THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Biometric Properties for Identification in a Secure E-voting Application

Erick K. Rotich
Chief Technologist, Department of Maths and Computer Science, University of Eldoret, Kenya
Ph.D. Student, Kibabii University, Kenya
Ikoha Anselemo P.
Lecturer, Department of Information Technology, Kibabii University, Kenya
Jotham M. Wasike
Librarian, Department of Library Services, Kirinyaga University, Kenya

Abstract:
Most of the E-voting architectures used currently to identify and verify a voter use single biometric source. Single biometric source have many problems which include noisy data, intra class disparity, inter class resemblances, universality, spoofing and insecure. On the other hand, multi-biometric sources use multiple source of information for individual authentication. The purpose of this paper was to investigate biometric properties for identification in secure e-voting applicationsfor identification that can be used to enhance security. This study was undertaken using mixed method design which included survey design and content analysis. Purposive sampling technique was used to sample the respondents. The study found that biometric properties for identification in a secure e-voting application vary in their application. The finding of this study is significant to Independent Electoral and Boundaries Commission (IEBC) and to the government in enhancing use of E-voting to improve transparency.

Keywords: *Biometric, E-voting, Security*

1. Introduction

Conventionally the use of biometric devices has enhanced the competence of providing authentication to access physical installations. Biometric is the technology of using human's unique physiological, behavioral, and morphological characteristic for positive personal identification. The technology is currently available for scanning fingerprints, handprints, iris, retina patterns, and face. Voice, signature and keystroke systems are close to biometric although they are not classified as such. In future the use of biometric is expected to grow hence becoming much more commonplace. Certain applications of biometric identification technology are now cheap, reliable and highly accurate (Tripathi, 2011). The biometric Features include uniqueness, universality, performance, and measurability and user friendliness. The advantages and features of biometric will enhance the voter authentication as well as building the competence of the voters to use the developed architecture.

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, Deoxyribonucleio Acid (DNA), and signatures. According to Dileep & Yeonseung, (2009) Using biometric systems is a powerful tool in identification and authentication issues in various areas including; immigration and customs, forensics, physical as well as computer security.

The paper is organized as follows. Section 1.1 describes E-voting implementation in developing countries. Section 1.2 describes Single and Multi-source Biometric. Section 1.3 presents biometric applications. Section 2.0 problem statement. Section 3.1 provides Study Population. Section 3.2 provides Data analysis. Section 4.0 presents the Findings. Section 5.0 provides discussion. Section 6.0 provides the conclusion and Section 7.0 provides Recommendation.

1.1. E-voting Implementation in Developing Countries

One of the gaps that exist in E-voting implementation in developing countries is the lack of spread of Internet connectivity and electricity. This gap provides a foundation for the research in which an E-voting architecture needs to be developed based on a polling station setup involving network technologies for example 3G and 4G technology and General Packet Radio Service (GPRS) for data transfer (Olaniyi, Adewumi & Arulogun, 2011).

An electronic voting (E-Voting) system is a structure where the election results are processed by way of recording and storing it as digital information (Abdalla & Samani, 2013). Punched cards, optical scan voting systems and specialized voting kiosks are classified as electronic voting technologies. It includes transmission of ballots through telephones, the Internet or personal computer networks.

There are generally two main types of E-voting; Supervised E-voting in which Electoral commissions physically supervise the election and Remote E-voting where Voters vote using their own computers, cellular phones or using the Internet (Buchsbaum, 2004). Some of the advantages of electronic voting technology are cost savings, increased participation rates, better informed voters, reduced administration, generate and deploy ballot fast and with no difficulty, Integrity of the vote, instant runoffs, last minute changes to the ballot, removal of human error in the vote counting, no need for recounts (Riera & Brown, 2003).

1.2. Single and Multi-source Biometric

In a secure e-voting application, single source biometric systems frequently face significant limitations due to noise in sensed data, spoof attacks, lack of distinctiveness, data quality, restricted level of freedom, non-universality, and other factors. Multi-source biometric systems are used because they increase the performance and enhance security that may not be attainable by using a single source biometric (Dileep & Yeonseung, 2009). Single biometric source has many problems such as noisy data, intra class disparity, inter class resemblances, not universal, sometimes can be affected by spoofing and at some point can be inaccurate or insecure (Kumari & Jaya, 2014).
According to Vishal, (2014) E-voting system using biometric allows a voter to cast his/her vote using internet in a polling place, double voting is not possible and entities know the voting result.

1.3. Biometric application

In this section biometric application in banking and payment are presented.
Figure 1.3.1 shows Usage of Biometric Technologies among banks in the United States of America.

1.3.1. Usage of Biometric Technologies Among banks in the United States of America

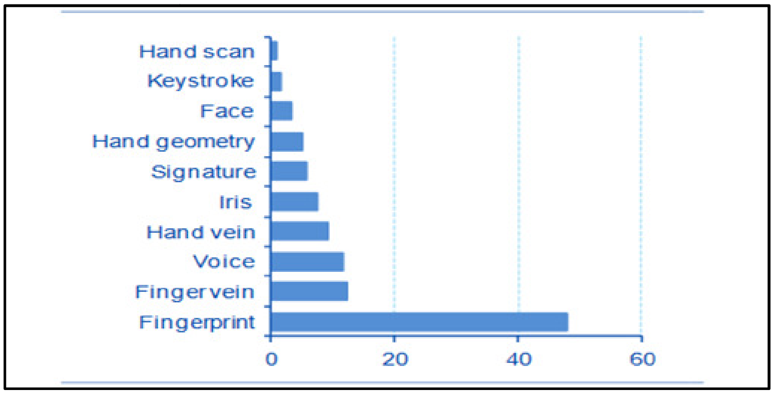

Figure 1
Source (adopted from Nathaniel, 2015)

Figure 1 suggests that although the entire biometric source has been used in America fingerprint has been used the most with about 45%. This confirms that fingerprint is the most studied biometric source supported by advanced development of devices used to scan fingerprints. Finger vein, voice and hand vein have attracted about 17% and on the least usage is the Hand scan and Keystroke,

Table 1 shows Biometric usage in Kenya, Canada, Ghana, U.S.A and Nigeria between 2006 and 2015.

Year	Country	Application Area	Type of biometric	Source
2013	Kenya	Voter registration and Identification	fingerprint-based biometrics	European Union Election Observation Mission to Kenya
2006	Canada	Staff Identification working in the secure areas in the Airport	Fingerprints biometric	http://www.cic.gc.ca/english/ department/biometrics-use.asp
2015	U.S.A	Patient identification	Fingerprint identification	http://www.biometricupdate.com/ wp-content/uploads/2015/02/biometric- in Healthcare.pdf
2012	Ghana	Voter registration and Verification identification	Fingerprints	https://www.genkey.com/news/ghana-uses-biometric-voter-verification-for-third-election-running/
2007	Nigeria	Voter registration and verification	Fingerprints	http://www.m2sys.com/biometric-fingerprint-software-case-studies-nigerian-voter-registration/
2015	United Arab Emirates	Screening at the airport	Eyes, iris, face and fingerprint	Iritech, Inc, (2016)

Table 1: Biometric usage

From Table 1 it can be seen that many countries have used biometric mainly the fingerprint, eyes and face. The application also vary, Kenya for example used fingerprint for Voter registration and Identification in 2013, staff identification at the airport in Canada 2006, patient identification U.S.A 2015, Voter registration and verification and identification in Ghana 2012 and in Nigeria in 2007. United Arab Emirates used eyes, iris, face and fingerprint for screening at the airport.

2. Problem Statement

Most of the E-voting architectures used currently to identify and verify a voter uses single biometric source mainly the fingerprint (Hazzaa & Kadry, 2012). Single biometric source has many problems such as noisy data, intra class disparity, inter class resemblances, not universal, sometimes can be affected by spoofing and at some point can be inaccurate or insecure (Kumari & Jaya, 2014). Multi-biometric sources use multiple source of information for individual authentication (Sanjekar & Patil, 2014) which eliminates irregularities in voter identification, vote casting, and vote counting, vote tallies and auditing. E-voting implementation in developing countries is hindered by lack of implementation of multi-biometric technologies. This study considered multi-biometric approach architecture to develop a secure electronic voting application. This approach addressed the gap observed in the single biometric approach.

3. Methodology

This study was undertaken using mixed method design which included survey design and content analysis. Purposive sampling technique was used to sample sixty six election coordinators and their deputies and two Information Communication Technology Officers from two Independent Electoral and Boundaries Commission (IEBC) regions of Kakamega and Bungoma. This study focused on the opinion of the IEBC Regional ICT officers and constituency election coordinators on ways and means in which a secure E-voting architecture can be developed.

3.1. Study Population

The population that was used for inclusion in this study was the IEBC constituency election coordinators and their deputies as well as IEBC Regional ICT officers Table 2.

Table 2 provides the study population.

Participants	Kakamega County	Bungoma County	Total
Election Coordinators	34	32	66
ICT Staff	1	1	2
Total	**35**	**33**	**68**

Table 2: Study Population

Table 2 shows that the study population comprised 34 election coordinators from Kakamega and 32 election coordinators from Bungoma, two Regional ICT officers one each from Kakamega and Bungoma IEBC regions giving a total of 68 respondents.

3.2. Data Analysis

The research adopted survey strategy; information was collected from a sample of the respondents by administering structured questionnaires. Descriptive and inferential statistics were used for the data analysis. Descriptive statistics was used to analyze data collected through questionnaire and Pearson’s Rank correlation was performed to measure the relationship between dependent and independent variables.

4. Findings and Discussions

The findings of this study were based on multimodal system, biometrics tool, multi-source biometric system, Multiple Parameters for Secure authentication, Passwords, IDs and PINs for User Identification are presented.

4.1. Fingerprints

The study sought to establish that fingerprints are unique, permanent, and easy to acquisition and the results are shown in Table 3

Fingerprints are probably the more extensively studied biometric		Region		Total
		Kakamega	Bungoma	
strongly Disagree	Count	1	0	1
	% within	100.0%	0.0%	100%
	% within Region	3.2%	0.0%	1.8%
Undecided	Count	3	2	5
	% within	60.0%	40.0%	100%
	% within Region	9.7%	8.0%	8.9%
Agree	Count	8	7	15
	% within	53.3%	46.7%	100%
	% within Region	25.8%	28.0%	26.8%
Strongly Agree	Count	19	16	35
	% within	54.3%	45.7%	100%
	% within Region	61.3%	64.0%	62.5%
Total	Count	31	25	56
	% within	55.4%	44.6%	100%
	% within Region	100.0%	100.0%	100%

Table 3: Fingerprints

From the findings of the total 56 respondents, 89.3% of the respondents agreed that fingerprints are unique, permanent, and easy to acquisition. 8.9% of the respondents were undecided, 1.8% of the respondents disagreed or strongly disagreed. The results from this study showed that the majority of the respondents admitted that fingerprints is a popular person identification. Fingerprint having been studied for long stand to be the best way authentication of voters can be achieved. The study has revealed that fingerprint biometric is unique and with the extensive study made on it has resulted in development of advanced devices to capture and make it easy to use.

4.2. A Multimodal System

The study sought to find out whether multimodal system is robust to fraudulent technologies and difficult to forge. The results are shown in Table 4.

multimodal system is robust to fraudulent technologies and difficult to forge		Region		Total
		Kakamega	Bungoma	
Disagree	Count	1	1	2
	% within Multimodal system is robust	50.0%	50.0%	100%
	% within Region	3.2%	4.0%	3.6%
Undecided	Count	2	1	3
	% within Multimodal system is robust	66.7%	33.3%	100%
	% within Region	6.5%	4.0%	5.4%
Agree	Count	10	9	19
	% within Multimodal system is robust	52.6%	47.4%	100%
	% within Region	32.3%	36.0%	33.9%
Strongly Agree	Count	18	14	32
	% within Multimodal system is robust	56.3%	43.8%	100%
	% within Region	58.1%	56.0%	57.1%
Total	Count	31	25	56
	% within Multimodal system is robust	55.4%	44.6%	100%
	% within Region	100.0%	100.0%	100%

Table 4: Multimodal System

From the findings majority of the respondents who stood at 91%, strongly agreed or agreed that multimodal system is robust to fraudulent technologies and difficult to forge. 5.4% of the respondents were undecided while 3.6% of the respondents disagreed. The combination of two or more biometric characteristics makes it more difficult for unauthorized user to access the E-voting system.

4.3. Biometric Tool

The study sought to find out if biometric is a powerful tool for use in identification and authentication. The results are shown in in Table 5.

Biometrics is a powerful tool for use in identification and authentication		Region		Total
		Kakamega	Bungoma	
Undecided	Count	3	1	4
	% within Biometrics is a powerful tool	75.0%	25.0%	100.0%
	% within Region	9.7%	4.0%	7.1%
Agree	Count	10	10	20
	% within Biometrics is a powerful tool	50.0%	50.0%	100.0%
	% within Region	32.3%	40.0%	35.7%
Strongly Agree	Count	18	14	32
	% within Biometrics is a powerful tool for	56.3%	43.8%	100.0%
	% within Region	58.1%	56.0%	57.1%
Total	Count	31	25	56
	% within Biometrics is a powerful tool	55.4%	44.6%	100.0%
	% within Region	100.0%	100.0%	100.0%

Table 5: Biometric Tool

The findings showed that of the total 56 respondents, 92.8% strongly agreed or agreed that biometric is a powerful tool for use in identification and authentication. 7.1% were undecided. While traditional security systems are reliant on passwords, personal identification numbers(PINs) or smart cards, you can achieve a high level of accuracy with biometrics systems. If the system is set up correctly, biological characteristics like fingerprints and iris scans can be used, which offer unique and accurate identification methods. These features cannot be easily duplicated, which means only the authorized person gets access and gives high level of security. Using biometric is considered to be a convenient security solution because they need not be remembered, or carry extra badges, documents, or ID cards.

4.4. Multi-Source Biometric System

The study sought to establish that multi-source biometric system increase the performance and enhance security as shown in Table 6.

Multi-source biometric systems increase the performance and enhance security		Region		Total
		Kakamega	Bungoma	
Strongly Disagree	Count	1	0	1
	% within Multi-source biometric systems	100.0%	0.0%	100.0%
	% within Region	3.2%	0.0%	1.8%
Undecided	Count	1	4	5
	% within Multi-source biometric systems	20.0%	80.0%	100.0%
	% within Region	3.2%	16.0%	8.9%
Agree	Count	14	5	19
	% within Multi-source biometric systems	73.7%	26.3%	100.0%
	% within Region	45.2%	20.0%	33.9%
Strongly Agree	Count	15	16	31
	% within Multi-source biometric systems	48.4%	51.6%	100.0%
	% within Region	48.4%	64.0%	55.4%
Total	Count	31	25	56
	% within Multi-source biometric systems	55.4%	44.6%	100.0%
	% within Region	100.0%	100.0%	100.0%

Table 4: Multi-Source Biometric System

From the findings out of the total 56 respondents 89.3% agreed or strongly agreed that multi-source biometric system increase the performance and enhance security. 1.8% strongly disagreed, 8.9% remain undecided. Multi-source biometric system uses information from two or more biometrics – (for example fingerprint and finger vein pattern; or fingerprint and iris or fingerprint and face) hence very accurate. There is increased and reliable recognition because multi-source biometric system permits a greater level of assurance for an accurate match in verification as well as identification.

4.5. Multiple Parameters for Secure authentication

The study sought to find out that secure authentication is provided by multiple parameters. The results are shown in Table 7

secure authentication is provided by multiple parameters		Region		Total
		Kakamega	Bungoma	
Disagree	Count	2	3	5
	% within Security	40.0%	60.0%	100.0%
	% within Region	6.5%	12.0%	8.9%
Undecided	Count	8	3	11
	% within Security	72.7%	27.3%	100.0%
	% within Region	25.8%	12.0%	19.6%
Agree	Count	11	9	20
	% within Security	55.0%	45.0%	100.0%
	% within Region	35.5%	36.0%	35.7%
Strongly Agree	Count	10	10	20
	% within Security	50.0%	50.0%	100.0%
	% within Region	32.3%	40.0%	35.7%
Total	Count	31	25	56
	% within Security	55.4%	44.6%	100.0%
	% within Region	100.0%	100.0%	100.0%

Table 7: Multiple Parameters for Secure authentication

From the findings out of the total 56 respondents, 71.4% strongly agreed or agreed that secure authentication is provided by multiple parameters. 19.6% remain undecided and 8.9%. The existing techniques of user authentication use IDs (identifiers), or identification cards and PINs (personal identification) which are not reliable.

4.6. Passwords, IDs and PINs for User Identification

The study sought to establish whether the use of either passwords or user IDs or identification cards and PINs are not reliable as shown in Table 8.

use of either passwords or user IDs or identification cards and PINs are not reliable		Region		Total
		Kakamega	Bungoma	
strongly Disagree	Count	0	4	4
	% within The existing techniques	0.0%	100.0%	100.0%
	% within Region	0.0%	16.0%	7.1%
Disagree	Count	0	2	2
	% within The existing techniques	0.0%	100.0%	100.0%
	% within Region	0.0%	8.0%	3.6%
Undecided	Count	4	4	8
	% within The existing techniques	50.0%	50.0%	100.0%
	% within Region	12.9%	16.0%	14.3%
Agree	Count	11	11	22
	% within The existing techniques	50.0%	50.0%	100.0%
	% within Region	35.5%	44.0%	39.3%
Strongly Agree	Count	16	4	20
	% within The existing techniques	80.0%	20.0%	100.0%
	% within Region	51.6%	16.0%	35.7%
Total	Count	31	25	56
	% within The existing techniques	55.4%	44.6%	100.0%
	% within Region	100.0%	100.0%	100.0%

Table 8: Passwords, IDs and PINs for User Identification

From the findings majority 75% of the respondents strongly agreed or agreed that the use of either passwords or user IDs or identification cards and PINs are not reliable. 14.3% of the respondents remain undecided, 10.7% of the respondents disagreed or strongly disagreed. Passwords and PINs can be acquired by wrong hands through covert observation. If the wrong person acquires the user ID and the password, then he/she will assume total access to the user's resources.

4.7. Pearson Correlation Coefficient

In statistics, Spearman's rank correlation coefficient or Spearman's rho or r_s is a nonparametric measure of rank correlation, statistical dependence between the rankings of two variables.(Crawshaw and Chambers, 2001,Norman and Martin, 2012).

Spearman's correlation coefficient varies from -1 to +1. The strength of the monotonic relationship is described by the absolute value of Spearman's Rank Order Correlation Coefficient (r_s). When the absolute value of r_s is closer to 0, the monotonic relationship between two variables becomes weaker (Liebetrau, 1976, Chen and Popovich, 2002). Spearman's rank correlation coefficient (rs) is fairly simple and reliable technique for testing both the strength and direction positive or negative for any correlation between two variables.

Table 9 presents Spearman's rank correlation coefficient values and its meaning

r_s Value	Meaning
$r_s = +1$	Means that the rankings have perfect positive association. Their rankings are exactly alike.
$r_s = 0$	Means that the rankings have no correlation or association.
$r_s = -1$	Means that the rankings have perfect negative association. They have exact reverse ranking to each other.

Table 9: Spearman's rank correlation coefficient values and its meaning

Source (adopted from Crawshaw and Chambers, 2001)

From Table 9 $r_s = +1$ means that the rankings are exactly alike, $r_s = 0$ means that the rankings have no association and $r_s = -1$ means that the rankings have exact reverse rankings to each other.

Table 10 shows the results of performing a Two-Tailed test of significance on six biometric properties for identification in a secure e-voting application.

Indicator	Measure	g1	g2	g3	g4	g5	g6
g1	Spearman's Correlation	1.000	.557**	.193	.364**	.455**	.211
	Significance	.	.000	.154	.006	.000	.119
g2	Spearman's Correlation	.557**	1.000	.201	.289*	.278*	.242
	Significance	.000	.	.138	.031	.038	.073
g3	Spearman's Correlation	.193	.201	1.000	.625**	.332*	.287*
	Significance	.154	.138	.	.000	.012	.032
g4	Spearman's Correlation	.364**	.289*	.625**	1.000	.488**	.407**
	Significance	.006	.031	.000	.	.000	.002
g5	Spearman's Correlation	.455**	.278*	.332*	.488**	1.000	.294*
	Significance	.000	.038	.012	.000	.	.028
g6	Spearman's Correlation	.211	.242	.287*	.407**	.294*	1.000
	Significance	.119	.073	.032	.002	.028	.
**. Correlation is significant at the 0.01 level (2-tailed).							
*. Correlation is significant at the 0.05 level (2-tailed).							

Table 10: Correlation between biometric properties for identification in a secure e-voting application

Key

g1. Fingerprints biometric

g2. Multimodal system

g3. Biometrics tool

g4. Multi-source biometric systems

g5. Multiple Parameters for Secure authentication

g6. Passwords, IDs and PINs for User Identification

Spearman rank-order correlations were conducted in order to determine if there were any relationships between:

a) The Fingerprints biometric correlated with five biometric technologies namely; Multimodal system, Biometrics tool, Multi-source biometric systems, Multiple Parameters for Secure authentication and Passwords, IDs and PINs for User Identification. A two-tailed test of significance indicated that there was a significant positive relationship between the Fingerprints biometric with Multimodal system rs(56) = .557, p < .05., Multi-source biometric systems rs(56) = .364, p< .05., Multiple Parameters for Secure authentication rs(56) = .455, p< .05. However, a similar two tailed test of significance indicated that the Fingerprints biometric was unrelated to Biometrics tool $r_s(56) = .193$, p > .05 and Passwords, IDs and PINs for User Identification rs(56) = .211, p > .05

b) Multimodal system correlated with five biometric technologies namely; Fingerprints biometric, Biometric tool, Multi-source biometric systems, Multiple Parameters for Secure authentication and Passwords, IDs and PINs for User Identification. A two-tailed test of significance indicated that the there was a significant positive relationship between the Multimodal system with Fingerprints biometric rs(56) = .557, p< .05., Wi-Fi Technology rs(56) = .476, p< .05., Multi-source biometric systems rs(56) = .289, p< .05., Multiple Parameters for Secure authentication rs(56) =.278, p < .05. However, a similar two tailed test of significance indicated that the Multimodal system was unrelated to Biometrics tool rs(56) = .201, p > .05 and Passwords, IDs and PINs for User Identification rs(56) = .242, p > .05. However, a similar two tailed test of significance indicated that the Multimodal system was unrelated to Biometrics tool rs(56) = .201, p > .05 and Passwords, IDs and PINs for User Identification rs(56) = .242, p > .05

c) The Biometric tool correlated with five biometric technologies namely; Fingerprints biometric, Multimodal system, Multi-source biometric systems, Multiple Parameters for Secure authentication and Passwords, IDs and PINs for User Identification. A two-tailed test of significance indicated there was a significant positive relationship between the Biometric tool with Multimodal system rs(56) = .577, p< .05., Multi-source biometric systems rs(56) = .625, p< .05.,Multiple Parameters for Secure authentication rs(56) = .323, p< .05., Passwords, IDs and PINs for User Identification rs(56) = .287, p < .05. However, a similar two tailed test of significance indicated that the Biometrics tool was unrelated to Multimodal system rs(56) = .201, p > .05 and Passwords, IDs and PINs for User Identification rs(56) = .242, p > .05

d) The Multi-source biometric systems correlated with five biometric technologies namely; Fingerprints biometric, Biometric tool, Multimodal system, Multiple Parameters for Secure authentication and Passwords, IDs and PINs for User Identification. A two-tailed test of significance indicated there was a significant positive relationship between the Multi-source biometric with Fingerprints biometric rs(56) = .364, p< .05., Multimodal system rs(56) = .289, p< .05., Biometrics tool rs(56) = .625, p< .05., Multiple Parameters for Secure authentication rs(56) = .488, p< .05., Passwords, IDs and PINs for User Identification rs(56) = .407, p < .05.

e) The Multiple Parameters for Secure authentication correlated with five biometric technologies namely; Fingerprints biometric, Biometric tool, Multimodal system, Multi-source biometric and Passwords, IDs and PINs for User Identification. A two-tailed test of significance indicated there was a significant positive relationship between the Multiple Parameters for Secure authentication with Fingerprints biometric rs(56) = .455, p< .05., Multimodal system rs(56) = .378, p< .05., Biometrics tool rs(56) = .332, p< .05., Multi-source biometric rs(56) = .488, p< .05., Passwords, IDs and PINs for User Identification rs(56) = .294, p < .05.

f) The Passwords, IDs and PINs for User Identification correlated with five biometric technologies namely; Fingerprints biometric, Biometric tool, Multimodal system, Multi-source biometric and Multiple Parameters for Secure authentication. A two-tailed test of significance indicated there was a significant positive relationship between the Passwords, IDs and PINs for User Identification with Biometrics tool rs(56) = .287, p< .05., Multi-source biometric rs(56) = .407, p< .05., Multiple Parameters for Secure authentication rs(56) = .294, p < .05.However, a similar two tailed test of significance indicated that the Passwords, IDs and PINs for User Identification was unrelated to Fingerprints biometric rs(56) = .211, p > .05 and Multimodal system rs(56) = .242, p > .05

5. Discussion

The main objective of this paper was to investigate biometric properties in real-world applications that can be used in an E-voting architecture. Fingerprints are unique, permanent, and easy to acquisition. The study has revealed that fingerprint biometric is unique and with the extensive study made on it has resulted in development of advanced devices to capture and make it easy to use as supported by 76.8% of the respondents.

Multimodal system is robust to fraudulent technologies and difficult to forge. The combination of two or more biometric characteristics makes it more difficult for unauthorized user to access the E-voting system as recommended by 91% of the respondents.

Biometric is a powerful tool for use in identification and authentication. If the system is set up correctly, biological characteristics like fingerprints and iris scans can be used, which offer unique and accurate identification methods. These features cannot be easily duplicated, which means only the authorized person gets access and gives high level of security. Using biometric is considered to be a convenient security solution because they need not be remembered, or carry extra badges, documents, or ID cards as recognized by 92.8% of the respondents.

Multi-source biometric systems increase the performance and enhance security. Multimodal biometrics uses information from two or more biometrics – (for example fingerprint and finger vein pattern; or fingerprint and iris or fingerprint and face) hence very accurate. There is increased and reliable recognition because multimodal biometric system permits a greater level of assurance for an accurate match in verification as well as identification as supported by 89.3% of the respondents.

Secure authentication is provided by multiple parameters. The existing techniques of user authentication use IDs (identifiers), or identification cards and PINs (personal identification) which are not reliable as maintained by 71.4% of the respondents.

The use of either passwords or user IDs or identification cards and PINs are not reliable. Passwords and PINs can be acquired by wrong hands through covert observation. If the wrong person acquires the user ID and the password, then he/she will assume total access to the user's resources as upheld by 75% of the respondents.

A two-tailed test of significance indicated that there was a significant positive relationship between the Fingerprints biometric with Multimodal system rs(56) = .557, p < .05., Multi-source biometric systems rs(56) = .364, p< .05., Secure environment rs(56) = .455, p< .05. However, a similar two tailed test of significance indicated that the Fingerprints biometric was unrelated to Biometrics tool rs(56) = .193, p > .05 and User authentication technique rs(56) = .211, p > .05.

This study shows that the biometric technologies considered in the study are really the main ways to be used in identification and authentication in an e-voting application.

6. Conclusion

This paper has presented biometric properties in real-world applications. The combination of two or more biometric characteristics makes it more difficult for unauthorized user to access the E-voting application. Biological characteristics like fingerprints and iris scans should be used, which offer unique and accurate identification methods. There is increased and reliable recognition because multimodal biometric system permits a greater level of assurance for an accurate match in verification as well as identification modes. The combination of two or more biometric characteristics makes it more difficult for unauthorized user to access the E-voting application. Passwords and PINs are not reliable because they can be acquired by wrong hands through covert observation. If the wrong person acquires the user ID and the password, then he/she will assume total access to the user's resources

7. Recommendation

Future research should focus on how to improve biometric capturing machines to be able to capture multiple biometric sources at once, for example capture fingerprints and face portrait. Research should be conducted to address the issue of biometric systems accuracy to correctly match the information.

8. References

i. Abdalla, A. & Samani. T. (2013). The Technical Feasibility and Security of E-Voting. The International Arab Journal of Information Technology, Vol. 10, No. 4, July 2013.
ii. Aruna, P., Kumari & Jaya, G. S.(2014). A novel multimodal biometric scheme for Personal authentication. Impact: International Journal of Research in Engineering & Technology (IMPACT: IJRET) ISSN (E): 2321-8843; ISSN (P): 2347-4599 Vol. 2, Issue 2, Feb 2014, 55-66.
iii. Biometric Technology Case Studies of Vertical Markets, (2007). Available at [http://www.m2sys.com/biometric-fingerprint-software-case-studies-nigerian-voter-registration/] retrieved on 28/03/2017
iv. Buchsbaum, T. (2004). E-voting. "International developments and lessons learnt. Proceedings of Electronic Voting in Europe Technology, Law, Politics and Society. Lecture Notes in Informatics. Workshop of the ESF TED Programme together with GI and OCG.
v. Burns, S.N. & Grove, S.K. (2003). Understanding nursing research. 3rd ed. Saunders. Philadelphia
vi. Chen, P. and Popovich, P., (2002) Correlation: Parametric and Nonparametric Measures. Thousand Oaks, CA: Sage Publications, Inc.; 2002.
vii. Dileep, K. & Yeonseung, R. (2009). A Brief Introduction of Biometric and Fingerprint Payment Technology. International Journal of Advanced Science and Technology Vol. 4, March, 2009.
viii. Ghana uses biometric voter verification for third election running, (2016). Available at {https://www.genkey.com/news/ghana-uses-biometric-voter-verification-for-third-election-running/} retieved on 28/03/2017
ix. Hazzaa, F. & Kadry, S. (2012). New System of E-voting Using Fingerprint. International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 10, October 2012
x. Iritech, Inc, (2016). Multimodal Biometrics for Airport Security on the Rise Available at [http://www.iritech.com/blog/multimodal-biometrics-airport/] retrieved on 29/3/2017
xi. Kumari, P.A. & Jaya, G.S. (2014). A novel multimodal biometric scheme for personal Authentication. International Journal of Research in Engineering & Technology (IMPACT: IJRET) ISSN (E): 2321-8843; ISSN (P): 2347-4599 Vol. 2, Issue 2, Feb 2014, 55-66.
xii. Liebetrau, A., (1976).Measures of Association. Beverly Hills and London: Sage Publications, Inc.; 1976.
xiii. Nathaniel K. (2015). Biometrics the Future of Mobile Payments U.S. Economic Watch 20 July 2015 BBVA Research
xiv. Navneet, S. & Vijay, S. R. (2012). Role of Biometric Technology over Advanced Security and Protection in Auto Teller Machine Transaction. International Journal of Engineering and Advanced Technology (IJEAT).
xv. Norman, F. and Martin, N. R., (2012). Assessment and Decision Analysis with BayesianNetworks CRC Press, 2012
xvi. Olaniyi, O.M., Adewumi, D.O. & Arulogun, O. T. (2011). Framework for Multilingual Mobile E-voting Service Infrastructure. African Journal of Computing & ICT Vol 4. No. 3. Issue 2.
xvii. Ratha, N. K., Connell, J. H. & Bolle, R. M. (2001). Enhancing Security and Privacy in Biometric-based Authentication systems. IBM Systems Journal, Vol. 40, No 3, 2001.
xviii. Rawlson O, K., (2015). Biometrics and Healthcare Biometrics research group, inc. Available at { http://www.biometricupdate.com/wp-content/uploads/2015/02/biometric- in Healthcare.pdf } retrieved on 28/03/2017
xix. Riera, A., & Brown, P. (2003). Bringing Confidence to Electronic Voting. Electronic Journal of e-Government Volume 1 Issue 1, 2003, (14-21).
xx. Sanjekar, P.S. &. Patil, J.B. (2014). An Overview of Multimodal Biometric Signal &Image Processing. An International Journal (SIPIJ) Vol.4, No.1, February 2013.
xxi. Tripathi, K. P. (2011). A Comparative Study of Biometric Technologies with Reference to Human Interface. International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011.Use of biometrics in Canada, (2015). Available at [http://www.cic.gc.ca/english/department/biometrics-use.asp] retrieved on 28/03/2016
xxii. Yong, W.J.and Byung, H.L., (2013). The Implementation of Secure Mobile Biometric System. International Journal of Bio-Science and Bio-TechnologyVol. 5, No. 4, August, 2013.).