	0.0	3.35	0.712
Automated Passport Control will boost customers' experience	32.2	46.1	13.9	7.8	2.97	0.881

Source: Field Data (2022).

From the findings of the study, 48.7 per cent agreed that they have a familiarity of the automated passport control technology. Approximately 29.6 per cent strongly agreed to the same. Furthermore, 16.5 per cent had a contrary response which was very alarming. However, only 5.2 per cent had a neutral response of neither agreeing nor disagreeing to the familiarity of the technology. Two interviewees noted that the technology was familiar to them and for operations at the airport. These results were in line with Sumner (2007) study which noted that familiarity is key to adoption of a technology in enhancing airport security. The findings further indicate that, on average, there was an agreement on familiarity of the technology as it was evident by a mean of 3.91 with a standard deviation of 1.003.

On whether every staff had an overall understanding of the technology for adoption, 73.8 per cent had a neutral response of neither agreeing nor disagreeing to have an overall understanding of the technology. This was alarming and incase of adoption of the technology, there has to be a training that has to be conducted. Further, 27.0 per cent agreed to understand the technology.

One of the key informants noted that;

> There was an overall understanding of how the technology works. Travelers are prompted to scan their passport, take a photograph using the kiosk, and answer a series of CBP inspection related questions verifying biographic and flight information. Once passengers have completed the series of questions, a receipt will be issued (Respondent 10).

These results were in line with Sumner (2007) study which noted that overall understanding is key to adoption of a technology in enhancing airport security. Therefore, on whether the staff had an overall understanding of the technology, it is clearly to state that most of the staff do not have a clear understanding as they had a neutral opinion as evident from the mean response of 3.27 with a standard deviation of 0.445.

Since most of the respondents had a neutral opinion, they had to be asked on whether there was enough information available to make an informed decision on whether or not to incorporate the technology. About 30.4 per cent were of neutral response, while 29.6 per cent had a disagreement on the statement. Furthermore, 20.9 per cent agreed to the statement while 19.1 per cent strongly agreed to the statement.

One of the key informants said;

> There was enough information available to make an informed decision on whether or not to incorporate the technology. Information on what the technology is, how it works, the advantages and disadvantages of automated passport control is available for me to make an informed decision on whether or not to incorporate the technology (Respondent 11).

These results were in line with Sumner (2007) study which noted that availability of information to make an informed decision is key to adoption of a technology in enhancing airport security. It is clearly evident that most of the respondents had a 50-50 opinion on whether there was information available on whether to incorporate the technology or not as it was seen by their mean of 3.30 with a standard deviation of 1.090.

Compatibility with operations is crucial to any technology, as of the key informants said;

> The technology was compatible with the current airport security operations. With the advances in technology now in the nation, automated passport control technology is the way to go. The airport security operations now are beefed up and the technology would be an actual fit for the operations (Respondent 12).

This factor was put under consideration and from the findings, 48.7 per cent agreed that the technology would be compatible to their security operations. Approximately 37.4 per cent were of neutral opinion. Only 13.9 per cent disagreed to the statement. These results were in line with Sumner (2007) study which noted that compatibility with current airport security operations is key to adoption of a technology in enhancing airport security. From the findings it would be appropriate to mention that the technology would be compatible with the airport security operations since majority agreed to the statement as seen from the mean response of 3.35 with a standard deviation of 0.712.

Another aspect that was put under study was the customers' experience with this technology. On whether the technology would boost customers' experience, 46.1 per cent had a neutral opinion. Further, 32.2 per cent agreed to the same. Moreover, 13.9 per cent of the respondents agreed that the technology would boost customers' experience. However, 7.8 per cent strongly agreed that the technology would boost customers' experience.

In addition, a key informant said;

> Adopting automated passport control technology would boost customers' experience. The APC kiosks would help customers to experience a difference in operations. At the airport, there will be reduced queues, efficiency and accuracy which will boost customers' experience (Respondent 13)

On average, most of the respondents had a neutral response as seen from the mean of 2.97 with a standard deviation of 0.881.

Efficiency of Automated Passport Control

This study further sought to determine the efficiency of Automated Passport Control in the airport. To determine whether the technology is efficient, several variables were put under study among them security level, increase in speed of procedures. Here, a five-point Likert scale was applied with ranged from 1 to 5 with 1 denoting strongly disagree, 2 representing disagree, 3 neutral, 4 agree and 5 strongly agree. The midpoint of the scale was a score of 3. The results were tabulated in Table 16 below.

From Table 16, the efficiency of the technology was put under study and the findings indicated that 61.7 per cent agreed that the technology would improve the level of security. Approximately 16.5 per cent disagreed to the same while 13.9 per cent had a neutral opinion on the matter. However, only 7.8 per cent had a strong agreement that adopting the technology would improve the level of security.

One of the key informants said;

> Adopting the technology would increase the level of security at the airport. The system provides border agents with a useable flow of information, including data from passports, visas, watch lists, Passenger Name Record, Advanced Passenger Information (Respondent 16).

Table 16

Efficiency of Automated Passport Control

Efficiency	2	3	4	5	Mean	Std. Dev
	%	%	%	%		
Automated Passport Control can increase the level of security	16.5	13.9	61.7	7.8	3.61	0.853
Automated Passport Control can speed up the security procedures	16.5	61.7	13.9	7.8	3.13	0.777
Automated Passport Control can speed up immigration	33.0	29.6	21.7	15.7	3.20	1.067
Automated Passport Control can speed up the boarding procedures	5.2	35.7	24.3	34.8	3.89	0.951
Automated Passport Control can speed up the check in procedures	16.5	56.5	15.7	11.3	3.22	0.854

Source: Field Data (2022).

From the mean response, it is clear that the technology would boost the level of security since an average of 3.61 with a standard deviation of 0.853 was observed which meant that majority of the respondents agreed that the level of security would be boosted.

Approximately 61.7 per cent had a neutral response on whether the technology would speed up the security procedures or not. 16.5 per cent disagreed with the statement. Further, 13.9 per cent agreed that the technology would speed up security procedures. However, it was observed that only 7.8 per cent of the respondents were in strong agreement that the technology would speed up the security procedures.

One of the key informants said;

> Adopting this technology would improve the speed of the security procedures. Automated Passport Kiosks efficiently manage passenger flow, whilst capturing imperative data and managing safe and secure access control. This reassures border authorities that essential biometric acquisition, health screening and passport scanning are being taken care of by a self-service solution (Respondent 15).

Therefore, it can be concluded that adopting the technology would neither speed up nor slow down the operations since majority of the respondents were not sure as seen from the mean response of 3.13 with a standard deviation of 0.777.

The findings further indicate that 33.0 per cent disagreed with the statement that incorporating the technology would speed up immigration processes. Further, 29.6 per cent were undecided with neither agreeing nor disagreeing with the statement. In addition, 21.7 per cent agreed to the statement which implied, from their response, that the technology would speed up immigration processes. However, only 15.7 per cent strongly agreed to the statement.

One of the key informants said;

> Use of mobile passport control is free and does not require pre-approval. Travelers who successfully use the mobile passport control app will no longer have to complete a paper form or use an APC kiosk. As a result, travelers may experience shorter wait times, less congestion and efficient processing (Respondent 16).

From the mean response of 3.20 with a standard deviation of 1.067, it is clear that most of the respondents had a neutral response on whether adopting the technology would speed up immigration processes.

On whether the technology would speed up the boarding procedures at the gate, 35.7 per cent were in a neutral opinion. 34.8 per cent strongly agreed on the statement. Moreover, 24.3 per cent agreed that the technology would speed up boarding process. however, 5.2 per cent disagreed to the statement.

One of the key informants said;

> Adopting automated passport control would increase the speed of boarding processes at the gate. Waiting times are reduced, and passengers can carry out the checks themselves in just a few seconds, meaning less hassle and more dwell time in the duty-free area (Respondent 17).

Adopting the technology would clearly speed up the boarding procedures as its evident from the mean of the responses which is 3.89 with a standard deviation of 0.951. Therefore, it would be appropriate to say that the technology would speed up the boarding procedures.

Check-in procedures are essential for at the airport. From the study, 56.5 per cent had a neutral opinion on the matter. Further, 16.5 per cent disagreed while 15.7 per cent agreed to the same. The findings further indicate that 11.3 per cent of the respondents strongly agreed that adopting the technology would speed up the check-in procedures.

One of the informants said;

> Adopting the technology would speed up check-in procedures. Travelers using APC experience shorter wait times, less congestion, and faster processing this will in turn reduce the check-in procedures (Respondent 18).

On average, it is appropriate to mention that adopting the technology would neither speed up the check-in procedures nor slow down the procedures as it is evident from the mean response of 3.22 with a standard deviation of 0.854.

Automated Passport Control and Airport Security

To determine whether Automated Passport Control could have an influence on airport security, the researcher conducted Analysis of Variance (ANOVA). The independent variables of the study were factors that would be considered on whether to adopt automated passport control while the dependent variable of the study was airport security. Tables 17 shows results of this analysis.

Table 17

ANOVA for Automated Passport Control and Airport Security

ANOVA

Source of Variation	Sum of Squares	DF	Mean Square	F	Sig.
Regression	3.853	1	3.853	108.999	.000*
Residual	8.060	228	0.035		
Total	11.914	229			

*Significant at *p*<0.05 level

ANOVA statistics test revealed that automated Passport Control had a significant influence on airport security. This implies that the technology has a positive impact on the state of security at the airports. From the findings, it was also clear that the technology had played a vital role in enhancing airport security. A sum of square due to regression of 3.853 was observed which imply that there was low variation of data points from the mean.

Further, correlation statistics were conducted to determine whether there was any relationship between biometric fingerprint recognition and airport security. The results are shown in the Table 18. Findings in Table 18 indicate a positive correlation of 0.541 between automated passport control and airport security. This implies that automated passport control is significant to airport security.

Table 18

Correlation between Automated Passport Control and Airport Security

Correlations

		APC	Airport security
APC	Pearson Correlation	1	$.569^{**}$
	Sig. (2-tailed)		.000
Airport security	Pearson Correlation	$.569^{**}$	1
	Sig. (2-tailed)	.000	

**. Correlation is significant at the 0.01 level (2-tailed).

Regression Statistics

The following is the regression model:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

whereby;

Y = Airport Security

β_0 = Constant

$\beta_1, \beta_2, \beta_3, \beta_4$ = Coefficients of determination

X_1 = Effectiveness of Biometric Face Recognition

X_2 = Adoption of Biometric Fingerprint recognition

X_3 = Adoption of Automated Passport Control ε = Error term

From the study, $\beta_0 = 2.220 \times 10^{-16}, \beta_1 = 0.596, \beta_2 = 0.636, \beta_3 = 0.557$.

Substituting these values in the equation;

$$Y = 2.220 \times 10^{-16} + 0.596X_1 + 0.636X_2 + 0.557X_3 + \varepsilon$$

From the ANOVA and correlation tables, it is clear that both β_1, β_2, and β_3 are significant to Y which implies

that both biometric facial, fingerprint recognition and automated passport control technologies are significant to airport security.

CONCLUSIONS AND RECOMMENDATIONS

The first research question was how effective is the biometric face recognition in enhancing airport security in JKIA, Kenya and from the study findings, it was found out that majority of the members of the staff at the airport felt that although biometric facial recognition works efficiently to combat security issues at the airport, the technology faces its own challenges which needed to be addressed efficiently. The study concludes that biometric facial recognition has a positive influence on airport security and plays a vital role in enhancing airport security. With facial recognition, airport security gets fast, accurate identity verification, so they can screen more passengers with fewer personnel.

The second research question was whether or not biometric fingerprint identification system should be adopted in enhancing airport security in JKIA, Kenya and from the study findings, adopting biometric fingerprint recognition system would play a major role in enhancing airport security. These findings further depict that majority of the staff were in support with the adoption of the technology at the airport. For incorporation of the technology, the study showed that all that were needed to adopt the technology were available. The study concludes that adopting biometric fingerprint recognition would have a positive impact on airport security. Fingerprint recognition technology provides high levels of security and reliability to address requirements related to identification and verification of personal identities hence enhances airport security.

The third research question was whether or not automated passport control system should be adopted in enhancing airport security in JKIA, Kenya and from the study findings, that majority of the respondents had a neutral opinion on all factors. The familiarity of the technology, efficiency of the technology and more generally overall understanding of the technology. The study concludes that adopting the technology would have a positive impact on airport security. Automated Passport Kiosks efficiently manage passenger flow, whilst capturing imperative data and managing safe and secure access control.

Based on Based on the study limitations, gaps and challenges experienced and also considering the study specific objectives, the following are the recommendations drawn for the study:

- Since biometric facial recognition technology plays an important role in enhancing airport security, the study recommends that more efforts should be put in the technology so as to enhance its efficiency as well as curb the challenges that it faces. This will ease the modes of operations at the airport.
- It would be efficient to adopt the biometric fingerprint recognition technology at the airport. However, the airport management should ensure that there is enough information available as well as training the staff appropriately to be able to use the technology.
- The study further recommends that it would be appropriate to incorporate automated passport control technology at the airport. Moreover, the study recommends thorough training on the staff as well as familiarizing the technology with the staff at the airport so as to improve its efficiency.

- From the findings of the study, it is recommended that biometric facial recognition, biometric fingerprint recognition and automated passport control should be put together to enhance airport security and also improve the efficiency of handling security issues at the airport.

Contributions of the Study

This study contributes to the growing literature regarding airport security and the role that biometric systems are deemed to have in heightening that security. After September 11th, 2001, the area of airport security came under extreme scrutiny. The literature surrounding the need for increased airport security and the appropriate mechanisms for success, while growing, has been based primarily on tentative arguments and less on empirical data. This study's primarily contribution is to offer the only nationwide study to empirically question airport security directors on their perceptions regarding biometric systems and to statistically test hypotheses regarding the likelihood of adoption of biometric systems by security directors for airport access control.

Theoretically, this study adds credence to previous studies regarding technology adoption conducted by Khan and Efthymiou, (2021), Sumner, (2007) and Spreeuwers et al. (2012), by suggesting that compatibility, overall understanding, availability of information to make an informed decision and customers' experience are important factors regarding the acceptance of biometric technology. By utilizing the results of this study, national regulators, can tangibly assess the perceptions that airport security directors have towards biometric applications and can, therefore, develop practical working solutions for guidance and support.

Areas for Further Research

As in all studies, this study highlights that there are many additional areas of research and consideration that can be explored with regard to biometric technology for airport access control. The first is that this study could be conducted on a global scale rather than limited to only JKIA. The use of email distribution and that ability of participants to respond via a web-based survey would allow for a quick, easy, confidential, and inexpensive method to survey airport security directors world-wide on their propensity to adopt biometric technology for airport access control. The responses from a global survey could be compared and/or contrasted to the response generated by this study which would make the responses generalizable on a world-wide scale rather than to just those airports in JKIA.

Secondly, the survey instrument used in this study could be used to measure the perceptions and the propensity to adopt biometric technology by those outside the realm of airports. For example, decision makers in any area in which biometric technology could be implemented into an access control system could be surveyed via the instrument used in this study. Hospitals, ports, government buildings, and nuclear plants are all examples of facilities that could potentially use biometric technology for access control purposes. Decision makers at each of these locations represent a population whose propensity to adopt biometric technology could be measured and examined.

REFERENCES

Abdelbary, A. M. (2011). Exploration of factors affecting adoption of biometric technology by five-star Egyptian hotel employees. *Iowa State University*.

Adam, A. M. (2020). Sample size determination in survey research. *Journal of Scientific Research and Reports*, 90-97.

Alameri, T., Hammood, M. N., Mezaal, J. K., & Eneizan, B. (2022). E-Payment Model For The Iraqi Public Sector: A Passport Issuance E-System. *Journal Of Engineering Science And Technology*, *17*(1), 0435-0451.

Aleksander, I., Clarke, T. J. W., & Braga, A. P. (1994). Binary neural systems: combining weighted and weightless properties. *Intelligent Systems Engineering*, *3*(4), 211-221.

Al-Raisi, A. N., & Al-Khouri, A. M. (2008). Iris recognition and the challenge of homeland and border control security in UAE. *Telematics and Informatics*, *25*(2), 117-132.

Anderson, M. S., & Steneck, N. H. (2011, January). The problem of plagiarism. In *Urologic Oncology: Seminars and Original Investigations* (Vol. 29, No. 1, pp. 90-94). Elsevier.

Anderson, R. (2017). Placing the Nation: The Politics of Spatial Production at Auckland Airport and Wellington Airport. *Journal of Pacific Archaeology–Vol, 10*(2).

Arif, M., Xinquan, Z., Rahman, M., & Kumar, S. (2013). A predictive model of the critical undeformed chip thickness for ductile–brittle transition in nano-machining of brittle materials. *International Journal of Machine Tools and Manufacture, 64*, 114-122.

Bager, L., Elsbernd, A., Nissen, A., Daugaard, G., & Pappot, H. (2018). Danish translation and pilot testing of the European Organization for Research and Treatment of Cancer QLQ-TC 26 (EORTC QLQ-TC26) questionnaire to assess health-related quality of life in patients with testicular cancer. *Health and Quality of Life Outcomes*, *16*(1), 1-6.

Black, S., &Daéid, N. N. (2018). 30-Second Forensic Science: 50 key topics revealing criminal investigation from behind the scenes, each explained in half a minute. *Ivy Press*.

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.

CBP. (2016). Preclearance Guidance Fy-2016-Final U.S. Customs And Border Protection [Online] Available From. *Https://Www.Cbp.Gov/Document/Guidance/Preclearanceguidance-Fy-2016-Final. [22 February 2021].*

Chan, S. H., & Lay, Y. F. (2018). Examining the reliability and validity of research instruments using partial least squares structural equation modeling (PLS-SEM). *Journal of Baltic Science Education*, *17*(2), 239.

Clarke, R. V. (2017). “Situational” crime prevention: Theory and practice. In *Crime Opportunity Theories* (pp. 471-482). Routledge.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review,* 588-608.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology, 44*(2), 431-464.

Crumpler, W. (2020). How Accurate are Facial Recognition Systems–and Why Does It Matter. *Center for Strategic and International Studies, 14*.

Del Rio, J. S., Moctezuma, D., Conde, C., de Diego, I. M., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. *Computers & security*, *62*, 49-72.

Dillingham, G.L. (2003). Aviation Security: Progress Since September 11, 2001, and the Challenges Ahead. In J. Zellan (Ed.), Aviation Security: Current Issues and Development (pp. 1-21). *New York: Nova Science,* Inc.

Dos Santos, C. E., & Schwartz, W. R. (2014, August). Extending face identification to open-set face recognition. In *2014 27th SIBGRAPI Conference on Graphics, Patterns and Images* (pp. 188-195). IEEE.

Dubey, R., Luo, Z., Gunasekaran, A., Akter, S., Hazen, B. T., & Douglas, M. A. (2018). Big data and predictive analytics in humanitarian supply chains: Enabling visibility and coordination in the presence of swift trust. *The International Journal of Logistics Management*.

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010, October). A study of users' acceptance and satisfaction of biometric systems. In *44th Annual 2010 IEEE International Carnahan Conference on Security Technology* (pp. 170-178). IEEE.

Ferrara, M., Franco, A., & Maltoni, D. (2016). On the effects of image alterations on face recognition accuracy. In *Face recognition across the imaging spectrum* (pp. 195-222). Springer, Cham.

Flynn, M., Smitherman, H. M., Weger, K., Mesmer, B., Semmens, R., Van Bossuyt, D., & Tenhundfeld, N. L. (2021, April). Incentive Mechanisms For Acceptance And Adoption Of Automated Systems. In *2021 Systems And Information Engineering Design Symposium (Sieds)* (Pp. 1-6). Ieee.

Hoge, J. F. & Rose, G. (2010). How Did This Happen? Terrorism and the New War. *New York: Public Affairs.*

Jain, A. K., Arora, S. S., Cao, K., Best-Rowden, L., & Bhatnagar, A. (2016). Fingerprint recognition of young children. *IEEE Transactions on Information Forensics and Security*, *12*(7), 1501-1514.

Kamau, P. M. K. D. P., & Mireri, C. (2016). Assessment Of the Security Preparedness And Adherence To International Civil Aviation Standards At Wilson Airport, Kenya.

Kant, C., & Nath, R. (2009). Reducing process-time for fingerprint identification system. *International Journals of Biometric and Bioinformatics*, *3*(1), 1-9.

Kenya Airport Authority. KAA. (2018).

Kenya Nation Bureau of Statistics [KNBS] (2019). 2019 Kenya Population and Housing Census Vol. I. Population by County and Sub County. www.knbs.or.ke

Kenya Vision 2030 Blueprint, 2009.

Khan, N., & Efthymiou, M. (2021). The Use of Biometric Technology At Airports: The Case Of Customs And Border Protection (Cbp). *International Journal Of Information Management Data Insights*, *1*(2), 100049.

Kirschenbaum, A. A. (2013). The cost of airport security: The passenger dilemma. *Journal of Air Transport Management*, *30*, 39-45.

KivutiNjeru, S., & Oboko, R. (2016). Comparative analysis of minutiae-based fingerprint matching algorithms. *AIRCC's International Journal of Computer Science and Information Technology*, *8*(6), 59-71.

Kosmerlj, M., Fladsrud, T., Hjelmås, E., & Snekkenes, E. (2006, January). Face recognition issues in a border control environment. In *International Conference on Biometrics* (pp. 33-39). Springer, Berlin, Heidelberg.

Kramer, R. S., Mireku, M. O., Flack, T. R., & Ritchie, K. L. (2019). Face morphing attacks: Investigating detection with humans and computers. *Cognitive research: principles and implications*, *4*(1), 1-15.

Kwakye, M. M., Boforo, H. Y., & Badzongoly, E. L. (2015). Adoption of Biometric Fingerprint Identification as an Accessible, Secured form of ATM Transaction Authentication. *International Journal of Advanced Computer Science and Applications*, *6*(10), 253-265.

Lai, X., & Rau, P. L. P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior*, *124*, 106894.

Lazarick, R. (1998, June). Airport Vulnerability Assessment: An Analytical Approach. *Proceedings of the NDIA Security Technology Symposium*, pg: 218- 226.

Lee, G., Hollinger, R. C., & Dabney, D. A. (1999). The relationship between crime and private security at US shopping centers. *American Journal of Criminal Justice*, *23*(2), 157-177.

Lombardi, S., Saragih, J., Simon, T., & Sheikh, Y. (2018). Deep appearance models for face rendering. *ACM Transactions on Graphics (TOG)*, *37*(4), 1-13.

Lyal, C. H., & Miller, S. E. (2020). Capacity of United States federal government and its partners to rapidly and accurately report the identity (taxonomy) of non-native organisms intercepted in early detection programs. *Biological Invasions*, *22*(1), 101-127.

Lyamin, A. V., & Cherepovskaya, E. N. (2016). An approach to biometric identification by using low-frequency eye tracker. *IEEE Transactions on Information Forensics and Security*, *12*(4), 881-891.

Madara, D. J. A., Okeyo, G., & Kimwele, M. (2017). A Fingerprint &Pin Authentication to Enhance Security At The Automatic Teller Machines.

Maheswari, S. U., & Chandra, E. (2013). An Efficient Fingerprint Denoiser for Fingerprint Recognition. *International Journal of Computer Applications*, *66*(22).

Makrushin, A., Neubert, T., & Dittmann, J. (2019). Humans Vs. Algorithms: Assessment of Security Risks Posed by Facial Morphing to Identity Verification at Border Control. In *VISIGRAPP (4: VISAPP)* (pp. 513-520).

Mandala, M. (2016). Terrorist assassinations: a criminological perspective. *The handbook of the criminology of terrorism*, 353.

Menzel, D., & Hesterman, J. (2018). Airport security threats and strategic options for mitigation. *Journal of Airport Management, 12*(2), 118-131.

Milivojevic, S. (2019). Border Policing and Security Technologies: Mobility and Proliferation of Borders in the Western Balkans. *Routledge.*

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision support systems, 56*, 103-114.

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Albahri, O. S., Alsalem, M. A., & Mohammed, K. I. (2018). Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: A multi-layer systematic review. *Journal of medical systems*, *42*(12), 238.

Mugenda, O., & Mugenda, A. (2003). Research methods: Quantitative and qualitative approaches. 2nd. *Rev. Ed. Nairobi*.

Negri, N. A. R., Borille, G. M. R., & Falcão, V. A. (2019). Acceptance of biometric technology in airport check-in. *Journal of Air Transport Management*, *81*, 101720.

Odhiambo, C. (2019). Use of Passenger Profiling to Enhance Aviation Security in Kenya *(Doctoral dissertation, United States International University-Africa).*

Patel, H., & Asrodia, P. (2012). Employee Attendance Management System Using Fingerprint Recognition. *International Journal of Electrical, Electronics and Computer Engineering*, *1*(1), 37-40.

Perry, S. C. (2014). What are your airport access control's weak links? LCN. http://www.lcnclosers.com/Whats_new_10_10_03.asp.

Plonsky, L., & Derrick, D. J. (2016). A meta-analysis of reliability coefficients in second language research. *The Modern Language Journal*, *100*(2), 538-553.

Putra, B. H., & Arifin, R. (2020). The Adoption Of Border Technology Of Immigration Control And Autogates In Indonesia. *Sintech (Science And Information Technology) Journal*, *3*(2), 137-148.

Ramos, A. P., Gustafsson, O., Labert, N., Salecker, I., Nilsson, D. E., &Averof, M. (2019). Analysis of the genetically tractable crustacean Parhyalehawaiensis reveals the organisation of a sensory system for low-resolution vision. *BMC biology*, *17*(1), 1-19.

Robertson, D. J., Mungall, A., Watson, D. G., Wade, K. A., Nightingale, S. J., & Butler, S. (2018). Detecting morphed passport photos: A training and individual differences approach. *Cognitive research: principles and implications*, *3*(1), 1-11.

Roncek, D. W., & Maier, P. A. (1991). Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of "hot spots". *Criminology*, *29*(4), 725-753.

Ros, T., Enriquez-Geppert, S., Zotev, V., Young, K. D., Wood, G., Whitfield-Gabrieli, S., ... & Thibault, R. T. (2020). Consensus on the reporting and experimental design of clinical and cognitive-behavioural neurofeedback studies (CRED-nf checklist).

Roth, P. L., & Craig, A. (1998). Response rates in HRM/OB survey research: Norms and correlates, 1990–1994. *Journal of management*, *24*(1), 97-117.

Sagawa, T., Murakami, T., Kano, T., Ito, W., Nakayama, M., & Ote, I. (2016). Integrated Physical Security Platform Concept Meeting More Diverse Customer Needs. *Hitachi Review*, *65*(8), 353.

Schwarz, F., Schwarz, K., & Creutzburg, R. (2021). Improving Detection of Manipulated Passport Photos-Training Course for Border Control Inspectors to Detect Morphed Facial Passport Photos-Part I: Introduction, State-of-the-Art and Preparatory Tests and Experiments. *Electronic Imaging*, *2021*(3), 136-1.

Sidiropoulos, G. K., & Papakostas, G. A. (2021, May). Machine Biometrics-Towards Identifying Machines in a Smart City Environment. In *2021 IEEE World AI IoT Congress (AIIoT)* (pp. 0197-0201). IEEE.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., &Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, *3*(1), 3.

Siyal, A. A., Shamsuddin, M. R., Rabat, N. E., Zulfiqar, M., Man, Z., & Low, A. (2019). Fly ash based geopolymer for the adsorption of anionic surfactant from aqueous solution. *Journal of Cleaner Production*, *229*, 232-243.

Smith, M. J., & Clarke, R. V. (2012). Situational crime prevention: Classifying techniques using "good enough" theory. *The Oxford handbook of crime prevention*, 291-315.

Smith, W. R., Frazee, S. G., & Davison, E. L. (2000). Furthering the integration of routine activity and social disorganization theories: Small units of analysis and the study of street robbery as a diffusion process. *Criminology*, *38*(2), 489-524.

Tassabehji, R., & Kamala, M. A. (2009, December). Improving e-banking security with biometrics: Modelling user attitudes and acceptance. In *2009 3rd International Conference on New Technologies, Mobility and Security* (pp. 1-6). IEEE.

Teodorović, S. (2016). The role of biometric applications in air transport security. *Nauka, bezbednost, policija*, *21*(2), 139-158.

Trockel, M., Bohman, B., Lesure, E., Hamidi, M. S., Welle, D., Roberts, L., & Shanafelt, T. (2018). A brief instrument to assess both burnout and professional fulfillment in physicians: reliability and validity, including correlation with self-reported medical errors, in a sample of resident and practicing physicians. *Academic Psychiatry*, *42*(1), 11-24.

Uchenna, C. P., Pascal, A., & Prince, O. (2018). Evaluation of a Fingerprint Recognition Technology for a Biometric Security System. *American Journal of Computer Science and Technology*, *1*(4), 74-84.

Watson, R. (2015). Quantitative research. *Nursing Standard (2014+)*, *29*(31), 44.

Weisburd, D., Bushway, S., Lum, C., & Yang, S. M. (2004). Trajectories of crime at places: A longitudinal study of street segments in the city of Seattle. *Criminology*, *42*(2), 283-322.

Westlake, B., Bouchard, M., & Frank, R. (2017). Assessing the validity of automated webcrawlers as data collection tools to investigate online child sexual exploitation. *Sexual Abuse*, *29*(7), 685-708.

Widdowson, D. (2007). The Changing Role of Customs: Evolution or Revolution. *World Customs Journal*, *1*(1), 31-37.

Wojtaszek, M. (2018). What You Touch Is (Not) What You See. The Haptic Unconscious and Digital In-corporeality in the Airport Space. *PrzeglądKulturoznawczy*, *38*(4), 536-549.

Worrall, J. L. (2000). The routine activities of maritime piracy. *Security Journal*, *13*(4), 35-52.