International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 108 - 119, 2015, ISSN:- 2319–8656

A Study of Approaches and Measures aimed at Securing Biometric Fingerprint Templates in Verification and Identification Systems

Joseph Mwema
SCIT
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Stephen Kimani
SCIT
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Michael Kimwele
SCIT
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Abstract: The need for fool proof authentication procedures away from traditional authentication mechanisms like passwords, security PINS has led to the advent of biometric authentication in information systems. Biometric data extracted from physiological features of a person including but not limited to fingerprints, palm prints, face or retina for purpose of verification & identification is saved as biometric templates. The inception of biometrics in access control systems has not been without its own hitches & like other systems it has its fair share of challenges. Biometric fingerprints being the most mature of all biometric spheres are the most widely adopted biometric authentication systems. Biometric systems effectiveness lies on how secure they are at preventing inadvertent disclosure of biometric templates in an information system's archive. This however has not been the case as biometric templates have been fraudulently accessed to gain unauthorized access in identification and verification systems. In order to achieve strong and secure biometric systems, biometric systems developers need to build biometric systems that properly secure biometric templates. Several biometric template protection schemes and approaches have been proposed and used to safeguard stored biometric templates. Despite there being various biometric template protection schemes and approaches in existence, none of them has provided the most authentic, reliable, efficient and deterrent means to totally secure biometric fingerprint templates. This research sought to establish status of the current biometric template protection techniques and methods by conducting a survey and analyzing data gathered from a sample of seventy-eight (78) respondents. We will report these results and give our conclusion based on findings of the survey in this paper.

Keywords: Biometrics; Fingerprints; Templates; Security; Encryption; Unimodal Biometric Systems

1. INTRODUCTION

The advent of increased security threats in information systems and need to guarantee unbeatable systems security has enticed system designers & developers to incorporate use of passwords, PINs and access codes for system users' authorization. Unfortunately these have not provided the most needed security and have been hacked or obtained illegally as emphasized by [1].System designers & developers went further and considered use of biometrics in design of systems' verification and identification procedures. Tan in [2] showed that use of biometric authentication schemes is more efficient over traditional password based access control methods. Statistics however show that biometric systems have not been known to be impervious to hacks and there are several known possible attacks on biometric systems which have rendered them insufficient in providing water tight security as is evidenced by [3].

Biometrics is the automatic identification of a person's physiological or behavioral patterns or traits. Biometric patterns captured from a person are saved as biometric templates. Ahmad et al [4] caution that 'security of biometric templates in a biometric system' as one of the technical issues and challenges regarding use of biometric systems.

This research will study schemes and approaches aimed at securing biometric fingerprint templates in biometric authentication systems, report data results and findings from respondents who were surveyed from a selected sample of seventy-eight (78) respondents picked from a study population of biometric system developers.

The objectives of this research work are:

- To review existing biometric fingerprint template protection schemes and approaches.
- To determine strengths and drawbacks of existing biometric fingerprint template protection methods.
- To identify what are the best practices for securing fingerprint templates in unimodal biometric systems.
- To establish what features would an ideal unimodal biometric fingerprint template protection scheme have.

2. EXISTING BIOMETRIC TEMPLATE PROTECTION SCHEMES & APPROACHES

Jain et al in [15] categorized biometric template protection schemes into *Feature Transformation* and *Biometric Encryption.* The existing biometric template protection schemes and approaches currently in use usually fall into these two categories. We discuss Bio-hashing, Cancellable biometrics, Fuzzy vault, Fuzzy commitment and Watermarking.

2.1 Bio-Hashing

Bio-hashing is a biometric template protection approach in which features from a biometric template are transformed using a transformation function defined by a password or a key known only to the user [5]. This key or password needs to

be securely stored and remembered by the user for subsequent authentication. The key or password used by user in bio-hashing increases entropy of biometric template which further deters adversary attacks. Direct mixing of pseudo-random number (which is kept secret) and biometric data is used to compute a binarized key of 80-bits key with a 0.93% false rejection rate of the system [6]. This generated physical token can be used in smartcard or USB tokens as shown by [5] thus fostering more security than passwords or PINs where controlled levels of access are required.

2.2 Cancellable biometrics

Unlike passwords, PINs and access codes, biometric templates can never be replaced with newer ones if compromised. To circumvent this challenge cancellable biometrics was introduced where biometric templates can be cancelled and replaced [7]. Cancellable biometrics scheme is an intentional and systematic repeatable distortion of biometric template data with the purpose of protecting it under transformational-based biometric template protection. In the concept of cancellable transformation, a transformed template can be cancelled and re-issued by changing transformation parameters if misplaced [8].

2.3 Fuzzy vault

Fuzzy vault is a cryptographic construct that was first proposed by Jules and Sudan in [9] where secret information is encrypted and decrypted securely using a fuzzy unordered set of genuine points and haff points. Geetika & Kaur described a biometric fuzzy vault as a biometric cryptosystem used for protecting private keys and releasing them only when the legitimate users enter their biometric data [10] while Deshpande & Joshi defined a fuzzy vault as a scheme utilized for secure binding of randomly generated key with extracted biometric features [11].

2.4 Fuzzy commitment

Fuzzy Commitment is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector [12]. Jeny & Jangid further described a fuzzy commitment scheme as one where a uniformly random key of length 1 bits is generated and used to exclusively index an n-bit codeword of suitable error correcting code where the sketch extracted from the biometric template is stored in a database.

2.5 Watermarking

The aim of watermarking is to use biometric fingerprint templates as a 'message' to be embedded in a robust watermarking application like copyright protection in order to enable biometric recognition after the extraction of the watermark. In a biometric watermarking scheme, if an attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden as evidenced in [13].

3. RESEARCH METHODOLOGY

3.1 Research Design

This research adopted survey research design because it is extensive thus ensuring we could get an accurate sample from the target population in which to gather targeted results and be able to draw conclusions and findings. Survey research is flexible for online surveys as well as for collecting data for later analysis. The study largely employed Quantitative research approach to compute results and Qualitative research approach where descriptive and broad understanding was required in questions asked to respondents.

3.2 Study Population

The target population in this research constituted of all biometric software developers who currently are in the roles of developing biometric software systems or integrating biometrics into information systems and persons who work or have worked as biometric systems developers in biometric projects in Kenya. We used LinkedIn the social networking site for professionals to draw our target study population.

3.3 Sampling Technique and Sample Size

This research employed simple random sampling. We chose to use this method over other random sampling methods because it provisioned for an equal likelihood of a biometric software developer from the study population being included. Individuals have the same probability of being chosen at any stage in a simple random sampling process as evidenced by [14]. We chose a sample size of seventy-eight (78) biometric systems developers as respondents from the target population.

3.4 Research Instrument and Data Analysis Tools

Online Questionnaires were selected because they enabled us to collect standardized data from biometric systems developers in LinkedIn. Questionnaires gather data that is ready for later statistical analysis of responses. Questionnaires were tailored to capture data pertinent to the research's objective and research questions. This study used Statistical Package for Social Sciences (SPSS) software for data analysis and interpretation.

4. DATA ANALYSIS AND DISCUSSION

Questions in the Questionnaires were open ended and closed ended. Closed ended questions were comprehensive and equally exclusive to avoid ambiguity of collected data in scenarios of non-conforming select options of the questions presented to respondents. Questionnaire used in the study comprised of these (4) sections: Biometric System Developer's Background, Biometric Templates Security, Efficiency of Encryption Methods and Biometric Templates Security Challenges.

4.1 Biometric System Developers' Background

Biometric system developers' particulars and relevant data based on their experience with biometrics systems were captured in this section. These details included age, years of experience as biometric systems developers, type of biometric systems developed, if they had undertaken studies in biometric systems development, knowledge in data encryption and what their thoughts were on impediments preventing wide scale adoption of biometrics.

4.1.1 Respondents' Age

Data collected had the following statistics for ages of the respondents. The age 20 years and below had 0(0%) entries, 3(3.8%) of the respondents were between *21-25* years, The age 26-30 years had 27(34.6%) respondents. 21 (26.9%) respondents were in the age bracket 31-35 years and 27 (34.6%) were of age 35 years and above. This data is shown in Table 1 below.

Table 1. Statistics of Respondents Age

Age of respondents in years	No. of Respondents	No. of Respondents in percentage (%)
21 - 25	3	3.8%
26 - 30	27	34.6%
31 - 35	21	26.9%
35 and above	27	34.6%
Total	**78**	**100.0%**

4.1.2 Respondents' Experience as Biometric Systems Developers

From the data collected, 52 (66.7%) of the respondents had 1-5 years of experience as biometric systems developers, 19 (24.4%) had experience of 6-10 years. While only 5 (6.4%) respondents had 11-15 years of experience, only 2 (2.6%) had an experience of 16 years and above. This data is shown in details in Table 2.

Table 2. Statistics of Respondents Experience as Biometric Systems Developers

Experience in years as a Biometric Systems Developer	No. of Respondents	No of respondents in percentage (%)
1 - 5 years	52	66.7%
6 - 10 years	19	24.4%
11 - 15 years	5	6.4%
16 years and above	2	2.6%
Total	**78**	**100.0%**

4.1.3 Type of Biometric Systems Developed

Data collected indicated 64(82.1%) of respondents had experience developing *fingerprint systems*, 43(55.1%) had developed *face recognition systems* while 16 (20.5%) had been developing *iris systems*. A further 14 (17.9%) had experience in developing *voice recognition systems* and 7 (9.0%) had been developing palm *vein recognition systems*. 12 (15.4%) of respondents had experience developing other biometric systems which included *online signature*, *finger vein* and *score level fusion of face and fingerprints*. This data is shown in Table 3 and Table 4.

Data results showing where respondents develop more than one type of biometric system is shown in Table 4. From the data results in Table 4, the most developed biometric systems by the sampled respondents are fingerprints & face biometric systems being developed by 32(41.0%) of the sampled respondents.

Table 4. Statistics of Type of Biometric Systems Developed

Type of Biometric Systems Developed	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Fingerprint	64	78	82.1%
Face	43	78	55.1%
Iris	16	78	20.5%
Voice	14	78	17.9%
Palm Vein Recognition	7	78	9.0%
Other(s)	12	78	15.4%
Total		**78**	**100.0%**

4.1.4 Respondents who have studied about Biometric Systems Development

Data collected revealed that 46 (59.0%) of respondents had undertaken studies or a course in biometric systems development while 32(41.0%) were active biometric systems developers without having had any particular training in the field. These statistics were tabulated in Table 5.

Table 5. Statistics of Respondents who have studied Biometric Systems Development

Studied Biometric Systems Development	No. of Respondents	No of respondents in percentage (%)
Yes	46	59.0%
No	32	41.0%
Total	**78**	**100.0%**

Table 3. Statistics of Respondents who Develop One or More Biometric Systems

Biometric Systems Developed by Respondents	No. of Respondents	No. of respondents in percentage (%)
Face	3	3.8%
Face, Iris	4	5.1%
Face, Palm Vein Recognition	1	1.3%
Face, Score level fusion of face and fingerprint	1	1.3%
Face, Voice	1	1.3%
Fingerprints	4	5.1%
Fingerprints, Face	32	41.0%
Fingerprints, Face, Iris, Palm Vein Recognition	1	1.3%
Fingerprints, Finger vein	1	1.3%
Fingerprints, Iris	10	12.8%
Fingerprints, Palm Vein Recognition	6	7.7%
Fingerprints, Voice	10	12.8%
Iris	1	1.3%
Iris, Voice	1	1.3%
Voice	1	1.3%
Voice, online signature	1	1.3%
Total	**78**	**100.0%**

4.1.5 Respondents' Experience in Data Encryption

Respondents' knowledge in data encryption was captured during data collection to determine their level of expertise in securing data with encryption & prevent adversary attacks on archived data.

Table 6. Statistics of Respondents Knowledge in Data Encryption

Respondents Knowledge in Data Encryption	Score Level Weights	No. of Respondents	No. of Respondents in Percentage (%)
Excellent	5	14	17.9%
Above Average	4	31	39.7%
Average	3	28	35.9%
Poor	2	5	6.4%
Very Poor	1	0	0.0%
	Mean=3.63	**Total =78**	**Total =100.0%**

Respondents' knowledge in data encryption as shown above in Table 6. illustrated that 14(17.9%) of respondents considered there knowledge in data encryption as *excellent*, 31(39.7%) respondents ranked *above average* while 28(35.9%) respondents data encryption knowledge was ranked as *poor*. None of the respondents in the data collected thought their data encryption skills fared *very poorly*. The overall mean for the rankings of respondents' data encryption knowledge was 3.63 which is slightly more than average tending to above average and a good pointer that biometric developers are keen on security of data.

4.1.6 Impediments towards wide scale adoption of Biometric Systems

From data collected, impediments preventing wide scale adoption of biometric systems, *high costs of biometric hardware & software* was the main reason identified by respondents at 53(67.9%) followed by 41(52.6%) of respondents who cited *lack of expertise to develop, implement & support biometric systems*. 31(39.7%) of respondents were of the opinion that *accuracy of biometric identification systems* was a contributing factor while *big data size of biometric templates* and *known security flaws* were singled out by 15(19.2%) and 10(12.8%) of respondents respectively. Other impeding factors identified by the remainder of 18 (23.1%) of respondents were *verification & identification time, low bandwidth because of the big size of biometric data, users' unwillingness to give out their biometric data alluding security concerns and trust*. This data is presented in Table 7.

Table 7. Statistics of Impediments that delay wide scale adoption of Biometric Systems

Impediments Towards Wide Scale Adoption of Biometric Systems	No. of Respondents	Total No. of Respondents	No. of Respondents in Percentage (%)
High Costs of Biometric Hardware & Software	53	78	67.9%
Known Security Flaws	10	78	12.8%
Lack of Expertise to Develop, Implement & Support Biometrics Systems	41	78	52.6%
Accuracy (False Acceptance Rate and False Rejection Rate)	31	78	39.7%
Big data size of Biometric Templates in storage space	15	78	19.2%
Other(s)	18	78	23.1%
Total		**78**	**100.0%**

4.2 Biometric Templates Security

This section sought to discover preferred area of storage for biometric templates, determine whether there are measures to protect biometric templates, ascertain if there are policies in place that emphasize on securing of biometric templates in storage, then identify which biometric template protection techniques & methods are used and finally find out from respondents which biometric encryption schemes they used.

4.2.1 Biometric Templates Storage Space

Identifying the preferred storage space for biometric templates among the respondents was of importance to us so that we could identify which parts of biometric template storage space are likely to be attacked by hackers and this study sought to determine the storage space used by respondents to save biometric templates in biometric systems. Table 8 below shows results from study as follows; 55(70.5%) of respondents saved their biometric templates in *databases* while only 1(1.3%) of respondents saved biometric templates in *USB modules*. 7(9.0%) of respondents chose *folders* and 10(12.8%) of respondents preferred *smart cards*. The remainder 5(6.4%) of respondents who identified *other* places listed the following storage places; *encrypted databases* and *a combination of both databases and smartcards*.

Table 8. Statistics of where Respondents save Biometric Templates

Biometric Templates Storage Space	No. of Respondents	No. of Respondents Percentage (%)
Folders	7	9.0%
Databases	55	70.5%
Smart cards	10	12.8%
USB Modules	1	1.3%
Other(s)	5	6.4%
Total	**78**	**100.0%**

4.2.2 Respondents who have measures in place aimed at Protecting Biometric Templates

We sought to determine if there were any measures aimed at protecting biometric templates from the sampled respondents and this study showed that 66(84.6%) of respondents had measures in place while 12(15.4%) of respondents did not. These results are shown in Table 9.

Table 9. Statistics to show if Respondents have any Measures in place to Protect Biometric Templates

Are there Measures in place to Protect Biometric Templates	No. of Respondents	No. of Respondents Percentage (%)
Yes	66	84.6%
No	12	15.4%
Total	**78**	**100.0%**

4.2.3 Policies aimed at Protecting Biometric Templates in Storage

To further investigate the magnitude with which security of biometric templates is put into consideration we inquired from the respondents whether there were any policies in their organizations governing security of biometric templates. The results presented in Table 10 showed that 61(78.2%) of respondents had policies in place while 17(21.8%) of respondents admitted that they did not have any governing policies in place.

Table 10. Statistics showing if there are Biometric Templates Security Policies

Are there Biometric Templates Security Policies	Respondents	No. of Respondents Percentage (%)
Yes	61	78.2%
No	17	21.8%
Total	**78**	**100.0%**

Observing that 17(21.8%) of respondents in Table 3.2.3. did not have policies to mitigate biometric templates attacks, asked what measures they had in place to mitigate Biometric template attacks in storage. We established that the following practices were used; *matching live finger again, file access permissions were established in Linux, cryptologic tools, servers without external access were used, databases were password protected and database access permissions were regulated or denied*.

4.2.4 Biometric Templates Protection Techniques

We narrowed further down from determining whether there were measures and policies in place targeted at protecting biometric templates to ascertaining which template protection techniques respondents used. It was established that 39(50%) of respondents used *Biometric Encryption Technique* to secure biometric templates while 16(20.5%) of respondents made use of *Feature Transformation Technique*. 23(29.5%) of respondents did not use any biometric template protection techniques leaving them exposed to experiencing biometric template attacks in their biometric systems. These statistics were presented in Table 11.

Table 11. Statistics for Biometric Templates Protection Techniques Used

Biometric Template Protection Technique	No. of Respondents	No. of Respondents Percentage (%)
Feature Transformation	16	20.5%
Biometric Encryption	39	50.0%
None	23	29.5%
Total	**78**	**100.0%**

4.2.5 Biometric Encryption Technique & Biometric Encryption Schemes

From Table 12, it was established that the majority of respondents 39(50.0%) had indicated that they used *Biometric Encryption* technique. we determined from the study that of the two methods *Key Binding* and *Key Generation* found in *Biometric Encryption* Technique that 16(20.5%) of respondents used Key Binding while 23(29.5%) used Key Generation. From these results also presented in Table 12 it is evident that *Key Generation* method is the most preferred *Biometric Encryption* method than *Key Binding* because there is more security with generating encryption keys than binding encryption keys while securing data.

Table 12. Statistics for Biometric Encryption Methods Used

Biometric Encryption Methods	No. of Respondents	No. of Respondents Percentage (%)
Key Binding	16	20.5%
Key Generation	23	29.5%
None	39	50.0%
Total	**78**	**100.0%**

The current biometric encryption schemes used to protect biometric templates were explored. It was required for respondents to identify the schemes they used to protect biometric templates. From the data collected and tabulated in Table 13 it was shown that 10(12.8%) of respondents had used *Fuzzy Vault*, 6(7.7%) of respondents had used *Water Marking*, 40(51.3%) had used *RSA & ECC* and 9(11.5%) indicated they had used *Fuzzy Commitment* and 12(15.4%) specified they had used *Cancellable Biometrics*. 22(28.2%) of respondents indicated that they did not use any *biometric encryption schemes* while 4(5.1%) of respondents indicated that they used other biometric encryption schemes. The *other* schemes specified by respondents included *private encryptions*, *AES 128b*. The results of the *Biometric Encryption Schemes* used by respondents are shown in Table 13.

Table 13. Statistics of Biometric Encryption Schemes used Under Key Generation Method

Biometric Encryption Schemes	No. of Respondents	Total No. of Respondents	No of respondents in percentage (%)
Fuzzy Vault	10	78	12.8%
Water Marking	6	78	7.7%
RSA and ECC	40	78	51.3%
Fuzzy Commitment	9	78	11.5%
Cancellable Biometrics	12	78	15.4%
None	22	78	28.2%
Other(s)	4	78	5.1%
Total		**78**	**100.0%**

4.3 Efficiency of Encryption Methods

This section was significant in reviewing efficiency of biometric encryption methods used to protect biometric fingerprint templates. It consisted of the following subsections; Views of respondents on efficiency of encryption methods they used, Encryption keys and biometric templates storage space, Practices improving biometric encryption, Encrypting data with biometric encryption keys derived from fingerprint templates, Biometric encryption keys' entropy strength, Biometric encryption keys future use in data encryption.

4.3.1 Respondents' views on Efficiency of Encryption Methods They Use

The scales were equated with values shown in brackets next to them as follows for easier analysis and interpretation of data;

Strongly Disagree(1), Disagree(2), Neutral(3), Agree(4) and Strongly Agree(5).

This section was a basis for determining from respondents if there were risks of hacking biometric encryption methods used to secure biometric templates. We established that 10(12.8%) of respondents *Strongly Disagreed*, 31(39.7%) of respondents *Disagreed*, 22(28.2%) of respondents *Agreed* while 5(6.4%) *Strongly Agreed* and 10(12.8%) neither agreed nor disagreed to any extent and were categorized as *Neutral*. These results were presented in Table 14 below.

Table 14. Statistics showing if there is Risk of Hacking Biometric Encryption Method Used

There is Risk of Hacking Biometric Systems in the Encryption Method Used	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	10	12.8%
Disagree	31	39.7%
Neutral	10	12.8%
Agree	22	28.2%
Strongly Agree	5	6.4%
Total	**78**	**100.0%**

This section was a basis for determining from respondents if encryption methods used to secure biometric templates were considered fool proof. We established that 7(9.0%) of respondents *Strongly Disagreed*, 19(24.4%) of respondents *Disagreed*, 19(24.4%) of respondents *Agreed* while 9(11.5%) *Strongly Agreed* and 24(30.8%) neither agreed nor disagreed to any extent and were categorized as Neutral. These results were presented in Table 15.

Table 15. Statistics showing if Encryption Methods used by Respondent are Fool Proof

The Encryption Methods Used by Respondent are Fool Proof	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	7	9.0%
Disagree	19	24.4%
Neutral	24	30.8%
Agree	19	24.4%
Strongly Agree	9	11.5%
Total	**78**	**100.0%**

This section was a basis for determining from respondents if encryption methods used were satisfactory in securing biometric data. We established that 5(6.4%) of respondents *Strongly Disagreed*, 15(19.2%) of respondents *Disagreed*, 31(39.7%) of respondents *Agreed* while 12(15.4%) *Strongly Agreed* and 15(19.2%) neither agreed nor disagreed to any extent and were categorized as Neutral. These results were presented in Table 16.

Table 16. Statistics of Respondents whose Biometric Encryption Method is satisfactory

Biometric Template Encryption Method used is Satisfactory	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	5	6.4%
Disagree	15	19.2%
Neutral	15	19.2%
Agree	31	39.7%
Strongly Agree	12	15.4%
Total	**78**	**100.0%**

The mode for *if there is risk of hacking biometric systems in Encryption Method used* is **2** whose equivalent is *Disagree*. The greater percentage of respondents Disagreed *that there is risk of hacking biometric systems based on the Encryption Method they used* implying that they believed their biometric encryption method was not so exposed to the risk of hacking.

The mode for *if biometric encryption methods are fool proof* is **3** whose equivalent is *Neutral*. The greater percentage of respondents were not sure whether *biometric encryption methods they used are fool proof* implying that they do not really doubt or consider them to be insecure.

The mode for *if biometric template security is satisfactory in Encryption Method used is* **4** whose equivalent is *Agree*. The greater percentage of respondents agreed that biometric template security is satisfactory based on the Encryption Method they used implying that they believed the biometric encryption method they used provided satisfactory security on biometric templates of the biometric systems they developed. *Spearman's rho* was used to find *correlations* between *encryption methods efficiencies*.

Table 17. Correlations of Encryption Methods based on their Efficiencies

			If there is risk of hacking biometric systems in Encryption Method Used	If biometric encryption methods are fool proof	If biometric template security is satisfactory in Encryption Method Used
Spearman's rho	If there is risk of hacking biometric systems in Encryption Method Used	Correlation Coefficient	1.000	-.223	-.376**
		Sig. (2-tailed)	.	.050	.001
		N	78	78	78
	If biometric encryption methods are fool proof	Correlation Coefficient	-.223	1.000	.322**
		Sig. (2-tailed)	.050	.	.004
		N	78	78	78
	If biometric template security is satisfactory in Encryption Method Used	Correlation Coefficient	-.376**	.322**	1.000
		Sig. (2-tailed)	.001	.004	.
		N	78	78	78

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

The correlations presented in Table 17, are described as follows;

There is a moderate **negative** Correlation of **-0.376** with a **p** value of **0.001** between *if there is risk of hacking biometric systems in Encryption Method used* and *if biometric template security is satisfactory in Encryption Method used* implying that if the risk of hacking biometric systems based on biometric encryption method used *increases* then the encryption method's efficiency *reduces* and is not satisfactory.

There is a moderate **positive** Correlation of **0.322** with a **p** value of **0.001** between *if biometric encryption methods are fool proof* and *if biometric template security is satisfactory in Encryption Method used* implying that if biometric encryption method *excels* in being fool proof then the encryption method's efficiency *increases* and is considered satisfactory.

Table 18 gives results for Mean, Median and Mode of *Efficiency of Encryption Methods used*.

Table 18. Mean, Median and Mode of Efficiency of Encryption Methods

	If there is risk of hacking biometric systems in Encryption Method Used	If biometric encryption methods are fool proof	If biometric template security is satisfactory systems in Encryption Method Used
N	78	78	78
Mean	2.76	3.05	3.38
Median	2.00	3.00	4.00
Mode	2 (Disagree)	3 (Neutral)	4 (Agree)

4.3.2 Encryption Keys & Encrypted Biometric Templates Storage Space

We observed that 65(83.3%) of respondents would not want to keep encryption keys in the same storage space with Encrypted Biometric Templates. 13(16.7%) of respondents would on the contrary keep encryption keys together with encrypted biometric templates in the same storage space. The tabulated results are shown in Table 19. The objective of a biometric system developer would be to make it hard for an adversary to decode biometric data in a biometric system by keeping biometric encryption keys in a different location away from encrypted biometric data.

Table 19. Statistics of Respondents who would keep Encryption Keys in the same storage space with Encrypted Biometric Templates

Would keep Encryption Keys in same storage space with Encrypted Biometric Templates	No. of Respondents	No. of Respondents Percentage (%)
Yes	13	16.7%
No	65	83.3%
Total	**78**	**100.0%**

4.3.3 Practices Improving Biometric Encryption

Respondents identified various practices they deemed would improve biometric encryption as follows; 52(66.7%) of respondents believed *Improving Accuracy and Security of Biometric Encryption Algorithms* would help. *Use of Multimodal Biometrics* came in second having been identified by 38(48.7%) of respondents. 36(46.2%) of respondents would rather *Improve Image Acquisition Process* while 31(39.7%) and 24(30.8%) of respondents would *Make Biometric Encryption Resilient against attacks* and *Develop Biometric Encryption Applications* respectively. The Other 3(3.8%) of respondents listed *speeding of biometric identification & verification* and *performing liveliness detection* as other practices that would improve biometric encryption. These results are tabulated in Table 20 and Table 21 below.

Table 20. Statistics of Practices Biometric Encryption

Practices Improving Biometric Encryption	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Improving Image Acquisition Process	36	78	46.2%
Making Biometric Encryption Resilient against attacks	31	78	39.7%
Improving Accuracy and Security of Biometric Encryption Algorithms	52	78	66.7%
Use of Multimodal Biometrics	38	78	48.7%
Develop Biometric Encryption Applications	24	78	30.8%
Other(s)	3	78	3.8%
Total		**78**	**100.0%**

Table 21. Statistics of Combination of Practices Improving Biometric Encryption

Combination of Best Practices Improving Biometric Encryption	No. of Respondents	No of Respondents in percentage (%)
Encryption Apps	2	2.6%
Accuracy & Security	5	6.4%
Accuracy & Security, Encryption Apps	3	3.8%
Accuracy & Security, Multimodal	8	10.3%
Image Acquisition	3	3.8%
Image Acquisition, Encryption Apps	1	1.3%
Image Acquisition, Accuracy & Security	8	10.3%
Image Acquisition, Accuracy & Security, Encryption Apps	1	1.3%
Image Acquisition, Accuracy & Security, Multimodal	2	2.6%
Image Acquisition, Accuracy & Security, Multimodal, Encryption Apps	1	1.3%
Image Acquisition, Resilient to Attacks	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Encryption Apps	1	1.3%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Multimodal	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Multimodal, Encryption Apps	6	7.7%
Image Acquisition, Resilient to Attacks, Multimodal	1	1.3%
Image Acquisition, Multimodal	5	6.4%
Image Acquisition, Multimodal, Encryption Apps	1	1.3%
Resilient to Attacks	2	2.6%
Resilient to Attacks, Encryption Apps	2	2.6%
Resilient to Attacks, Accuracy & Security	5	6.4%
Resilient to Attacks, Accuracy & Security, Encryption Apps	2	2.6%
Resilient to Attacks, Accuracy & Security, Multimodal	4	5.1%
Resilient to Attacks, Accuracy & Security, Multimodal, Encryption Apps	2	2.6%
Multimodal	4	5.1%
Multimodal, Encryption Apps	2	2.6%
Other(s)	3	3.8%
Total	**78**	**100.0%**

Key for Table 21:

Image Acquisition : Improving Image Acquisition Process
Multimodal : Use of Multimodal Biometrics
Resilient to Attacks : Making Biometric Encryption Resilient against attacks
Encryption Apps : Develop Biometric Encryption Applications
Accuracy & Security : Improving Accuracy and Security of Biometric Encryption Algorithms
Other(s) : Other(s)

4.3.4 Encrypt Data with Biometric Encryption Keys Derived From Fingerprint Templates

We also wanted to know whether respondents considered *encryption of data using encryption keys derived from biometric fingerprint templates* a feasible idea. The results shown in Table 22 revealed that 48(61.5%) of respondents believed it would be achievable while 30(38.5%) declined. These results proved that if respondents had a way to derive biometric encryption keys from fingerprints they would use this approach.

Table 22. Statistics of Respondents who believed Encryption Keys Derived from Fingerprint templates could be used to protect data in storage

Encrypted Biometric Templates and Biometric Encryption Keys in same Storage Space	No. of Respondents	No. of Respondents Percentage (%)
Yes	48	61.5%
No	30	38.5%
Total	**78**	**100.0%**

4.3.5 Biometric Encryption Keys Entropy Strength

To understand entropy strengths associated with biometric keys we sought to establish whether respondents believed encryption keys derived from biometric templates would be rich in entropy for encrypting data than a combination of passwords and access codes. The study revealed that 72(92.3%) of respondents thought encryption keys derived from biometrics would provide rich entropy than passwords and access codes. 6(7.7%) of respondents were not convinced and when asked why they explained that *there would be overlaps in combination of keys from biometric templates if there are more people* and *strength of security keys is depended on quality of biometric templates implying poor samples would result in lower strength of encryption keys*. These results were presented in Table 23.

Table 23. Statistics of Respondents who Think Encryption Keys Derived from Biometrics would be Rich and Strong in Entropy

If Encryption Keys Derived from Biometrics would be Rich and Strong in Entropy	No. of Respondents	No. of Respondents Percentage (%)
Yes	72	92.3%
No	6	7.7%
Total	78	100.0%

4.3.6 Biometric Encryption Keys Future Use in Data Encryption

The study revealed that 62(79.5%) of respondents agreed that in the foreseeable future, encryption of data using biometric encryption keys will become a common practice among systems developers. 16(20.5%) of respondents did not think it would be possible. In asking this question we wanted to estimate respondents' expectations of future trends of biometric encryption security in this section. These results were shown in Table 24.

Table 24. Statistics of Respondents who Foresee Use Of Entropy from Biometrics in Data Encryption

Does it seem feasible in the near future for Entropy to be Derived from Biometrics and used in Data Encryption?	No. of Respondents	No. of Respondents Percentage (%)
Yes	62	79.5%
No	16	20.5%
Total	78	100.0%

4.4 Biometric Templates Security Challenges

This section sought to establish if respondents faced security challenges with regards to biometric template security then determine biometric attacks encountered and discover if biometric templates storage areas had been compromised. We also sought respondents' opinions on whether they considered databases as the most ideal preference for biometric templates storage and why they would not choose databases for biometric templates storage. Finally, the section investigates options respondents would use to ensure biometric templates are safely stored in databases.

4.4.1 Challenges Pertaining to Biometric Template Security

From the data collected, 15(19.2%) of respondents agreed to having encountered challenges related to biometric template security while 63(80.8%) did not. The respondents who admitted to having faced biometric template security issues were asked to specify in particular which challenges they experienced and they listed the following; *data theft from customer locations, difficulty in guaranteeing high accuracy levels while ensuring security levels are upheld, biometric templates modifications, leaking of biometric template information to unauthorized users, encryption keys being based on combination of passwords possibly known to adversaries, difficulty in generating random chaff surrounding biometric features in mobile devices due to limited processing resources and non-secure infrastructure*. Table 25 below shows these statistics.

Table 25. Statistics of Challenges Encountered in Biometric Template Security

Are there challenges encountered in Biometric Template Security?	No. of Respondents	No. of Respondents Percentage (%)
Yes	15	19.2%
No	63	80.8%
Total	**78**	**100.0%**

4.4.2 Type of Biometric Templates Attacks Encountered

The major attacks waged on biometrics templates by adversaries in biometric systems were; *spoofing* which is the fooling of biometric system by using fake finger, face or iris templates. *Spoofing* ranked as the most encountered attack reported by 43(55.1%) of respondents followed by *Tampering* at 20(25.6%).*Tampering* is where biometric attackers modify biometric feature sets to obtain high verification scores. *Trojan* attacks which entail the replacing of the biometric matcher programs with ones that always allow access were identified as the third most recurring attacks on biometric templates being identified by 19(24.4%) of respondents. *Replay attacks* where biometric system sensors are circumvented by running pre-saved biometric templates and *Substitution attacks* which involve replacing of users' biometric templates with those of adversaries each had 17(21.8%) of respondents identifying them respectively. A further 12(15.4%) of respondents did not encounter any biometric attacks as they specified *none* by selecting the *other* select option. These results were presented in Table 26 and Table 27.

Table 26. Statistics of Biometric Attacks Encountered

Combination of Biometric Attacks Encountered	No. of Respondents	No of Respondents in percentage (%)
Replay attacks	3	3.8%
Replay attacks, Substitution attacks	1	1.3%
Replay attacks, Tampering	1	1.3%
Replay attacks, Trojan attacks	1	1.3%
Spoofing	24	30.8%
Spoofing, Replay attacks	2	2.6%
Spoofing, Replay attacks, Substitution attacks	2	2.6%
Spoofing, Replay attacks, Substitution attacks, Tampering	2	2.6%
Spoofing, Replay attacks, Substitution attacks, Tampering, Trojan attacks	3	3.8%
Spoofing, Replay attacks, Tampering, Trojan attacks	1	1.3%
Spoofing, Replay attacks, Trojan attacks	1	1.3%
Spoofing, Substitution attacks	1	1.3%
Spoofing, Substitution attacks, Tampering	1	1.3%
Spoofing, Substitution attacks, Trojan attacks	1	1.3%
Spoofing, Tampering	3	3.8%
Spoofing, Trojan attacks	2	2.6%
Substitution attacks	2	2.6%
Substitution attacks, Tampering	2	2.6%
Substitution attacks, Tampering, Trojan attacks	2	2.6%
Tampering	3	3.8%
Tampering, Trojan attacks	2	2.6%
Trojan attacks	6	7.7%
Other(s)	12	15.4%
Total	**78**	**100.0**

Table 27. Statistics of Biometric Attacks Encountered

Biometric Attacks Encountered	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Spoofing	43	78	55.1%
Replay Attacks	17	78	21.8%
Substitution Attacks	17	78	21.8%
Tampering	20	78	25.6%
Trojan Attacks	19	78	24.4%
Other(s) None	12	78	15.4%
Total		**78**	**100.0%**

4.4.3 Biometric Templates Storage Compromised

Other than investigating types of biometric attacks experienced by respondents, we established that 2(2.6%) of respondents had their biometric template storage space compromised implying that adversaries not only attacked biometric templates but also attacked biometric storage space as well. 76(97.4%) of respondents had not experienced any attacks on their biometric templates storage space. The Table 28 shows these results.

Table 28. Statistics showing if Biometric Template Storage has ever been Compromised

Biometric Template Storage Space ever been Compromised	No. of Respondents	No of Respondents in percentage (%)
Yes	2	2.6%
No	76	97.4%
Total	**78**	**100.0%**

Information systems archive data in databases and since most biometric systems too store biometric templates in databases as well we discovered that 61(78.2%) of respondents considered databases as the most ideal storage space for biometric templates while 17(21.8%) of respondents did not. These results are shown in Table 29. The respondents who would not opt for databases to store biometric templates cited *security concerns, long time taken to find template match* and *risks involved in central storage databases*. They would instead *save biometric templates in dedicated memory sticks, encrypted folders* and *smart cards using MOC technology*. Other results showed suggestion of, '*a secure device where the operating system would be incapable of accessing'.*

Table 29. Statistics of Respondents using Databases as Ideal Template Storage Space

Respondents using Databases as Ideal Template Storage Space	No. of Respondents	No of Respondents in percentage (%)
Yes	61	78.2%
No	17	21.8%
Total	**78**	**100.0%**

4.4.4 Measures used to ensure Safe Storage of Biometric Templates in Database

We observed that 59(75.6%) of respondents indicated that *Encrypting of Biometric Templates Before Saving Them in Database* would ensure safe storage of biometric templates in database, 50(64.1%) of respondents would rather *Reduce Levels of Access to Database* while 38(48.7%) and 36(46.2%) of respondents would *Use strong passwords* and *change database passwords often* respectively. 4(5.1%) of respondents who had selected *others* specified that they would *implement strong access control to database, use finger scans to access database, use data vaults, deploy database firewalls* and *implement audit software*. These data results are shown in Table 30 and Table 31.

Table 30. Statistics of Measures ensuring Safe Biometric Templates in Database

Measures used to ensure Safe Storage of Biometric Templates in Database	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Change Database Passwords often	36	78	46.2%
Use Strong Passwords	38	78	48.7%
Reduce Levels of Access to Database	50	78	64.1%
Encrypt Biometric Templates Before Saving them in Database	59	78	75.6%
Other(s)	4	78	5.1%
Total		**78**	**100.0%**

Table 31. Statistics of Combination of Measures ensuring Safe Biometric Templates in Database

Combination of Measures used to ensure Safe Storage of Biometric Templates in Database	No. of Respondents	No of Respondents in percentage (%)
Change DB passwd	5	6.4%
Change DB passwd, Encrypt Bio Templates	1	1.3%
Change DB passwd, Reduce DB access	2	2.6%
Change DB passwd, Reduce DB access, Encrypt Bio Templates	3	3.8%
Change DB passwd, Strong passwd, Encrypt Bio Templates	2	2.6%
Change DB passwd, Strong passwd, Reduce DB access	3	3.8%
Change DB passwd, Strong passwd, Reduce DB access, Encrypt Bio Templates	20	25.6%
Encrypt Bio Templates	14	17.9%
Reduce DB access	1	1.3%
Reduce DB access, Encrypt Bio Templates	10	12.8%
Strong passwd	1	1.3%
Strong passwd, Encrypt Bio Templates	1	1.3%
Strong passwd, Reduce DB access	3	3.8%
Strong passwd, Reduce DB access, Encrypt Bio Templates	8	10.3%
Other(s)	4	5.1%
Total	**78**	**100.0%**

Key for Table 31:

Change DB passwd : Change Database passwords often
Reduce DB access : Reduce levels of access to database
Strong passwd : Use strong passwords
Encrypt Bio Templates : Encrypt biometric templates before saving them in database
Other(s) : Other(s)

4.4.5 Valuable Suggestions and Hints for furthering Safety of Biometric Templates

The sampled respondents mentioned that *biometric templates security is key to the advancement of the field of biometrics, passwords for biometric systems' databases should be changed every 90 days and no later than 180 days* and that *clearing i.e. zeroing data of de-allocated memory in biometric systems is of utmost significance as memory is vulnerable if malicious scripts could potentially read it and retrieve biometric image data before being emptied.*

5. CONCLUSION

The existing biometric fingerprint template protection schemes and approaches were reviewed. It was discovered that some biometric encryption schemes were preferred over others. From the data collected, majority of respondents saved biometric templates in databases. Spoofing was the most experienced attack on biometric templates. Results from sampled respondents showed that, a combination of measures and not one form of prevention measure were required to protect biometric templates against adversary attacks. In future work, we will propose a two-step encryption & decryption approach for securing biometric fingerprint templates stored in a database.

6. REFERENCES

[1] Das, Ashok Kumar. "Cryptanalysis And Further Improvement Of A Biometric-Based Remote User Authentication Scheme Using Smart Cards." *International Journal of Network Security & Its Applications*, 2011, 13-28.

[2] Tan, Z. "An efficient biometrics-based authentication scheme for telecare medicine information systems." *Przeglad Elektrotechniczny, ISSN 0033-2097, R. 89 NR 5/2013*, 2013, 200-204.

[3] Rathgeb, C., & Busch, C. (2012). "Multi-Biometric Template Protection: Issues and Challenges." *Intech*, 2012, 173-190.

[4] Ahmad, Sharifah Mumtazah Syed, Borhanuddin Mohd Ali, and Wan Azizun Wan Adnan. "Technical Issues and Challenges Of Biometric Applications as Access Control Tools Of Information Security." *International Journal of Innovative Computing, Information and Control Volume 8, Number 11, November 2012*, 2012: 7983-7999.

[5] D, Kannan, and Thilaka K. "Multibiometric Cryptosystem Based On Fuzzy Vault with Biohashing." *IOSR Journal of Electronics and Communication Engineering(IOSR-JECE)*, 2013: 34-43.

[6] Radha, N, and S Karthikeyan. "A Study On Biometric Template Security." *Ictact Journal on Soft Computing*, no. 01 (July 2010): 31-41.

[7] Radha, N, and S Karthikeyan. "An Evaluation Of Fingerprint Security Using NonInvertible Biohash." *International Journal of Network Security & Its Applications (IJNSA)* 3, no. 4 (July 2011).

[8] Ratha, Nalini, Sharat Chikkerur, Jonathan Connell, and Ruud Bolle. "Generating Cancelable Fingerprint Templates." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29 (April 2007): 561-572.

[9] Juels, Ari, and Madhu Sudan. "A Fuzzy Vault Scheme." *IEEE International Symposium Information Theory*, 2002.

[10] Geetika, and Manavjeet Kaur. "Fuzzy Vault with Iris and Retina: A Review." *International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 3, Issue 4, April 2013 ISSN:2277 128X, 2013.

[11] Deshpande, Avanti, and R B Joshi. "Information Security using Cryptography and Image Processing." *IJSRD - International Journal for Scientific Research & Development* 1, no. 9 (2013).

[12] Jeny, J.Rethna Virgil, and Chanda J. Jangid. "Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion." *International Journal of Emerging Technology and Advanced Engineering , (Volume 3, Issue 3, March 2013)*, 2013.

[13] D, Kannan, and Thilaka K. "Multibiometric Cryptosystem Based On Fuzzy Vault with Biohashing." *IOSR Journal of Electronics and Communication Engineering(IOSR-JECE)*, 2013: 34-43.

[14] Yates, Daniel S., and David S. Moore. *The practice of statistics*. New York: W.H. Freeman, 2008.

[15] Jain, A. K., Ross, A., & Uludag, U. (2005). "Biometric Template Security: Challenges and Solutions." *European Signal Processing Conference (EUSIPCO), (Antalya, Turkey), September 2005.*