

ALIGNMENT-FREE CANCELABLE IRIS KEY BINDING SCHEME

CH'NG KAI LIANG

**A project report submitted in partial fulfilment of the
requirements for the award of Bachelor of Engineering
(Honours) Mechatronics Engineering**

**Lee Kong Chian Faculty of Engineering and Science
Universiti Tunku Abdul Rahman**

May 2020

DECLARATION

I hereby declare that this project report is based on my original work except for citations and quotations which have been duly acknowledged. I also declare that it has not been previously and concurrently submitted for any other degree or award at UTAR or other institutions.

Signature : CH'NG _____

Name : Ch'ng Kai Liang _____

ID No. : 15UEB03759 _____

Date : 13 May 2020 _____

APPROVAL FOR SUBMISSION

I certify that this project report entitled “**ALIGNMENT-FREE CANCELABLE IRIS KEY BINDING SCHEME**” was prepared by **CH’NG KAI LIANG** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Engineering (Honours) Mechatronics Engineering at Universiti Tunku Abdul Rahman.

Approved by,

Signature

:



Supervisor

:

Mr. Chai Tong Yuen

Date

:

15/5/2020

The copyright of this report belongs to the author under the terms of the Copyright Act 1987 as qualified by the Intellectual Property Policy of Universiti Tunku Abdul Rahman. The due acknowledgement shall always be made of the use of any material contained in, or derived from, this report.

© 2020, Ch'ng Kai Liang. All right reserved.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor, Mr Chai Tong Yuen, who has guided me patiently and given me unconditional support from the beginning up till the very end. Without persistent help, it would be much tougher to achieve the goal of this research.

Besides, I would like to acknowledge the great love and overwhelming support from my family, friends, and course mates who have been constantly showering me with the moral support that was needed to endure all the problems faced.

ABSTRACT

The application of iris in the usage of biometric recognition systems has gain popularity over the years. It has raised the public concern on the reliability and consistency that could be achieved by using iris as part of the biometric recognition. This study aims to determine how the proposed framework performed when it is tested with a different database and the strength of the security. The proposed framework consists of 3 different processes, which include the Bloom Filter, Indexed First One Hashing, and the Key Binding Process. Four different databases have been used to test out the framework and the security's strength. Initial parameters have been optimized through extensive trials with the aids of using the Taguchi Method. The three main parameters that are crucial to determine the performance and security strength have been tested and the results have been tabulated in this report. The results indicate that the database with better quality will show much more promising results in terms of performance. The strength of the security is partially dependent on the performance. The trade-off between the performance and strength of the security can be observed across four different databases. Further research with a more recent public database that shall have better quality is needed to fully identify the performance and strength of the security for the proposed methods.

TABLE OF CONTENTS

DECLARATION		i
APPROVAL FOR SUBMISSION		ii
ACKNOWLEDGEMENTS		iv
ABSTRACT		v
TABLE OF CONTENTS		vi
LIST OF TABLES		viii
LIST OF FIGURES		x
LIST OF APPENDICES		xii
CHAPTER		
1	INTRODUCTION	1
1.1	General Introduction	1
1.2	Problem Statement	3
1.3	Objectives	4
1.4	Scope and Limitation of the Study	4
1.5	Outline of the Report	4
2	LITERATURE REVIEW	5
2.1	Introduction	5
2.2	Biometric Cryptosystem – Fuzzy Commitment	6
2.2.1	Fuzzy Vault	8
2.3	Cancellable Biometrics	8
2.4	Alignment-Free Chaffed Cancellable Iris Key Binding Scheme	11
2.4.1	Bloom Filter	11
2.4.2	Indexing-First-One-Hashing	12
2.4.3	Performance Evaluation	12
2.4.4	Security Analysis	15
2.5	Hill Climbing Attack	16
2.6	Summary	18

3	METHODOLOGY AND WORK PLAN	19
3.1	Alignment-Free Chaffed Cancellable Iris Key Binding Scheme	19
3.1.1	Bloom Filter	20
3.1.2	Key Binding	22
3.1.3	Indexing-First-One Hashing	22
3.1.4	Key Retrieval	25
3.2	Hill Climbing Attack	25
3.2.1	Rathgeb Method	26
3.3	Evaluation Metrics	27
3.4	Work Plan	28
4	RESULTS AND DISCUSSION	30
4.1	Performance Evaluation	30
4.2	Performance of Bloom Filter Iris Code and IFO Hashing	32
4.3	Performance of the Proposed Key Binding Method	34
4.4	Evaluation of Similarity Score Threshold t	34
4.5	Evaluation of Cryptographic Key Length n	38
4.6	Evaluation of Hashed Code Length m	39
4.7	Security Analysis	42
4.7.1	Renewal and Cancelability	42
4.7.2	Brute Force Attack	42
4.7.3	Hill Climbing Attack	43
4.8	Summary	44
5	CONCLUSIONS AND RECOMMENDATIONS	45
5.1	Conclusions	45
5.2	Recommendations for Future Work	45
	REFERENCES	46
	APPENDICES	49

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Comparison of Various Biometric Characteristic (Eng and Wahsheh, 2013)	1
2.1	Summary of State-of-the-arts	18
4.1	Summary of 4 Different Databases	30
4.2	Summary of Parameters used for 4 Different Databases	32
4.3	Summary of the Performances for 4 Different Databases	33
4.4	Configurations of Parameters for 4 Different Databases	34
4.5	System Performance for Parameter Set $(t, 10,100)$ on CASIA-v3-interval	35
4.6	System Performance for Parameter Set $(t, 10,250)$ on CASIA-v1	35
4.7	System Performance for Parameter Set $(t, 10,50)$ on CASIA-Iris Thousand	36
4.8	System Performance for Parameter Set $(t, 10,50)$ on ND0405	36
4.9	Overview Comparison of Best EER across 4 Database	37
4.10	Similarity Score Threshold for all the Database	37
4.11	Configurations of Parameters for 4 Different Databases	38
4.12	Configurations of Parameters for 4 Different Databases	39
4.13	Configurations of Parameters for 4 Different Databases	40

4.14	System Performance for Parameter Set (0.21,10, m) on CASIA-v3-interval	40
4.15	System Performance for Parameter Set (0.26,10, m) on CASIA-v1	40
4.16	System Performance for Parameter Set (0.60,10, m) on CASIA-Iris-Thousands	41
4.17	System Performance for Parameter Set (0.62,10, m) on ND0405	41
4.18	Summary Results for 4 Different Databases	44

LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	Encryption Process (Ali and Tahir, 2018)	9
2.2	System Performance for the Hashed IrisCode and Original Alignment-Free (Chai et al., 2019)	12
2.3	System Performance for Parameter Set $(t, 10, 100)$ (Chai et al., 2019)	13
2.4	System Performance for Parameter Set $(0.2, n, 100)$ (Chai et al., 2019)	14
2.5	System Performance for Parameter Set $(0.2, 10, m)$ (Chai et al., 2019)	14
2.6	Indistinguishability Between Synthetic and Genuine Iris Template (Chai et al., 2019)	15
2.7	Comparison of Complexity for Brute Force and False Accept Attacks (Chai et al., 2019)	16
3.1	Overview of Proposed Scheme (Chai et al., 2019)	19
3.2	Segmentation of Iris Code to Iris Block	20
3.3	Bloom Filtered Iris Code (Normal Circumstances)	21
3.4	Bloom Filtered Iris Code (Loss of Information)	21
3.5	Masking of Iris Code	22
3.6	Permutation of Bloom Filtered Iris Code with $p = 2$	23
3.7	Hadamard Multiplication 1	24
3.8	Hadamard Multiplication 2	24
3.9	Extracting Index when K Window is 4	25
3.10	Possible Attack Entry Point	26

3.11	Modification of Rathgeb's Hill-Climbing Attack	27
3.12	Gantt Chart for First Semester	28
3.13	Gantt Chart for Second Semester	29
4.1	Example Image for 4 Different Databases	30
4.2	Genuine and Imposter Matching Score for CASIA-v3-interval	38

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Table	49
B	Figures	53

CHAPTER 1

INTRODUCTION

1.1 General Introduction

Biometrics is often coined with the works that are related to the application of statistical and measuring analysis to any biometric characteristic, which can be extracted from an individual to undergo the process of biometric recognition (International Organization for Standardization, 2017). These biometric characteristics would include facial skin texture, finger topography, iris structure, retinal pattern, etc (International Organization for Standardization, 2017).

The implementation of biometric recognition systems across various industry especially airports has been gaining momentum over the years (Del Río et al., 2015). However, it also raised the public's concern regarding the security of the implemented system. During the occurrence of the event where the biometric characteristic has been compromised, it would render it useless in all the other involved biometric applications as well.

Table 1.1 below shows the comparison between several popular biometric characteristics with some of their characteristic which includes ease of use, accuracy, acceptability, security, and permanence (High = H, Medium = M, Low = L). Among various biometric characteristics, high confidence in the recognition of an individual's identity can be achieved via iris (Daugman, 2004).

Table 1.1: Comparison of Various Biometric Characteristic (Eng and Wahsheh, 2013)

Characteristic	Face	Fingerprint	Speech	Hand	Iris	Signature
Ease of Use	M	H	H	H	L	H
Accuracy	M	H	M	M	H	L
Acceptability	H	M	H	H	M	H
Security	M	H	M	M	H	L
Permanence	M	H	M	M	H	L

Iris has become a popular choice when it comes to biometric recognition systems due to its high accuracy, high permanence, and high security. Iris itself is secure as it is not directly accessible by others since it is a part of our human organ and it is unique. Although this would reduce the ease of use for iris, thanks to the availability of non-contact biometric technologies in the market, it helps to resolve the issue and at the same time, it also contributes to the high security (Kaudki and Bhurchandi, 2018).

Despite all the benefits that have been mentioned, there is still a downside when it comes to utilizing iris in a biometric recognition system. The major issues of using iris are the existence of variability which contribute by not limited to lacking clarity due to the fallen of eyelids, affected by the eyelashes, reflection on the lens, as well as the changes in pupil size due to the non-redundant deformation (Nazmdeh et al., 2019).

Another factor to be taken into consideration is the biometric recognition system that is used to process or store the iris database. Iris database will still be susceptible to leakage of privacy and loss of uniqueness data if the biometric recognition system has been compromised. To overcome this issue, the core function of conventional cryptography has been integrated with the authentication feature of biometric, which this method is also known as Biocryptography.

Secure communication between two parties can be performed through cryptography where the unauthorised third parties and potential attackers exist in the public environment (Pawar and Harkut, 2018). The high security of the cryptography is contributed by its encryption and decryption process. During the encryption process, a random key will be generated and bound with the data that would require to be transmitted and converted into an unreadable format which is known as the cypher. To decrypt the cypher, the key will have to be present to revert the encryption process. The high security that can be offered by utilizing cryptography makes it become a favourable option to be integrated with the biometric recognition system.

The high security by the cryptography would contribute to its low robustness at the same time. It will not allow a single bit of variation to exist in the generated key for the encryption and decryption process. The existence of the variability in iris itself would compromise the system easily and it will not

be recognised as the authorized user to gain access. Inevitably, this would lead to the limitation of the key length that can be generated. In general, the longer the generated key length, the higher the complexity it would be, thus increasing the secureness that it can offer. But in this scenario the longer the generated key that will be bind with the iris data, there will be more chances for the variability in the code itself to disrupt the “arrangement” of the key which will inevitably compromise the system.

To resolve this issue while integrating cryptography into a biometric recognition system, alignment-free cancellable iris key binding scheme has been proposed by Chai et al. In the proposed method, the iris code was protected through the mean of strong and size varying non-invertible cancellable transform (Chai et al., 2019), The proposed method is unique in a way that it allows the hashed code length to be a controllable parameter which in return could provide flexibility in authentication speed and system storage. Constant storage of seeds and the re-enrolment process that can be found in the conventional biocryptography system has been removed as well due to the introduction of the fast key regeneration process.

1.2 Problem Statement

Based on the new proposed cancellable iris-based key binding scheme, it was able to show promising results for the complexity and security level against potential attack when applied on public iris database CASIA v3-Interval (Chai et al., 2019). The newly proposed method also shows the complexity of 2^{100} bits for the brute force attack whereas 2^{66} bits for a false acceptance attack under the worst-case scenario.

However, for various biometric cryptosystems, they are vulnerable to various potential attack which not just only limited to brute force and false acceptance attacks (Rathgeb and Uhl, 2011a). One of the major potential threats that did not verify by Chai et al is the masquerade/hill-climbing attack. Since the hill-climbing attack is a major potential threat, without the support of evidence, the validity of the proposed scheme can be questioned. Aside from the potential threat, the performance of the proposed scheme was tested on just one public iris database. The deviation of results might occur if the proposed scheme was used to run through another iris database.

Therefore, the speculations that can be made would be whether the new proposed alignment-free cancellable iris key binding scheme is susceptible to a hill-climbing attack as well as what is its performance when it is used to run through another set of public iris database.

1.3 Objectives

The objectives of this study are to identify the performance of the proposed scheme under two different condition, which includes:

1. The security resistance of the proposed scheme against the hill-climbing attack and brute force attack.
2. Evaluate the performance and security of the proposed scheme thoroughly through other publicly available databases.

1.4 Scope and Limitation of the Study

In this study, the performance of the proposed scheme will be solely based on the key binding method itself. Chai has assumed that during the communication between the bloom filter process and indexing-first-one (IFO) hashing is secure and will not be tapped in by the potential malicious attackers. Security analysis will be performed solely on the proposed scheme as a whole.

The quality of the database would be part of the limitation as well. 3 out of 4 for the tested public iris database were having the rather noisy iris image. Therefore, it can be observed that the results for these 3 noisy databases would deteriorate when compared to the better iris database.

1.5 Outline of the Report

Further organization of this paper is as described: Chapter 2 is the section of literature review which allows the readers to have a better understanding of what is a biometric recognition system, how it could integrate with cryptography, and how did its implementation has changes throughout history. Chapter 3 explains the methodology of how the experiments will take place to achieve the objectives of this study. Chapter 4 would include the results and the discussion that has been obtained through the experiment. Last but not least, Chapter 5 will conclude this study, and recommendations for further study will be included.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The authentication feature of biometric that was used to integrate with conventional cryptography to create biocryptography is known as a biometric template. In general, these biometric templates can be further categorised into Cancellable Biometric (CB) and Biometric Cryptosystem (BCS). To achieve data privacy preservation, the designs of these schemes have to fulfil three main criteria, which is the unlikability, cancelability, and irreversibility (Chai et al., 2019).

The philosophy of the biometric cryptosystem can be differentiated into two major processes, which are the key binding process and key generation process. Binding a biometric data onto a digital key securely is known as the key binding process whereas regenerating the digital key through the biometric data is known as the key generation process. To achieve a secure biometric cryptosystem, first and foremost, it has to be only storing the biometric dependent data instead of the cryptographic key itself (Chai et al., 2019). Secondly, the biometric data or the digital key has to be computationally difficult to retrieve. Last but not least, during the authentication process, the input query has to show sufficient similarity above the threshold value to retrieve the key as it has to take the slight variation in the biometric data input into consideration.

Cancellable biometrics, on the other hand, is another approach for biometric template protection by utilizing the effort of altering the biometric template through repeating the transformation process, which then allowed the authentication process to take place in the transformed domain (Ratha et al., 2007). The storing of the distorted biometric template is more secure as in the event of compromised, the new templated can be always reconstructed through the transformation process. Therefore, during the design stage for the cancellable biometric scheme, four crucial criteria must be fulfilled, which include:

1. Performance: The accuracy that can be achieved by the cancellable template when compare to the prior conversion process should yield similar results.
2. Revocability: In the event where *multiple* protected templates have been compromised, the original biometric data must not be able to derive.
3. Unlikability: The protected biometric template from an individual shall be distinct in the way that cross-matching across various applications is infeasible.
4. Non-invertibility: In the event where the protected template has been compromised, it should be impossible to be reverse engineered to obtain the original biometric data.

2.2 Biometric Cryptosystem – Fuzzy Commitment

Fuzzy commitment and fuzzy vault are two crucial schemes that have been designed to utilize the key binding approach (Chai et al., 2019). Juels and Wattenberg are the pioneers of combining the Error Correction Code (ECC) with cryptography to produce what is known as the fuzzy commitment scheme in these days (C. Rathgeb and Uhl, 2010).

In a fuzzy commitment scheme, it will consist of a function F , which will be used as a witness where, $w \in \{0,1\}^n$ and to commit a codeword where $c \in \mathcal{C}$. The \mathcal{C} is a set that would contain the error-correcting codewords c with respective to the length of n and the witness would be a n bits binary string which will be representing the enrolled biometric template (C. Rathgeb and Uhl, 2010). The helper data, δ is the difference vector between w and c , which can be obtained via bit-wise XOR operation, $\delta = w \oplus c$. The helper data, δ will be stored into the database with $h(c)$ together with the hashed function $h(\cdot)$. During the authentication stage, whenever the query binary string provides sufficient similarity within the error correction code capability when compare to the enrolled template, the results will be first hash then tested against $h(c)$. If it was the authorised access, the comparison would yield a result of $h(c') = h(c)$ (Chai et al., 2019).

The first implementation of a fuzzy commitment scheme on biometric was performed by Hao et al (C. Rathgeb and Uhl, 2010). Using the in-house

dataset, a false acceptance rate (FAR) was able to achieve 0% while 99.53% for the genuine acceptance rate (GAR) (Hao et al., 2006). The main idea of their scheme was to eliminate the bits error caused by the variance by applying Hadamard code and the burst errors will be corrected by the Reed-Solomon codes (Hao et al., 2006). Their approach was to bind the 140-bit cryptographic code with the 2048-bit iris codes.

However, this approach is deemed to be having a high false rejection rate of 0.47% (C. Rathgeb and Uhl, 2010). Instead of using the Reed-Solomon code, Bringer and et al then proposed a similar approach by using a matrix consist of two different Reed-Muller codes (C. Rathgeb and Uhl, 2010). By using these approaches, Philips and et al were able to achieve zero FAR and GAR of 94.83% on the ICE 2005 iris database (Phillips et al., 2008).

False acceptance rate and genuine acceptance rate are the two parameters that use to measure the effectiveness of a biometric cryptosystem (Nagar et al., 2012). Generally, the false acceptance rate of a biometric cryptosystem is expected to have a value of zero. Although several approaches included those mention above show a promising result of zero for the false acceptance rate, fuzzy commitment did not perform well in terms of security (Nagar et al., 2012). Fuzzy commitment and fuzzy vault will not able to generate revocable templates, which make them vulnerable to linkage attacks (Nagar et al., 2012). Aside from the linkage attack, researchers have also performed statistical attacks and decodability attacks.

Rathgeb and Uhl have proposed and performed a statistical attack against iris-biometric fuzzy commitment schemes based on error correction code histogram (Rathgeb and Uhl, 2011). They have concluded that the fuzzy commitment scheme is still vulnerable to the proposed attack even though the binary feature vector should have already provided sufficient entropy and able to bind with cryptographic key securely (Rathgeb and Uhl, 2011).

The decodability attack for the vulnerability of the fuzzy commitment scheme that was based on linear ECC was first published by Stoianov (Kelkboom et al., 2011). This vulnerability arises if decoding the XOR of the auxiliary elements can be cross-matched across several different databases and leads to a valid codeword, there is a high possibility that the “cracked” codework belongs to the same individual thus can be labelled as genuine (Kelkboom et al.,

2011). Kelkboom et al proved that implementing a bit-permutation mechanism could help improve the resistance toward a decodability attack.

Aside from vulnerable to potential attacks, fuzzy commitment can only be performed in the binary form as matching in the hamming domain can only handle binary numbers. Thus, this has limited the scheme to achieve better performance as it would not be able to utilize a more effective matching technique and feature extraction process (Chai et al., 2019). Therefore, the vulnerabilities of iris-based fuzzy schemes in terms of the potential attack as well as the limitation, the privacy and security it can provide is doubtful (Chai et al., 2019).

2.2.1 Fuzzy Vault

Other than fuzzy commitment, the fuzzy vaults scheme that was introduced by Juels et al would be able to contribute to the error-tolerant verification as well as protection for a biometric cryptosystem. Lee et al was the first one to implement the scheme with iris and was able to obtain genuine acceptance rate of 80% together with the zero false acceptance rate when the employing bit keys are equivalent to 128 when it is performed on a CASIAv3-Interval Iris database (Lee et al., 2008).

The lack of implementation of a fuzzy vault scheme for a biometric cryptosystem leads to a lack of detailed security and performance analysis (Chai et al., 2019). However, there was a case where the vulnerability of fuzzy vaults in biometric was first exposed by Juels and Sudan, it was susceptible to linkage attack and correlation attacks when fused it with fingerprint instead of iris (Chai et al., 2019). Chai et al conclude that the implementation of the fuzzy vault for biometric is impractical in terms of the decoding complexity are infeasible.

2.3 Cancellable Biometrics

The first cancellable biometric was introduced by Ratha et al (Rathgeb et al., 2013). To achieve a revocable template, Ratha et al have performed surface-folding as well as imaged based block permutations (Rathgeb et al., 2013). The vulnerability of Ratha et al method was then found in terms of the non-invertibility although the high accuracy performance was able to be achieved (Bringer et al., 2015). Despite the setback, the opening of “Pandora’s Box” has

encouraged more researchers to look into biometric template protection (Chai et al., 2019).

In general, cancellable biometric can be classified into non-invertible transformation as well as biometric salting. By applying the non-invertible transformation, the transformed biometric template will then be able to store securely inside the system itself. To achieve non-invertible transformation, Ali and Tahir proposed an encryption process that will be able to distort the biometric template while retaining the original biometric information (Ali and Tahir, 2018). The encryption will first obtain the size of the array, $s = x \times y$, where x representing the rows and y representing the column. The encryption process will read through each row and concatenate the first odd element with the next odd element that followed by. An additional new array A_N will be used to store the concatenated odd value. The same process will then be repeated for the even element. Storing of the element between odd and even value be repeated until the end of the array. Figure 2.1 below shows a graphical representation of the proposed encryption process.

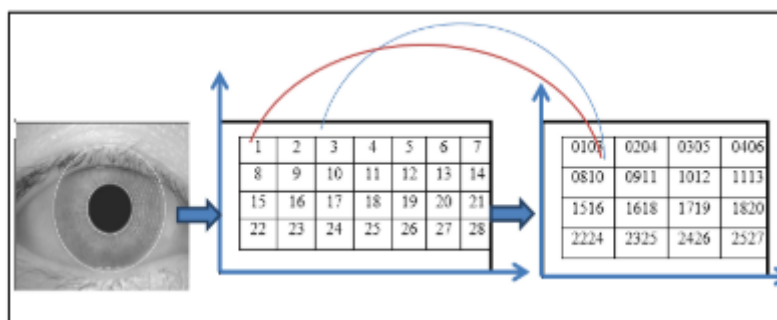


Figure 2.1: Encryption Process (Ali and Tahir, 2018)

The proposed encryption method by Ali and Tahir will only be implemented after the feature extraction and encoding process (Ali and Tahir, 2018). In their framework, the support vector machine is used as the classifier, fusion of mask, and profile approach for iris detection of the pupil and 2D Gabor filter as their feature extraction (Ali and Tahir, 2018).

The proposed method is then tested on the Bath-A database with a total of 1000 samples of iris image which then half of it will be used for training

purposes and another half of it to be used as testing. It was able to achieve the result of 0.09% FAR and a recognition rate of 99.99% (Ali and Tahir, 2018).

Another variation of non-invertible transformation has been performed by Rathgeb et al which titled alignment-free cancelable iris biometric templates based on adaptive bloom filter (Rathgeb et al., 2013). What makes bloom filter interesting is the capability to perform many-to-one mapping for the biometric data, which will make it non-invertible transformation at the same time (Chai et al., 2019). Comparing to the original counterpart, the bloom filter was able to achieve similar performance in terms of accuracy. However, the low complexity of 2^{25} was all it needs to perform the restoration of the biometric template (Mennink et al., 2014).

Security analysis was then performed by Bringer et al on the alignment-free cancelable iris biometric templates based on the adaptive bloom filter that was proposed by Rathgeb et al (Bringer et al., 2015). In terms of unlikability, it was found out that it was susceptible to a brute force attack due to small keyspace (Bringer et al., 2015). The attack was considered as a generic attack as the exploitation was made possible due to the small keyspace, rather than the biometric data itself. Bringer et al proposed a solution that would require the tradeoff between security and performance. Increasing the size of the key would increase the secureness but at the same time will degrade the authentication/identification results.

Moving on from non-invertibility transformation, the biometric template that undergoes invertible transform can be known as the biometric salting. To achieve the distorted biometric template, the biometric data will be combined with specific data which is known as the auxiliary data (Choudhury et al., 2017). Due to the binding of biometric data with auxiliary data, the revocability was able to achieve through the changing of the auxiliary data (Choudhury et al., 2017).

Aside from binding with the user-specific auxiliary data, another approach to performing biometric salting would be through the usage of synthetic patterns and random noise pattern (Choudhury et al., 2017). Zuo et al proposed the method where is known as GRAY-SALT for real-valued iris data and BIN-SALT for binary iris data (Zuo et al., 2008). To perform GRAY-SALT, a random pattern will be combined with real-valued iris data through either

multiplication or addition. A similar concept can be applied to BIN-SALT. Instead of multiplication or addition, XOR operations would be used to perform the combination.

The method proposed by Zuo et al was able to achieve the revocability as well, but there was a major flaw. To achieve high accuracy performance, the pre-alignment process is a must (Zuo et al., 2008). Several other invertible transformations have been proposed by other researchers such as sectorized random projections and S-Iris Code encoding (Chai et al., 2019). S-Iris Code encoding method suffers performance degradation by the noise that causes by weaker inner-product but it still can be improved/solved by implementing a noise mask.

On the other hand, the issue of sectorized random projection is either if the same random projections matrix has been applied to a different user, the performance would be compromised. There is also research showing that the disclosure of a random projection matrix will be able to invert the cancelable template, which makes it come short when comparing to other methods (Chai et al., 2019).

To sum up, for biometric salting to be feasible for the application of cancelable biometric, one crucial circumstance has to be fulfilled, which is the auxiliary data shall not be exposed to the public and has to be kept as a secret (Chai et al., 2019).

2.4 Alignment-Free Chaffed Cancellable Iris Key Binding Scheme

Alignment-free chaffed cancellable iris key binding scheme is a method that was proposed by (Chai et al., 2019) which they have integrated bloom filter and indexing-first-one hashing to generate the alignment-free biometric template. Figure 3.1 below shows the overall framework of the proposed scheme.

2.4.1 Bloom Filter

According to the experiment performed by (Rathgeb et al., 2013), the increase in the dimension of the smaller block, the biometric performance would suffer drastically lost as too much information has been missing during the many to one mapping. However, the application of the bloom filter can show promising results from the range of 1.14% to 1.83% for small block size without taking

the feature extract algorithm and word size into consideration (Rathgeb et al., 2013).

Although the methods proposed by (Rathgeb et al., 2013), has been proved to have the vulnerability toward generic attack due to low keyspace (Bringer et al., 2015), it was still able to obtain the complexity from the range of 2^{126} to 2^{283} depends on the size of the block (Rathgeb et al., 2013). Rathgeb et al also conclude that the trade-off between security and biometric performance in the cancellable biometric system is inevitable.

2.4.2 Indexing-First-One-Hashing

Lai et al have proven that indexing-first-one hashing was able to withstand several privacy and security attacks. A complexity of 2^{512} was able to achieve when subject to a single hash attack and 2^{136} for pre-image attack under no degradation of the accuracy performance. Revocability and unlikability was able to achieve as well and the permutation token for the user was not required to keep as a secret, which make this approach more user-friendly (Lai et al., 2017)

2.4.3 Performance Evaluation

EER are usually parts of the parameters that used to evaluate the performance of the biometric system, which can be obtained through the false rejection rate (FRR) and false acceptance rate (FAR) between the collected imposter and genuine score (Chai et al., 2019). In (Chai et al., 2019) approach, the EER was approximated as $EER \approx (FAR + FRR)/2$. The low value of EER indicate a better performance. The comparison between the performance of bloom filtered iris code and original iris code has been performed, which yield the results as shown in Figure 2.2 below.

CASIA v3 Database [29]	Equal Error Rate (EER %)
IrisCode	0.38
Bloom filtered IrisCode	0.50
Bloom filtered IrisCode (IFO applied)	0.58

Figure 2.2: System Performance for the Hashed IrisCode and Original Alignment-Free (Chai et al., 2019)

The results obtained from (Chai et al., 2019) shows that there is no significant drop in system performance. Aside from system performance, it also able to prove that the compatible performance with the application of index-first-one-hashing.

In (Chai et al., 2019) paper, three different evaluation has been measured to take into consideration on how similarity score threshold, t , cryptographic key length, n and hashed code length, m would affect the system performance of the proposed scheme. The results for FRR and FAR for t from the range of $t = [0.16, \dots, 0.25]$ with $m = 100$ and $n = 10$ are shown in Figure 2.3 below.

t	FRR (%)	FAR (%)	EER (%)
0.16	0.15	12.14	6.97
0.17	0.31	3.23	1.77
0.18	0.62	0.62	0.62
0.19	1.65	0.05	0.85
0.20	2.65	0.00	1.33
0.21	3.80	0.00	1.90
0.22	5.61	0.00	2.81
0.23	8.26	0.00	4.13
0.24	11.56	0.00	5.78
0.25	15.40	0.00	7.70

Figure 2.3: System Performance for Parameter Set ($t, 10, 100$) (Chai et al., 2019)

FAR are usually recommended to have a value of zero for a cryptosystem to be useful so that any unauthorised access personnel would not stand a chance to access the system. By keeping this in mind, Chai et al conclude that the optimal value for t shall fall under the range of $t \geq 0.2$ to achieve zero FAR.

Figure 2.4 below shows the system performance for when the value of cryptographic key length, n is equivalent to $n = [10, 20, 40, 60, 80, 100, 150, 200]$ while $t = 0.2$ and $m = 100$.

n	GAR (%)	FAR (%)	EER (%)
10	97.35	0.00	1.33
20	96.67	0.00	1.67
40	96.67	0.00	1.67
60	96.37	0.00	1.82
80	96.37	0.00	1.82
100	96.37	0.00	1.82
150	96.37	0.00	1.82
200	96.37	0.00	1.82

Figure 2.4: System Performance for Parameter Set (0.2, n , 100) (Chai et al., 2019)

Aside from the FAR and EER, a genuine acceptance rate (GAR) was included with $GAR = 100 - FRR$. It can be observed that a shorter key length would yield a higher GAR. Other observations such as EER remain constant when the key length has increased to 200, which represents that the performance of the system has been able to retained (Chai et al., 2019).

Figure 2.5 below tabulates the system performance for hashed code length, m from the range of $m = [10, 50, 100, 150, 200, 250, 300]$ where $t = 0.2$ and $n = 10$. There was an additional column that labelled as storage/bit included as well.

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/ n)
10	89.51	0	5.25	0.19
50	95.97	0	2.02	0.94
100	96.37	0	1.82	1.90
150	96.37	0	1.82	2.81
200	96.37	0	1.82	3.75
250	96.37	0	1.82	4.69
300	96.37	0	1.82	5.63

Figure 2.5: System Performance for Parameter Set (0.2, 10, m) (Chai et al., 2019)

Overall, the FAR was able to maintain at the value of zero whereas the GAR remain stagnant at a value of 96.37%. Changing of hashed code length will be able to alter the storage per bit at the cost of the system performance. The proposed scheme by Chai et al also proofed to have a more compact form of storage when compared to (Li et al., 2010) which achieves an average of $31.2kb$ for fingerprint application.

2.4.4 Security Analysis

In Chai et al proposed scheme, the synthetic biometric template has been utilized, thus it was important to ensure that the unauthorised access personnel would not be able to distinguish the genuine and synthetic template. Chai et al had designed an indistinguishability game to examine the performance of the proposed scheme. Figure 2.6 shows the summary of the result for the indistinguishability between synthetic and genuine iris template through the proposed game where $S(B_g, B') = [0.16, 0.17, 0.18, 0.19]$, $M = 10000$ and $n = [1, 50, 100, 200]$.

$S(B_g, B')$	$\text{Adv}_{\text{Gen-Syn}}^n$ ($n=1$)	$\text{Adv}_{\text{Gen-Syn}}^n$ ($n=50$)	$\text{Adv}_{\text{Gen-Syn}}^n$ ($n=100$)	$\text{Adv}_{\text{Gen-Syn}}^n$ ($n=200$)
0.16	2.0561×10^{-26}	1.0281×10^{-24}	2.0561×10^{-24}	4.1122×10^{-24}
0.17	3.0075×10^{-15}	1.5038×10^{-13}	3.0075×10^{-13}	6.015×10^{-13}
0.18	1.4936×10^{-7}	7.6480×10^{-6}	1.4936×10^{-5}	2.9872×10^{-5}
0.19	0.0058	0.29	0.58	1.16

Figure 2.6: Indistinguishability Between Synthetic and Genuine Iris Template (Chai et al., 2019)

It can be observed that when the total advantages will obtain the value that is greater than 1 when the cryptographic key length reaches a length of 200. This is due to the increase in the number of iris templates that used to bind with the key would have greater information leakage (Chai et al., 2019).

In the event when the cryptographic key has been compromised, the renewal process is rather easy which would not require the re-enrollment process. The new cryptographic key can be updated by just swapping the position of the genuine and synthetic template together with the corresponding hashing group (Chai et al., 2019).

A potential attack such as brute force attack shows a complexity up to 2^{200} . This is due to the nature of the brute force attack which randomly guessing the n bit cryptography key. The best performance that can be achieved by the proposed scheme was when $n = 200$ with 1.82% *EER*, which explain the complexity of 2^{200} (Chai et al., 2019).

False accept attack was another potential attach that has been studied in the scheme proposed as well. Different from the brute force attack, the false

accept attack will tap into the adversary of the cancellable storage (Chai et al., 2019). Figure 2.7 below shows the comparison for false accept attack and brute force attack with the similarity score $S(B_g, B') = [0.195, 0.196, 0.197, 0.199, 0.20]$, $m = 200$ and $t = 0.20$.

$S(B_g, B')$	$Bf_{n=100}$	$fa_{KRR_{imp}}$
0.195	2^{100}	2^{162}
0.196	2^{100}	2^{133}
0.197	2^{100}	2^{107}
0.198	2^{100}	2^{85}
0.199	2^{100}	2^{66}

Figure 2.7: Comparison of Complexity for Brute Force and False Accept Attacks (Chai et al., 2019)

In general, the complexity of the false accept attack is lower compared to the brute force attack. By taking the worst-case into scenario into consideration, the proposed scheme would have a false accept complexity of 2^{66} bits (Chai et al., 2019).

2.5 Hill Climbing Attack

Hill climbing is an algorithm that will approach an existing problem with an arbitrary solution to find for the global optimum solution. The algorithm will then keep on improving itself to find a better solution by exploring the other possible neighbouring solution. One of the major issues with hill climbing is that it will be terminated when a peak is reached, in which the results might be trapped in a local optimum. Hill climbing attack is often quoted to be similar to a brute force attack, but there are differences in nature.

When a hill-climbing attack is applied to an iris biometric system, it is performing the task of generating synthetic representations and attacking the system iteratively until successful recognition is achieved. During the hill-climbing attack, it will improve itself based on a fixed algorithm and will retain the changes if the observed function or objection score was able to achieve improvement whereas a brute force attack will be just merely attacking the system blindly until it was able to trick the system with a correct combination.

Hill climbing attack has been modified into several variations to suit the biometric scheme that the researcher is targeting.

In the proposed method by (Christian Rathgeb and Uhl, 2010), an assumption has to be made, which is the attacker has to be able to tap into the communication channel of the biometric system to retrieve the matching score. Rathgeb has summarized his proposed hill-climbing attack into four simple steps. First of all, a predefined constant will be used to increase the value of a pixel and the authentication will be performed. Such modification will be retained if the matching score return has been shown to have increased. If the return value of the matching score is reduced or remains the same, the modified pixel value will be then decreased by the predefined constant, and authentication is performed again. If the return value of the matching score has improved, the modification will then be retained. The whole process is then repeated until the modified input has been accepted by the system or no significant improvement can be made anymore (Christian Rathgeb and Uhl, 2010).

However, the proposed HCA will only return high matching score value if the target iris biometric system shares the same similarity on the feature extraction process as proposed by Masek (Christian Rathgeb and Uhl, 2010).

In another study of (Maiorana et al., 2015) for the hill-climbing attack that will be applied to a multi-biometric recognition system. Several different approaches have been discussed that are targeted to approach the system with a fixed-length template.

SPSA is a stochastic approach that is used to measure the gradient. A starting point will be pre-determined and it will be run for a fixed iteration. If the estimated gradient is below a pre-defined threshold, the process will be restart with another set of perturbation vector that is randomly generated (Maiorana et al., 2015).

The implicit filtering algorithm shares some similarities when compared to the SPSA algorithm. A scale factor is added into each of the generic iterations. The scale will be updated when the obtained estimated gradient is lower than a given threshold. The function of the scale is to avoid the local maximum as well as in the event when the algorithm went into stagnation, the last working point with the largest scale will be used to restart the algorithm (Maiorana et al., 2015).

To implement the proposed algorithm on a unimodal biometric recognition system, the obtained similarity scores will be used as the evaluation for the unknown objective function.

2.6 Summary

Table 2.1 below shows the summary or the comparison between the reviewed method with the available genuine acceptance rate and false acceptance discussed in Chapter 2.

Table 2.1: Summary of State-of-the-arts

Methods	GAR (%)	FAR (%)
Fuzzy Commitment (Hao et al., 2006)	99.53	0
Fuzzy Commitment (Phillips et al., 2008)	94.38	0
Fuzzy Vault (Lee et al., 2008)	80.00	0
Cancellable Biometric (Ali and Tahir, 2018)	-	0.09
Key Binding Scheme (Chai et al., 2019)	97.35	0

CHAPTER 3

METHODOLOGY AND WORK PLAN

3.1 Alignment-Free Chaffed Cancellable Iris Key Binding Scheme

Referring to Figure 3.1, the proposed scheme can be further categorized into three main stages/process, which is the enrolment process, query process, and authentication process (Chai et al., 2019).

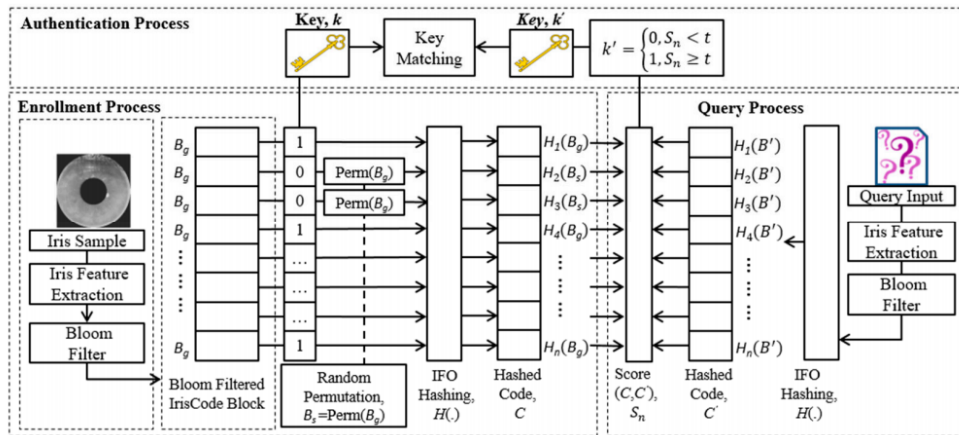


Figure 3.1: Overview of Proposed Scheme (Chai et al., 2019)

Iris sample that is fed into the proposed scheme will first undergo a feature extraction process. In Chai et al paper, they utilized the public available iris database, CASIA v3-interval, which is a pre-processed iris code. The iris code will then go through a bloom filter, followed by the indexing-first-one-hashing before the final hashed code that is already bound with a ‘secret key’ is stored (Chai et al., 2019).

For the authentication process to take place, matching between the reference hashed codes and queries will then be performed. Matching will be performed through the method of calculating the difference of similarity score with a pre-defined threshold. Eventually, a final binary string of keys will be able to retrieve if the query input was able to obtain the similarity score that is higher than the predefined threshold.

The evaluation of the proposed scheme will be tested with four different databases, which include the CASIA-v3-interval database, CASIA-Iris-

Thousand database, CASIA-v1 database, and ND0405 database with a laptop that equipped with processor core of Intel i7-5500U, 8GB RAM and MATLABR2018a.

3.1.1 Bloom Filter

Bloom filter technique that was proposed by (Rathgeb et al., 2013) was adopted by Chai et also that the head rotation issues in iris code can be resolved. The original iris code is denoted by, $I \in \{1,0\}^{n_1 \times n_2}$ will be transformed into a matrix which is denoted as bloom filtered iris code, B .

The matrix of iris code will first be split into $I_1 \cdot I_2$ blocks, where $I_1 = \frac{n_1}{L}$ and $I_2 = \frac{n_2}{W}$. Smaller block section will be formed inside the $I_1 \cdot I_2$ blocks with a fixed dimension of W and L , indicating the column and row respectively. Each of this smaller block section will be governed by bloom filter with the value of $b \in \{0,1\}^{2^L}$. All the elements in b will first set to be 0 and the element of '1' will be added into it depends on the calculated decimal position govern by the column codeword, $x_j \in \{1,0\}^L \mid j = 1, 2, \dots, W$ in each block (Chai et al., 2019). To construct the final matrix for bloom filtered iris code, $B \in \{0,1\}^{I_1 \cdot I_2 \times 2^L}$, the compilation of every bloom filter b_i for each block (for $i = 1, 2, \dots, I_1 \cdot I_2$) will be performed (Chai et al., 2019).

In this experiment, the iris code from the various database will first be segmented into smaller iris blocks govern by the parameters of width, W , and length, L . Figure 3.2 below shows the illustration of segmenting iris code into the iris blocks.

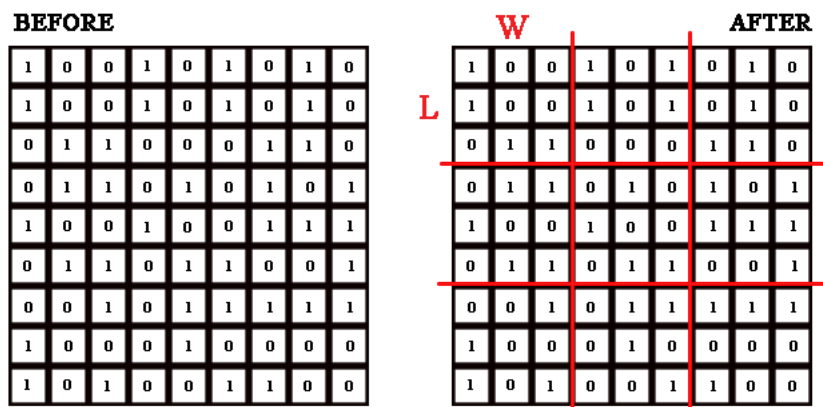


Figure 3.2: Segmentation of Iris Code to Iris Block

Under normal circumstances where the noise in the iris code is negligible, no mask will be applied on it and the decimal number will be extracted based on the index of the '1' element in a column-wise manner as shown in Figure 3.3 below. By default, all the elements in $R1$ will be '0' elements.

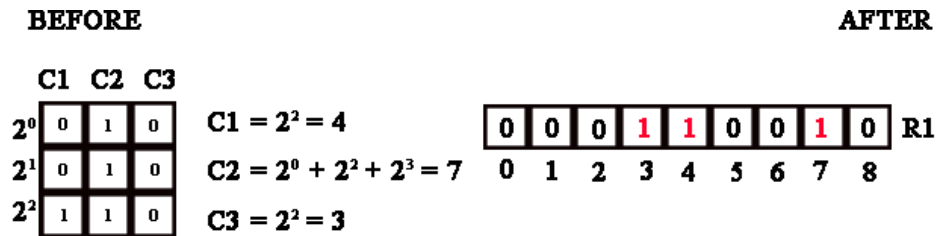


Figure 3.3: Bloom Filtered Iris Code (Normal Circumstances)

As mentions in (Rathgeb et al., 2013), one of the features of Bloom Filter was it was able to perform many to one mapping which being part of the trade-off between the performance and the security. Figure 3.4 below shows the scenario of how the bloom filtered would look like when the column-wise index returns the same value.

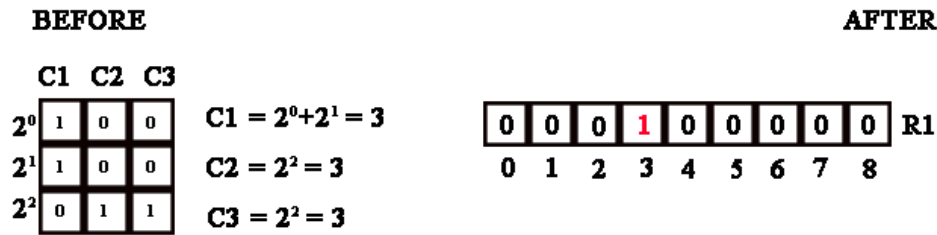


Figure 3.4: Bloom Filtered Iris Code (Loss of Information)

3.1.1.1 Masking of Bloom Filter

In this experiment, the iris block will be a mask with a binary mask that has the same dimension of width, W , and length, L . A pre-defined noise threshold, T will be the first set. During the event of the particular iris block having a high number of noisy bits that have already over the pre-defined threshold, it will be ignored and filtered out without generating a new entry for the bloom filtered iris code. Figure 3.5 below shows the illustration for the masking process.

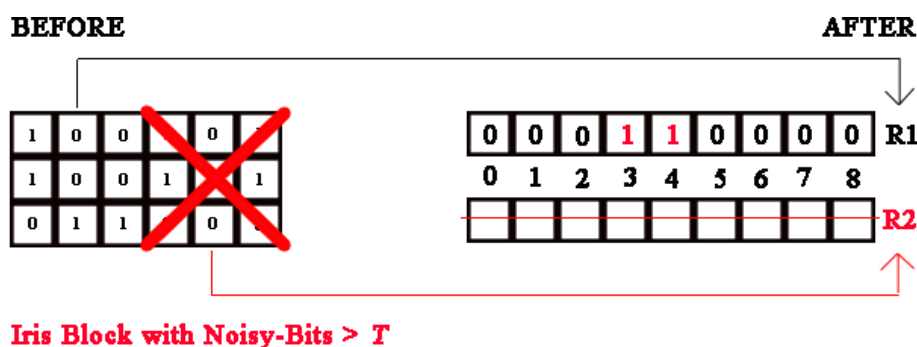


Figure 3.5: Masking of Iris Code

3.1.2 Key Binding

A random binary cryptographic key, K with a predefined length will first be generated. In the binary key, the '1' element will be bind with the genuine template, which is the bloom filtered iris code while the '0' element would be bind with a synthetic template. The synthetic template will then be generated by applying permutation on the genuine template.

The binary cryptographic key which has now stored the biometric data will then be going through the indexing-first-one hashing process so that hashed code will be stored in the database instead of the cryptographic key, K to ensure the secureness of it.

3.1.3 Indexing-First-One Hashing

Similarly, with Bloom Filter, Indexing First One Hashing is one of the methods that can be implemented to achieve alignment-free biometric generation (Chai et al., 2019). IFO hashing is an extension of utilizing modulo thresholding with Hadamard product code coupled with Min-Hashing. To perform IFO Hashing, the process itself can be summarised into six steps (Lai et al., 2017).

First of all, a p number of random permutation will be generated for the iris code with the dimension of $n_1 \times n_2$ in a column-wise manner (Lai et al., 2017). p -ordered Hadamard product code will be obtained through the mean of multiplying all the randomly permuted iris code. This step is essential as to avoid reverse engineered of iris code feasible in the event when it has been compromised since large amount of binary information will be lost (Lai et al., 2017).

A K window will be first constructed which will use to select the first ‘1’ element that appears within that particular window. The concept of min-hashing is utilized during this stage (Chai et al., 2019). The index of the first ‘1’ element that appears will then be extracted before it was passed through modulo thresholding. Implementation of modulo thresholding is to further strengthen the non-invertibility properties of the biometric template due to the modulo threshold that can induce many to one mapping (Lai et al., 2017). All these steps would be repeated by using the independent hash function, m to obtain a $n_1 \times m$ matrix of IFO hashed code $C \in \mathbb{Z}_{K-T}^{n_1 \times m}$ (Lai et al., 2017).

In this experiment, to perform the IFO hashing, a predefined amount of the number of permutation, p will be determined. Each row of the bloom filtered iris code will then go through p amount of permutation. Figure 3.6 below shows the permutation of first-row bloom filtered iris code with $p = 2$.

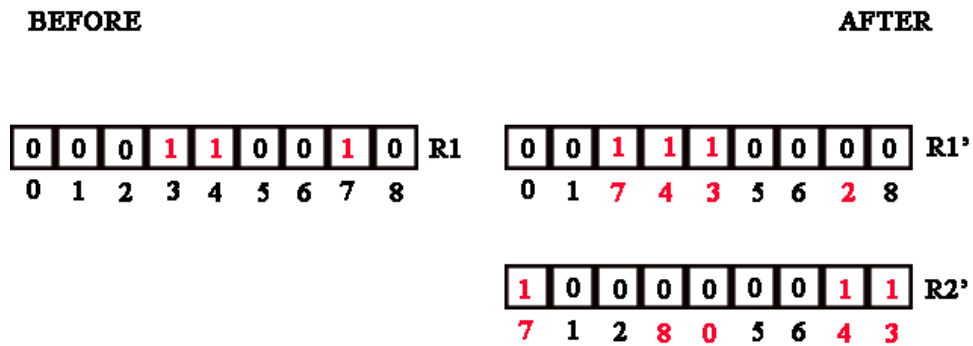


Figure 3.6: Permutation of Bloom Filtered Iris Code with $p = 2$

Hadamard Multiplication will then be performed on the permuted iris code which transforms the p row of permuted iris code into a single row of product code. Figure 3.7 below shows the illustration of the Hadamard multiplication.

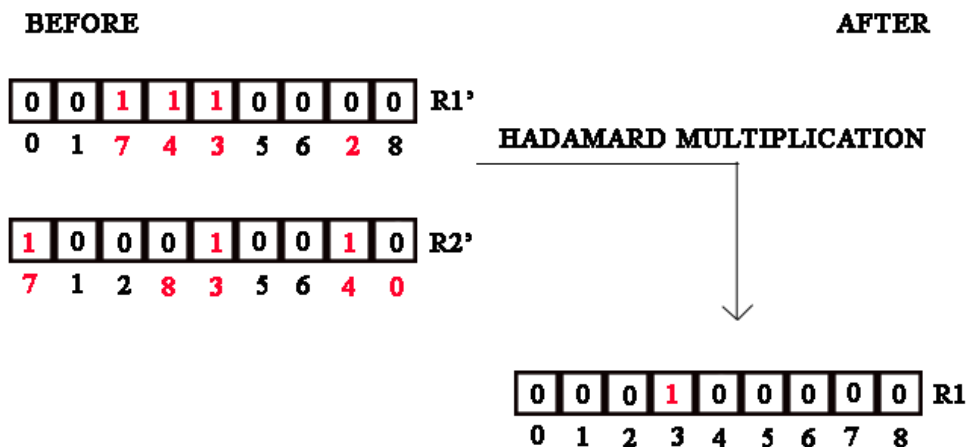


Figure 3.7: Hadamard Multiplication 1

As mention in (Lai et al., 2017), IFO hashing was able to reduce stored information. This occurs during the stage of Hadamard Multiplication and selection of window for first '1' elements that appear. Figure 3.8 shows the situation of how Hadamard Multiplication could achieve such behaviour.

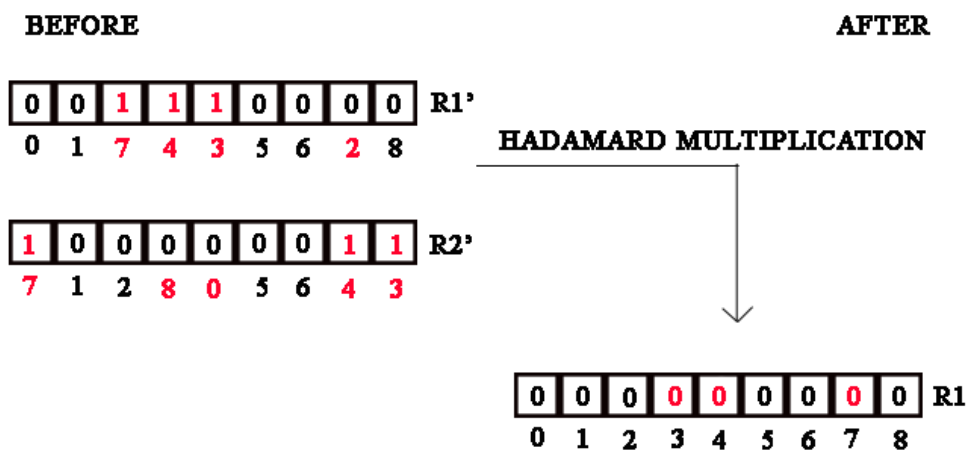


Figure3.8: Hadamard Multiplication 2

The index of the first '1' element that appears in a predefined K window will then be extracted. Based on Figure 3.9 below, it shows the extracted index for assuming the K window of 4. Loss of information can occur at this stage either is affected by the previous Hadamard Multiplication results or the K window size.

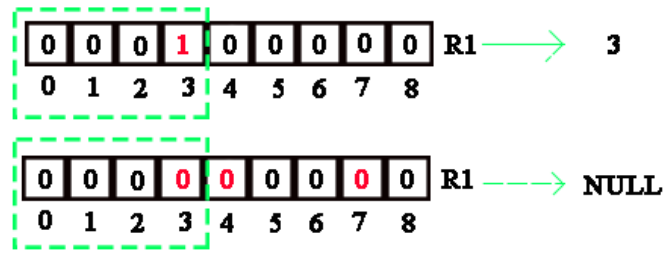


Figure 3.9: Extracting Index when K Window is 4

The last step for IFO hashing is to induce the many to one mapping through the modulo thresholding through the threshold value, τ . For the extracted index, C_X that is larger than the difference between the K window and threshold value, $C_X \geq K - \tau$, $C_X' = C_X \bmod K - \tau$. All the process will then be repeated with different permutation number and all the extracted index that has pass-through modulo threshold will be stored as an IFO Hashed Code.

3.1.4 Key Retrieval

The matching score between the query IFO hashed code, C' and the stored IFO hashed code, C will be denoted as $S(C, C')$. The query input iris code will first have to go through the bloom filter transformation to generate the genuine template. The same IFO hashed group will be applied with the respective permutation to generate a query of hashed code.

An empty array with the same length of the cryptographic key, K will be first generated. Matching will take place to govern by a pre-defined threshold, t . If the $S(C, C') \geq t$, it will fill up the empty array with '1' elements whereas '0' for the situation where $S(C, C') \leq t$. By repeating the process, the final key, K' will be obtained.

Key matching between K and K' will then be carried out to determine whether the query input iris code is authorised personnel or malicious attacker.

3.2 Hill Climbing Attack

According to (Yang et al., 2019), the best entry point for a hill-climbing attack to take place would be the channel between the modules. Figure 3.10 below shows the possible entry point for the proposed scheme.

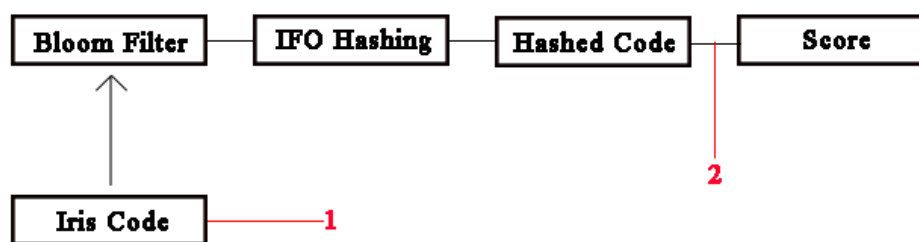


Figure 3.10: Possible Attack Entry Point

To emulate the potential hill-climbing attack on the proposed scheme, the query input of the iris code will be replaced with a synthetic or imposter template. The threshold for the similarity score to regenerate the genuine template is assumed to be known by the malicious attacker and the channel for the similarity score has been compromised and the attacker would be able to know the similarity score based on the synthetic or imposter template.

3.2.1 Rathgeb Method

One of the possible hill-climbing attack approaches that can be implemented would be the method that has been proposed by (Christian Rathgeb and Uhl, 2010) with a slight modification. The CASIA-Iris-Thousand iris database is the iris code that made up with the binary number, which indicates the possible value for a single pixel in the image would be either '1' or '0'.

A random imposter template can be first chosen to feed into the proposed scheme. A $N_1 \times N_2$ smaller window block will then be formed to determine the number of pixels that will be toggle ('1' pixel will toggle to become '0' and vice versa). The similarity score based on the new template will then be tapped into to check for any improvement. In the case where the similarity score improves and move nearer to the threshold, t , the toggle of the pixel in the $N_1 \times N_2$ window block will be retained and the next $N_1 \times N_2$ window block will be going through the same process again.

In the event where the similarity score become worst or remain unchanged, the original value in the $N_1 \times N_2$ window block will remain unchanged. After the first full run on the iris code with modification has been done, in the event where the similarity score is still not able to higher than the

threshold, a new iteration, k will begin with a new starting position, J_n . The new position will base on $J_n = J_1 + x$, where x is a user pre-defined value. The whole hill-climbing attack will be repeated based on the pre-defined k value or whichever the similarity score has already pass through the threshold. Figure 3.11 shows the illustration of the proposed method.

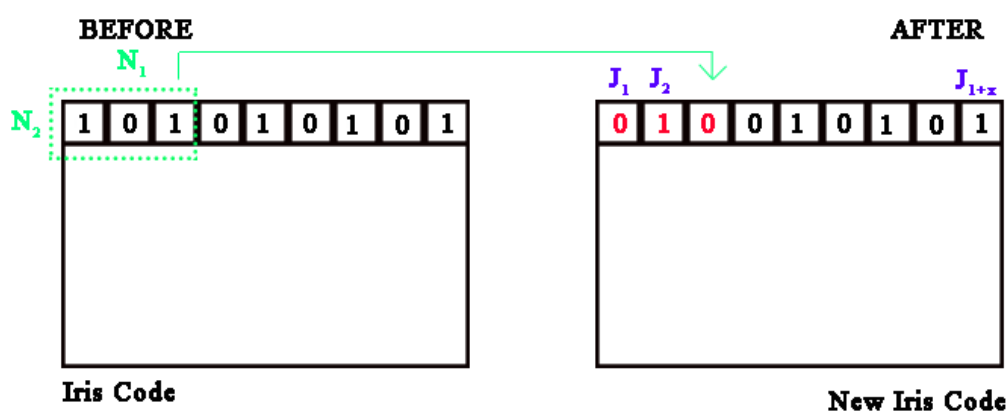


Figure 3.11: Modification of Rathgeb's Hill-Climbing Attack

3.3 Evaluation Metrics

Throughout the experiment, several evaluation metrics were used to determine the performance of the proposed scheme. The most found evaluation metric in this research would be the Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and Decidability.

False Acceptance Rate is defined as the percentage of imposters that were recognised as genuine by the biometric system. In general, FAR shall be minimized to as small as possible as the personnel that was not registered in the system shall not gain access.

On the other hand, the False Rejection Rate is defined as the percentage of genuine users being recognised as the imposter by the biometric system. FRR shall be minimized to as small as possible as well so that the system will not reject the genuine personnel when they were trying to gain access to the system. Genuine Acceptance Rate could be calculated through $100 - \text{FAR}$ as it indicates the percentage of genuine users that could be accepted by the system.

Equal Error Rate is defined as the intersection point where the both FAR and FRR curves were plots on a graph. Therefore, in this context, EER can be calculated by the approximation of $(FAR + FRR)/2$. Decidability on the other ends is the normalized distance between means of the imposter and genuine distributions which could obtain through Equation 3.1 shown below where μ_G represents the mean for genuine score and μ_I for the imposter score.

$$d' = \frac{|\mu_G - \mu_I|}{\sqrt{(\mu_G^2 + \mu_I^2)/2}} \quad (3.1)$$

EER is used to gauge the error rate of the database whereas decidability will be able to give an overview of the trend of the genuine and imposter score. Low EER and high decidability would be the desirable outcome as will indicate the difference between genuine and imposter template is huge and the rate for the system to behave inaccurately is low.

3.4 Work Plan

This research project span through two long semesters. Two detail Gantt Chart has been used to illustrate the timeline for the works has been done throughout this time in Figure 3.12 and Figure 3.13 below.

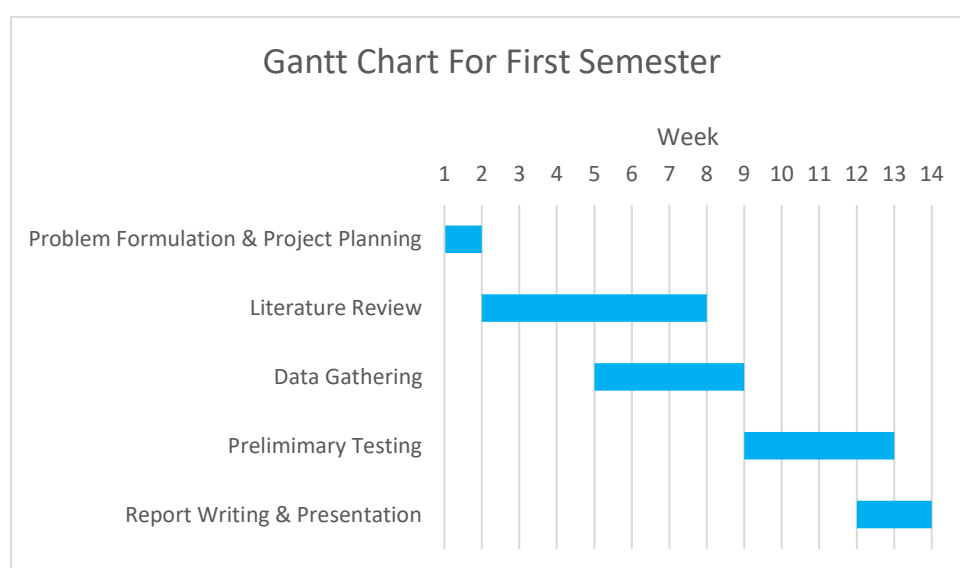


Figure 3.12: Gantt Chart for First Semester

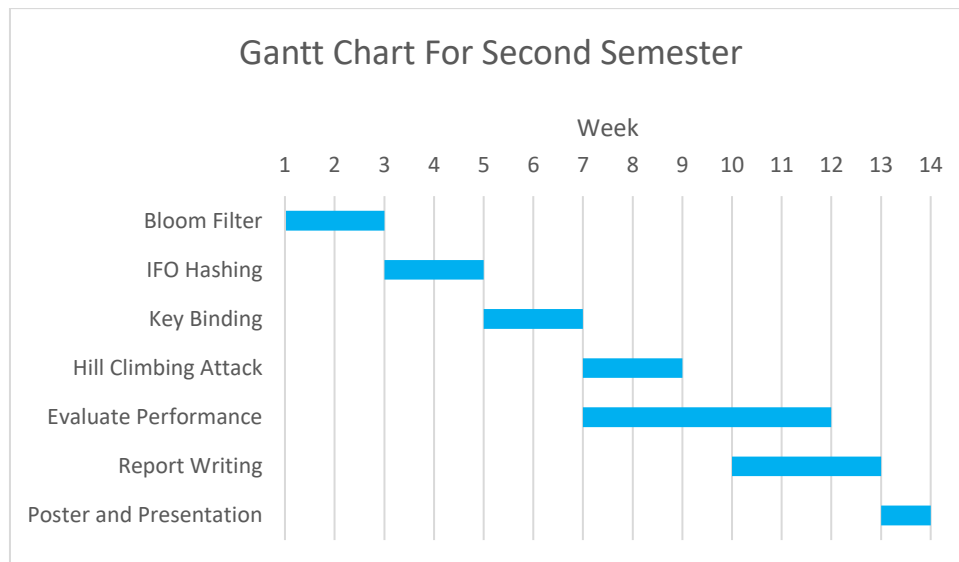


Figure 3.13: Gantt Chart for Second Semester

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Performance Evaluation

A comprehensive analysis of the security and performance of the proposed key binding scheme was conducted on 4 different public iris databases, which include CASIA-v3-interval database, CASIA-Iris-Thousand database, CASIA-v1 database, and ND0405. The difference between these databases is summarised as shown in Table 4.1 below.

Table 4.1: Summary of 4 Different Databases

Characteristics	Databases			
	CASIA-v3-interval	CASIA-v1	CASIA-Iris-Thousand	ND0405
No. of Subjects	249	108	1000	356
No. of Classes	395	108	2000	712
No. of Images	2639	756	20000	64980
Resolution	320*280	320*280	640*480	720*100
Image Quality	Highest	Lowest	Higher	Lower

The example images from the four datasets can be referred to Figure 4.1 below from Left to Right with the sequence following CASIA-v3 interval, CASIA-v1, CASIA-Iris-Thousand and ND0405.

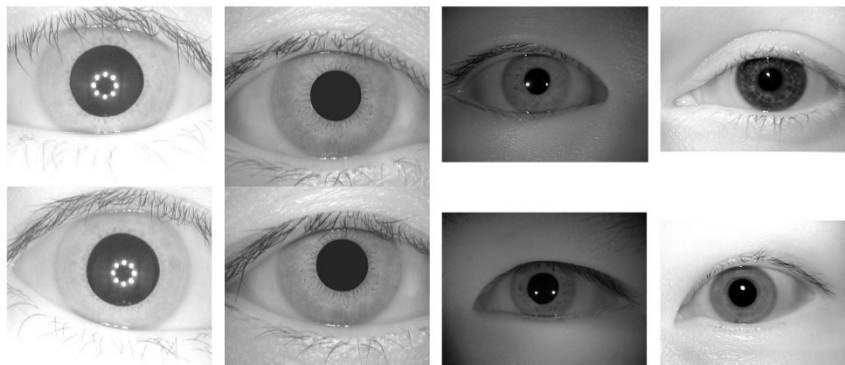


Figure 4.1: Example Image for 4 Different Databases

CASIA-v3-interval (also referred to as CASIA-v3 in this paper) has the clearest iris texture detail among all the databases whereas the remaining would contain the reflection from near-infrared (NIR) illuminator. This was due to the sensors, environment, and methods used to capture the iris image that was different across the 4 different databases.

The attributes of the subject for the database were different as well. Subject from CASIA-v3-interval and CASIA-v1 database are mostly graduate students whereas subjects from CASIA-Iris-Thousand (also referred to as CASIAT in this paper) and ND0405 are having a wide range distribution of ages.

CASIAT is a large database where the 1000 subjects were captured with near-infrared (NIR) wavelength at a close distance (Hu et al., 2017). It was captured by a commercial IKEMB-100 camera. This quality of the database is affected by the specular reflections and the spectacles wearer (Hu et al., 2017).

On the other hands, ND0405 is also a large database where it contains a total of 64980 images that were also taken in NIR wavelength at a close distance (Hu et al., 2017). It was capture by a LG2200 iris imaging system. Both CASIAT and ND0405 database was used to represent the iris data that came from a wide distribution of ages.

ND0405 has a lower quality when compared to CASIAT as the process of capturing was not performed under the ideal scenario. Several different real-work issues can be seen throughout the data set, which includes eyelids occlusion, rotation, blurring and off-angle. (Hu et al., 2017). Not to mention that some of the subjects were wearing contact lens during the capturing process, which would contribute to the distortion of the iris textures.

CASIA-v3 has the best image quality in overall as it used a self-developed close-up camera designed by the Chinese Academy of Sciences (CASIA) where its sole purpose was to capture clear iris images. CASIA-v1 on the other hands was the predecessor for CASIA-v3 where similar approaches have been used but higher intraclass variation contributed by various noise can be observed. Both these databases were used to represent the iris data that came from a rather “controlled” environment.

The experiments were conducted in a way where it will emphasize on the implementation and the security analysis. It does not take the limitation,

potential, and trade-off that might occur in iris biometrics into consideration. For starter, the performance trade-off in terms of Equal Error Rate (ERR) and decidability index upon the implementation of Bloom Filter and IFO Hashing in preserving the system's performance is shown in the following section. The low value of EER would indicate a better performance whereas a high value of decidability index would be preferable as it indicates the normalized distance between the means of the genuine and imposter distributions.

Next, it will follow by an overview of the performance of the proposed key binding scheme through standard metric evaluation. The inter-relation of the three main parameters: similarity threshold (t), cryptographic key length (n), and IFO hashed code length (m) were tested and examined.

4.2 Performance of Bloom Filter Iris Code and IFO Hashing

The experiments were first carried out by testing the bloom filtered iris code and IFO hashing respectively. Taguchi Method was implemented to obtain the parameters, W and L for Bloom Filter generation as well as the various IFO hashing parameters to achieve the optimum performance where it targets to reach the lowest possible EER while maintaining the high decidability. Table A-1, Table A-2, Figure B-1, and Figure B-2 show the examples of tabulation for data that was obtained through the Taguchi Method for CASIA-v3-interval database and CASIA-v1 database. The parameters that were used for the key binding scheme was then tabulated into Table 4.2 below.

Table 4.2: Summary of Parameters used for 4 Different Databases

Parameters	Databases			
	CASIA-v3-interval	CASIA-v1	CASIA-Iris-Thousand	ND0405
Width	7	5	3	3
Length	20	10	3	4
Noise Threshold	-	0.1	0.1	0.1
Number of Permutation	1	1	1	1
K Window	128	32	8	8
Modulo Threshold	0	0	0	0

The inter-relation of the parameters listed in Table 4.2 above was experimented thoroughly through the repetitive trial via manipulating one of the parameters while others remain as a constant. Table A-3 and Table A-4. Shows the tabulated results where the extensive experiment that was performed on the CASIA-v1 database to study its effects.

Throughout the experiment several different matching protocols have been performed, which include genuine and imposter matching. Genuine matching was done by comparing the hamming distance between different iris codes from the same class whereas the imposter matching was done by comparing the hamming distance between different iris codes from a different class, which can be also known as inter-class matching. Since 4 different databases have been used in this experiment, 4 different sets of genuine and imposter matching score will be obtained as the number of the class used were different. The same matching protocols were applied for the rest of the experiment when the process involved genuine and imposter matching.

The comparison between the performance in term of EER and decidability before the Key Binding scheme for 4 difference databases are shown in Table 4.3 below.

Table 4.3: Summary of the Performances for 4 Different Databases

Database	Equal Error Rate, %		Decidability, %	
	Bloom Filter	Ifo Hashing	Bloom Filter	Ifo Hashing
CASIA-v3	1.00	0.66	4.09	3.04
CASIAT	8.11	6.17	2.34	2.52
ND0405	10.74	8.17	2.30	2.56
CASIA-v1	5.91	5.81	2.71	2.77

The result shown in Table 4.3 shows that the system performance did not experience a significant deterioration after the IFO Hashing process.

4.3 Performance of the Proposed Key Binding Method

Extensive experiments were performed on all the databases under different parameters configuration to evaluate the performance of the proposed key binding method. FAR and FRR were the metric that was used to evaluate the performance. As mention in the earlier section, lower FAR and FRR value is much preferable as it indicates a higher system performance.

The protocols to obtain the value for FAR and FRR can be divided into two methods. The first one would be referring to the number of wrongly retrieved key divided by the total genuine matching score to obtain the FAR. The second protocol is referring to the number of correctly retrieved key divided by the total imposter matching score to obtain the FRR.

The retrieval process was done in a way where the intra and inter matching process between the hashed code will generate a string of key depends on the predefined threshold that would be then later compared with the enrolled key in the system to determine the number of correctly and wrongly retrieved key.

4.4 Evaluation of Similarity Score Threshold (t)

The evaluation of the similarity score threshold would require the parameter configuration from Table 4.2 to first generate the hashed code that would be stored in the system. The three main parameters for the overview proposed system (t, n, m) will then be tested with different sets of configurations depends on the set of databases that have been used. Table 4.4 below shows the configuration of fixed parameters n , and m as well as the range for the t that will be evaluate.

Table 4.4: Configurations of Parameters for 4 Different Databases

Databases	Parameters
CASIA-v3	$n = 10, m = 100, t = [0.17, 0.18, \dots, 0.26]$
CASIA-v1	$n = 10, m = 250, t = [0.22, 0.23, \dots, 0.31]$
CASIAT	$n = 10, m = 050, t = [0.56, 0.57, \dots, 0.65]$
ND0405	$n = 10, m = 050, t = [0.58, 0.59, \dots, 0.67]$

The results in terms of FAR and FRR as well as the calculated EER for every t across the 4 databases obtained through the genuine and imposter matching process are tabulated in Table 4.5, Table 4.6, Table 4.7, and Table 4.8 below.

Table 4.5: System Performance for Parameter Set $(t, 10, 100)$ on CASIA-v3-interval

t	FRR (%)	FAR (%)	EER (%)
0.17	0.19	10.27	5.23
0.18	0.27	2.65	1.46
0.19	0.69	0.55	0.62
0.20	1.92	0.09	1.01
0.21	2.92	0.00	1.46
0.22	4.16	0.00	2.08
0.23	6.61	0.00	3.30
0.24	9.02	0.00	4.51
0.25	12.40	0.00	6.20
0.26	16.36	0.00	8.18

Table 4.6: System Performance for Parameter Set $(t, 10, 250)$ on CASIA-v1

t	FRR (%)	FAR (%)	EER (%)
0.22	9.74	0.82	5.28
0.23	15.52	0.41	7.97
0.24	23.05	0.24	11.65
0.25	32.00	0.16	16.08
0.26	39.81	0.00	19.90
0.27	47.14	0.00	23.57
0.28	54.29	0.00	27.14
0.29	62.48	0.00	31.24
0.30	69.52	0.00	34.76
0.31	76.86	0.00	38.43

Table 4.7: System Performance for Parameter Set ($t, 10,50$) on CASIA-Iris

Thousand

t	FRR (%)	FAR (%)	EER (%)
0.56	4.63	14.92	9.78
0.57	9.54	5.40	7.47
0.58	15.17	1.43	8.30
0.59	21.53	0.16	10.84
0.60	30.97	0.00	15.49
0.61	41.14	0.00	20.57
0.62	50.59	0.00	25.30
0.63	58.13	0.00	29.06
0.64	65.67	0.00	32.83
0.65	72.66	0.00	36.33

Table 4.8: System Performance for Parameter Set ($t, 10,50$) on ND0405

t	FRR (%)	FAR (%)	EER (%)
0.58	9.51	3.52	6.51
0.59	13.81	0.95	7.38
0.60	19.72	0.28	10.00
0.61	25.29	0.04	12.66
0.62	32.49	0.00	16.25
0.63	39.73	0.00	19.87
0.64	48.12	0.00	24.06
0.65	56.29	0.00	28.15
0.66	64.76	0.00	32.38
0.67	71.30	0.00	35.65

Based on the results tabulated in Table 4.5 to Table 4.8, the best EER from each of the databases did not experience significant deterioration after the key binding process. Table 4.9 below shows the comparison between the best EER across 4 databases prior and after the key binding process.

Table 4.9: Overview Comparison of Best EER across 4 Database

Database	Equal Error Rate, %	
	I/O Hashing	Key Binding
CASIA-v3	0.66	0.62
CASIAT	6.17	7.47
ND0405	8.17	6.51
CASIA-v1	5.81	5.28

However, in order to have a cryptosystem that is useful, the FAR shall remain zero, so that the system itself will not allow any unauthorised access by the imposter, thus increasing the system security. The best EER shown in Table 4.9 above does not yield the results of FAR= 0, therefore the value for the threshold to be selected shall be the one that first yields the results of FAR= 0. The suitable threshold for all the databases is tabulated into Table 4.10 below.

Table 4.10: Similarity Score Threshold for all the Database

Databases	Parameters
CASIA-v3	$t = 0.21$
CASIA-v1	$t = 0.26$
CASIAT	$t = 0.60$
ND0405	$t = 0.62$

The selected value for the parameters in Table 4.10 above can be further justified by Figure 4.1 below where it was plotted based on the genuine and imposter matching score. According to the zoomed region shown in Figure 4.2, the best threshold value to be select for t that will successfully block any unauthorised access for the CASIA-v3-interval database would be 0.21. Therefore, the value chosen for the parameters from the graph itself is tally with the data that has been tabulated in Table 4.5 where it shows the value of FAR is equivalent to 0 when the threshold was set to be 0.21.

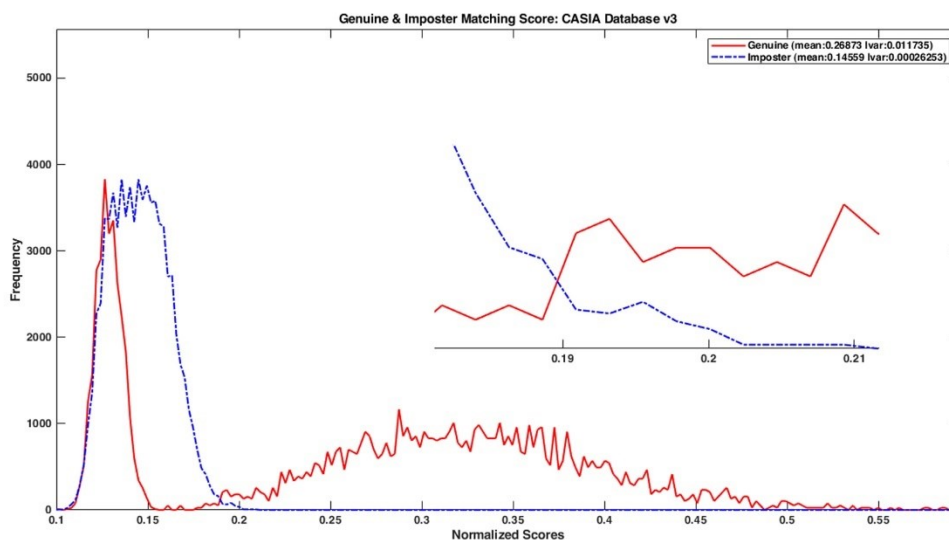


Figure 4.2: Genuine and Imposter Matching Score for CASIA-v3-interval

Aside from the justification, it can be observed that there was an overlapping region between the genuine and imposter matching score. This was due to the imposter synthetic template matched with the imposter template, which results in the system will recognize it as a genuine query. This is useful for the proposed system as it will be able to conceal the true genuine IFO hashed code from the potential malicious attacker if they were able to tap into the system database. The graph for the genuine and imposter matching score for the remaining database can be referred to Figure B-3, Figure B-4, and Figure B-5.

4.5 Evaluation of Cryptographic Key Length (n)

The evaluation of cryptographic key length would require the parameter configuration from Table 4.2 to first generate the hashed code that would be stored in the system. Table 4.11 below shows the configuration of fixed parameters t , and m as well as the range for the n that will be evaluate.

Table 4.11: Configurations of Parameters for 4 Different Databases

Databases	Parameters
CASIA-v3	$m = 100, t = 0.21, n = [10, 20, 40, 60, 80, 100, 150, 200]$
CASIA-v1	$m = 250, t = 0.26, n = [10, 20, 40, 60, 80, 100, 150, 200]$
CASIAT	$m = 050, t = 0.60, n = [10, 20, 40, 60, 80, 100, 150, 200]$
ND0405	$m = 050, t = 0.62, n = [10, 20, 40, 60, 80, 100, 150, 200]$

The results in terms of FAR as well as the calculated Genuine Acceptance Rate, $GAR = 100 - FRR$, and EER for every n across the 4 databases obtained through the genuine and imposter matching process are tabulated in Table 4.12 below. Format of the tabulated data follows the sequence/format of CASIA-v3/ CASIA-v1/ CASIAT/ ND0405.

Table 4.12: Configurations of Parameters for 4 Different Databases

n	GAR (%)	FAR (%)	EER (%)
10	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
20	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
40	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
60	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
80	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
100	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
150	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25
200	97.08/60.19/69.03/67.51	0/0/0/0	1.46/19.91/15.49/16.25

Based on Table 4.12 above, it can be observed that the increase of key length will not cause the performance of the system to deteriorate across 4 different databases. Thus, the proposed key binding scheme has the advantage where it could increase the length of the cryptographic key for security yet still maintain the system's performance at the same time.

4.6 Evaluation of Hashed Code Length (m)

The evaluation of hashed code length would require the parameters configuration from Table 4.2 to first generate the hashed code that would be stored in the system. Table 4.13 below shows the configuration of fixed parameters t , and n as well as the range for the m that will be evaluate.

Table 4.13: Configurations of Parameters for 4 Different Databases

Databases	Parameters
CASIA-v3	$n = 10, t = 0.22, m = [10, 50, 100, 150, 200, 250, 300]$
CASIA-v1	$n = 10, t = 0.26, m = [10, 50, 100, 150, 200, 250, 300]$
CASIAT	$n = 10, t = 0.60, m = [10, 50, 100, 150, 200, 250, 300]$
ND0405	$n = 10, t = 0.62, m = [10, 50, 100, 150, 200, 250, 300]$

The results in term of FAR and FRR was recorded and the corresponding GAR, EER, and storage per bit kB/n were computed and tabulated into Table 4.14, Table 4.15, Table 4.16 and Table 4.17 below.

Table 4.14: System Performance for Parameter Set (0.21,10, m) on CASIA-v3-interval

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/n)
10	95.31	0.25	2.47	0.07
50	95.58	0.00	2.21	0.68
100	95.84	0.00	2.08	1.71
150	95.97	0.00	2.02	3.31
200	95.97	0.00	2.02	4.54
250	95.85	0.00	2.07	5.66
300	95.89	0.00	2.05	6.80

Table 4.15: System Performance for Parameter Set (0.26,10, m) on CASIA-v1

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/n)
10	53.05	0.00	23.48	0.50
50	61.14	0.16	19.51	4.20
100	59.62	0.00	20.19	8.50
150	59.43	0.00	20.29	12.60
200	61.33	0.00	19.33	16.80
250	60.19	0.00	19.91	20.80
300	59.52	0.00	20.24	25.00

Table 4.16: System Performance for Parameter Set (0.60,10, m) on CASIA-Iris-Thousands

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/n)
10	74.39	0.16	12.89	19.70
50	69.03	0.00	15.49	98.50
100	65.30	0.00	17.35	194.00
150	60.22	0.00	19.89	293.00
200	54.50	0.00	22.75	394.00
250	57.95	0.00	21.03	494.00
300	58.58	0.00	20.71	604.00

Table 4.17: System Performance for Parameter Set (0.62,10, m) on ND0405

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/n)
10	68.77	0.02	15.62	14.60
50	67.51	0.00	16.25	72.20
100	62.42	0.00	18.79	143.00
150	58.30	0.00	20.85	217.00
200	53.62	0.00	23.19	292.00
250	55.25	0.00	22.37	364.00
300	54.85	0.00	22.58	438.00

The IFO hashed code length plays an important role where it comes to system storage. Aside from affecting the performances of the systems, the IFO hashed code length has to be kept within an acceptable length as it will take up infinite storage space if there was not any limit. Based on Table 4.14-Table4.17, it can be observed that the increment of the hashed code has various impacts on system performance. For CASIA-v3 that has the best iris texture, the impact of the performance was not that significant to compare to the other 3 databased that contain noise. However, all of these share the same trend, which is the increase of hashed code length will increase the storage per bit.

4.7 Security Analysis

The security for the proposed key binding scheme will be evaluated through 2 different aspect, which is the cancelability and potential security attacks that might face by the proposed system.

4.7.1 Renewal and Cancelability

During the occurrence of the event where the current cryptographic key has been compromised, a new key shall be reissued for the security purpose. One of the advantages contributes by the proposed system was that no re-enrolment of any data is required during this process. The update can be done merely by swapping the position of the genuine and synthetic template with their corresponding hashed code. The process of regenerating a new cryptographic key is fast and simple for this proposed method.

Moving on to the aspect of the cancelability, the regeneration of the cancellable template is guaranteed by the unlikability and revocability of the IFO Hashing Scheme (Chai et al., 2019). Referring to the thorough security analysis that can be found in Lai et al paper, it has proven that the derivation of original biometric information from the IFO hashed code is computationally infeasible (Lai et al., 2017). In his paper, various comprehensive analysis supported by the empirical data has proven that the IFO hashing scheme will be able to satisfy both the unlikability and revocability criteria, which results in the implementation of IFO hashing in the proposed key binding methods is suitable.

4.7.2 Brute Force Attack

In order to perform a brute force attack toward the proposed key binding system, it relies on the random guessing for the n bits cryptographic key without actually have to intercept the process in between the proposed system. Thus, the complexity of the attack is merely depending on the cryptographic key length itself, which is the parameter n in the proposed system. The complexity of the brute force attack can be simplified into Equation 4.1 as shown below.

$$Bf_n = 2^n \quad (4.1)$$

The higher the value for n will result in a higher complexity as it would require more cancellable template (hashed code) to be bound with during the key binding process. For example, brute force attack complexity would be 2^{200} if the length of the cryptographic key was 200.

Based on Table 4.12 above, it shows that the performance of the proposed system will not experience any deterioration when the cryptographic key length was up to until 200. Therefore, the proposed method provides flexibility in terms of allowing the user to decide the complexity of the system without having to worry about the performance of the system.

4.7.3 Hill Climbing Attack

Apart from the brute force attack, another attack that has to be taken into consideration was the hill-climbing attack. In conjunction with the brute force attack, a hill-climbing attack requires an interception of information from the system itself. Instead of guessing randomly, the hill-climbing attack will penetrate the system by proposing a synthetic template that will keep on improving after each attack. In this experiment, the number of the trial is limited to the resolution of the iris code. The proposed hill-climbing attack was designed as follows:

1. The threshold for the IFO hashed code using the genuine matching protocol was first recorded.
2. The objectives of this attack were to improve the synthetic template until a point where after it undergoes the genuine matching protocol and will be able to trick the system by achieving the pre-recorded threshold.
3. The number of attacks will be depending on the resolution of the IFO hashed code as the improvement of the synthetic template was performed by a bitwise operator.

Throughout several comprehensive trials, the hill-climbing attack will not be able to penetrate the proposed system. This is due to the many-to-one mapping that was induced in the proposed key binding system during the bloom filter process. The bitwise operator that changes the bits of the synthetic

template was not able to create a drastic impact on the genuineness of the synthetic template.

The validity of the many to one function can be further proven by the inverse function from the bloom filtered iris code are not able to be constructed as it would violate the definition of many to one mapping as discussed earlier.

Hill climbing attack is a method where it can be interrupted at any time, in a sense that it can be run for infinite time unless a stopping criterion has been predefined or else it would be only returning “the best result so far” that it was able to achieve. The hill-climbing method might not be able to provide absolute best results, as it yet to reach the global maximum. Thus, it only makes sense that the complexity for the hill-climbing attack shall be measure in time, which yields the Equation 4.2 as shown below.

$$HCAf_n = \infty \quad (4.2)$$

Given the high resolution of the iris code from the various database, it was infeasible for a hill-climbing attack to occur as the time needed for it to run is up to infinite as the loss of information will keep on occurring during the many to one mapping. Eventually, the threshold for the synthetic template will not be able to converge toward the actual genuine threshold.

4.8 Summary

Based on the experiments that have been done for 4 different databases, it has been compiled together into Table 4.18 below.

Table 4.18: Summary Results for 4 Different Databases

Database	GAR (%)	FAR (%)	Keybits
CASIA-v3	97.08	0	100
CASIA-v1	60.19	0	250
CASIAT	69.03	0	50
ND0405	67.51	0	50

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

Based on the tabulated results, it shows that the implementation of IFO hashing would allow the user to control the storage size while at the same time achieve the unlikability and non-invertibility requirements. The best performance of GAR=97.08% can be achieved with the CASIA-v3 database. The results for the database that is not that high-quality fall between the range of GAR= 60.19-69.03%. However, it is important to understand the degrade of performance was caused by the trade-off between performance and strength of the security. This was proven by the best EER after the key binding process did not undergo much deteriorate as compare to the EER right after IFO hashing.

In terms of the strength of the security, it has proven that the proposed key length will not induce any trade-off between performance and security. It has shown a promising complexity up to 2^{200} across 4 various databases. It was also proven that the occurrence of a hill-climbing attack will not compromise the proposed methods as it would have the complexity up to infinite and the many to one mapping function will have reduced the impact of the changes that have been made during each iteration.

5.2 Recommendations for Future Work

Based on the drawn conclusion, the degradation of performance when it comes to the database that is not that high quality is highly affecting the trade-off between the performance and strength of the security. To fully study the performance of the proposed method, a more recent database with better quality shall be used.

REFERENCES

- Ali, M.A.M. and Tahir, N.M., 2018. Cancelable biometrics technique for iris recognition. *ISCAIE 2018 - 2018 IEEE Symposium on Computer Applications and Industrial Electronics*. 2018 IEEE, pp. 434–437.
- Bringer, J., Morel, C. and Rathgeb, C., 2015. Security analysis of Bloom filter-based iris biometric template protection. *Proceedings of 2015 International Conference on Biometrics, ICB 2015*, pp.527–534.
- Chai, T.Y., Goi, B.M., Tay, Y.H. and Jin, Z., 2019. A new design for alignment-free chaffed cancelable iris key binding scheme. *Symmetry*, 11(2).
- Choudhury, B. et al., 2017. Cancelable iris Biometrics based on data hiding schemes. *Proceedings - 14th IEEE Student Conference on Research and Development: Advancing Technology for Humanity, SCOReD 2016*. 2017 IEEE, pp. 1–6.
- Daugman, J., 2004. How Iris Recognition Works. *The Essential Guide to Image Processing*, 14(1), pp.21–30.
- Eng, A. and Wahsheh, L.A., 2013. Look into my eyes: A survey of biometric security. *Proceedings of the 2013 10th International Conference on Information Technology: New Generations, ITNG 2013*, pp.422–427.
- Hao, F., Anderson, R. and Daugman, J., 2006. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*, 55(9), pp.1081–1088.
- Hu, Y., Sirlantzis, K. and Howells, G., 2017. Optimal Generation of Iris Codes for Iris Recognition. *IEEE Transactions on Information Forensics and Security*, 12(1), pp.157–171.
- International Organization for Standardization, 2017. Information technology — Vocabulary — Part 37: Biometrics.
- Kaudki, O. and Bhurchandi, K., 2018. A Robust Iris Recognition Approach Using Fuzzy Edge Processing Technique. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp.1–6. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8493855>.
- Kelkboom, E.J.C. et al., 2011. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1), pp.107–121.

Lai, Y.L. et al., 2017. Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognition*, 64(November 2016), pp.105–117. Available at: <http://dx.doi.org/10.1016/j.patcog.2016.10.035>.

Lee, Y.J. et al., 2008. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 38(5), pp.1302–1313.

Li, P. et al., 2010. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications*, 33(3), pp.207–220. Available at: <http://dx.doi.org/10.1016/j.jnca.2009.12.003>.

Maiorana, E., Hine, G.E. and Campisi, P., 2015. Hill-climbing attacks on multibiometrics recognition systems. *IEEE Transactions on Information Forensics and Security*, 10(5), pp.900–915.

Mennink, B. et al., 2014. When a Bloom Filter is a Doom Filter: Security Assessment of a Novel Iris Biometric Template Protection System. *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*. 2014 Gesellschaft für Informatik e.V. - GI., p. 3001.

Nagar, A., Nandakumar, K. and Jain, A.K., 2012. Multibiometric cryptosystems based on feature-level fusion. *IEEE Transactions on Information Forensics and Security*, 7(1), pp.255–268.

Nazmdeh, V. et al., 2019. Iris recognition; From classic to modern approaches. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, pp.981–988.

Pawar, H.R. and Harkut, D.G., 2018. Classical and Quantum Cryptography for Image Encryption Decryption. *Proceedings of the 2018 3rd IEEE International Conference on Research in Intelligent and Computing in Engineering, RICE 2018*, pp.1–4.

Phillips, P.J. et al., 2008. The iris challenge evaluation 2005. *BTAS 2008 - IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems*.

Ratha, N.K., Chikkerur, S., Connell, J.H. and Bolle, R.M., 2007. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), pp.561–572.

Rathgeb, C., Breiting, F. and Busch, C., 2013. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. *Proceedings - 2013 International Conference on Biometrics, ICB 2013*. 2013 IEEE, pp. 1–8.

Rathgeb, C. and Uhl, A., 2011a. A Survey on Biometric Cryptosystems. , pp.1–

25.

Rathgeb, C. and Uhl, A., 2010. Adaptive fuzzy commitment scheme based on iris-code error analysis. *2010 2nd European Workshop on Visual Information Processing, EUVIP2010*, pp.41–44.

Rathgeb, Christian and Uhl, A., 2010. Attacking iris recognition: An efficient hill-climbing technique. *Proceedings - International Conference on Pattern Recognition*, pp.1217–1220.

Rathgeb, C. and Uhl, A., 2011b. Statistical attack against iris-biometric fuzzy commitment schemes. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp.23–30.

Del Río, J.S. et al., 2015. Face-based recognition systems in the ABC e-gates. *9th Annual IEEE International Systems Conference, SysCon 2015 - Proceedings*, pp.340–346.

Yang, W., Wang, S., Hu, J. and Zheng, G., 2019. SS Security and Accuracy of Fingerprint-Based Biometrics : A Review. *Symmetry*.

Zuo, J., Ratha, N.K. and Connell, J.H., 2008. Cancelable iris biometric. *Proceedings - International Conference on Pattern Recognition*, (December).

APPENDICES

APPENDIX A: Table

Table A-1: Taguchi Method for CASIA-v3-interval Database

Gvm	L	W	G	GAR	FAR	FRR	Decidability
50	5	20	1	98.81	1.19	1.19	3.59233
50	7	25	2	98.04	1.42	1.52	3.02762
100	5	20	2	98.76	1.23	1.24	3.19449
100	7	25	1	99.15	0.84	0.85	3.63363
150	5	25	1	99.06	0.92	0.94	3.69628
150	7	20	2	99.04	0.96	0.96	3.00624
200	5	25	2	99.08	0.92	0.92	3.31572
200	7	20	1	99.29	0.73	0.71	3.57648
Optimum Parameters							
200	5	25	1	98.97	1.04	1.03	3.69253

Table A-2: Taguchi Method for CASIA-v1 database

L	W	GVM	G	K	S	GAR	FAR	FRR	Decidability
5	5	10	1	2	0	85.63	14.29	14.37	2.12256
5	10	50	2	4	1	80.18	19.81	19.82	1.52657
5	14	100	3	8	2	69.34	30.86	30.65	0.89498
5	16	150	4	16	3	60.97	39.24	39.03	0.50945
5	20	200	5	32	4	57.76	42.38	42.23	0.32738
6	5	50	3	16	4	51.45	44.29	48.52	0.13456
6	10	100	4	32	0	54.54	44.48	45.46	0.24929
6	14	150	5	2	1	63.04	66.48	36.96	0.00924
6	16	200	1	4	2	90.97	8.95	9.03	2.62891
6	20	10	2	8	3	71.92	28.10	28.08	1.06512
7	5	100	5	4	3	0.00	0.00	0.00	0.00000
7	10	150	1	8	4	91.26	8.76	8.70	2.57426
7	14	200	2	16	0	72.31	28.00	27.69	1.05943
7	16	10	3	32	1	51.47	48.10	48.53	0.08279
7	20	50	4	2	2	51.72	49.43	48.28	0.02514
8	5	150	2	32	2	57.61	39.14	42.36	0.42564
8	10	200	3	2	3	0.00	0.00	0.00	0.00000
8	14	10	4	4	4	0.07	0.29	99.93	0.04945
8	16	50	5	8	0	0.00	0.00	0.00	0.00000
8	20	100	1	16	1	88.60	11.43	11.40	2.30545
9	5	200	4	8	1	0.00	0.00	0.00	0.00000
9	10	10	5	16	2	0.00	0.00	0.00	0.00000
9	14	50	1	32	3	87.51	12.48	12.49	2.07737
9	16	100	2	2	4	54.42	54.86	45.52	0.02421
9	20	150	3	4	0	42.34	42.57	57.92	0.00000
Optimum Parameters									
5	10	200	1	8	2	93.46	6.57	6.54	2.76486

Table A-3: Bloom Filter for CASIA-v1 database

L	W	Noise Threshold	GAR	FAR	FRR	EER	Decidability
5	10	0.00	93.89	6.10	6.11	6.10	2.77264
5	10	0.10	94.04	6.00	5.96	5.98	2.76436
5	10	0.25	94.00	6.00	6.00	6.00	2.72416
5	10	0.30	94.09	5.90	5.91	5.91	2.70747
5	10	1.00	91.72	8.29	8.28	8.28	2.31952
1	10	0.30	65.97	33.81	34.03	33.92	0.77828
2	10	0.30	88.16	11.81	11.84	11.82	2.28548
3	10	0.30	92.50	7.52	7.50	7.51	2.61653
4	10	0.30	92.94	7.05	7.05	7.05	2.65920
5	10	0.30	94.09	5.90	5.91	5.91	2.70747
6	10	0.30	93.92	6.10	6.08	6.09	2.70400
7	10	0.30	93.60	6.38	6.40	6.39	2.66420
8	10	0.30	93.66	6.29	6.34	6.31	2.59115
9	10	0.30	93.51	6.48	6.49	6.49	2.49636
10	10	0.30	93.19	6.67	6.81	6.74	2.39994
5	1	0.30	91.99	8.00	8.01	8.01	2.27715
5	2	0.30	92.60	7.43	7.40	7.41	2.42917
5	3	0.30	93.09	6.95	6.91	6.93	2.46910
5	4	0.30	93.03	6.95	6.97	6.96	2.50490
5	5	0.30	93.18	6.86	6.82	6.84	2.55493
5	6	0.30	93.11	6.86	6.89	6.87	2.60213
5	7	0.30	92.92	7.05	7.08	7.06	2.60075
5	8	0.30	93.49	6.48	6.51	6.49	2.65317
5	9	0.30	93.56	6.38	6.44	6.41	2.67530
5	10	0.30	94.09	5.90	5.91	5.91	2.70747
5	11	0.30	92.81	7.24	7.19	7.21	2.67969

Table A-4: IFO Hashing for CASIA-v1 database

L	W	Noise Threshold	GVM	G	K	S	GAR	EER	Decidability
5	10	0.3	200	1	8.00	2.00	93.53	6.47	2.70953
5	10	0.3	200	2	8.00	2.00	82.53	17.50	1.71598
5	10	0.3	200	3	8.00	2.00	70.17	29.91	0.91694
5	10	0.3	200	1	8.00	2.00	93.53	6.47	2.70953
5	10	0.3	200	1	16.00	2.00	63.65	6.36	2.71677
5	10	0.3	200	1	24.00	2.00	93.70	6.29	2.71973
5	10	0.3	200	1	32.00	2.00	93.71	6.29	2.72108
5	10	0.3	200	1	32.00	0.00	93.73	6.28	2.72115
5	10	0.3	200	1	32.00	1.00	93.72	6.28	2.72120
5	10	0.3	200	1	32.00	2.00	93.71	6.29	2.72108
5	10	0.3	200	1	32.00	3.00	93.75	6.27	2.72100
5	10	0.3	200	1	32.00	4.00	93.73	6.28	2.72106
5	10	0.3	50	1	32.00	3.00	93.36	6.60	2.70060
5	10	0.3	100	1	32.00	3.00	93.44	6.56	2.70112
5	10	0.3	150	1	32.00	3.00	93.74	6.27	2.71564
5	10	0.3	200	1	32.00	3.00	93.75	6.27	2.72100
5	10	0.3	250	1	32.00	3.00	93.92	6.09	2.72080
5	10	0.3	300	1	32.00	3.00	94.10	5.90	2.72126
5	10	0.1	250	1	32.00	0.00	94.19	5.81	2.77229

APPENDIX B: Figures



Figure B-1: Taguchi Method for CASIA-v3-interval Database

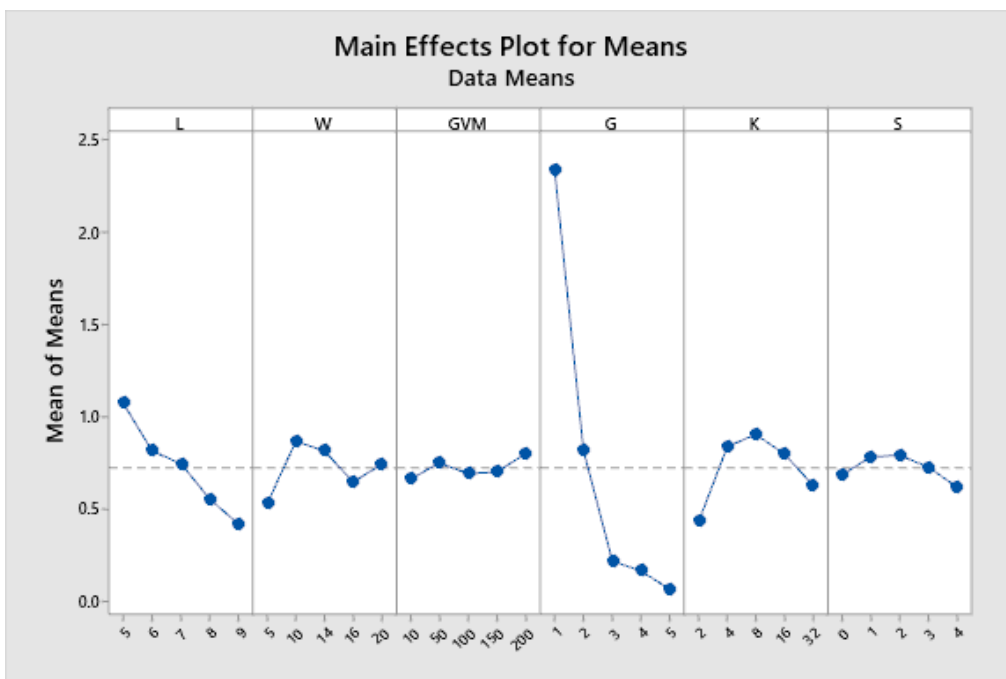


Figure B-2: Taguchi Method for CASIA-v1 database

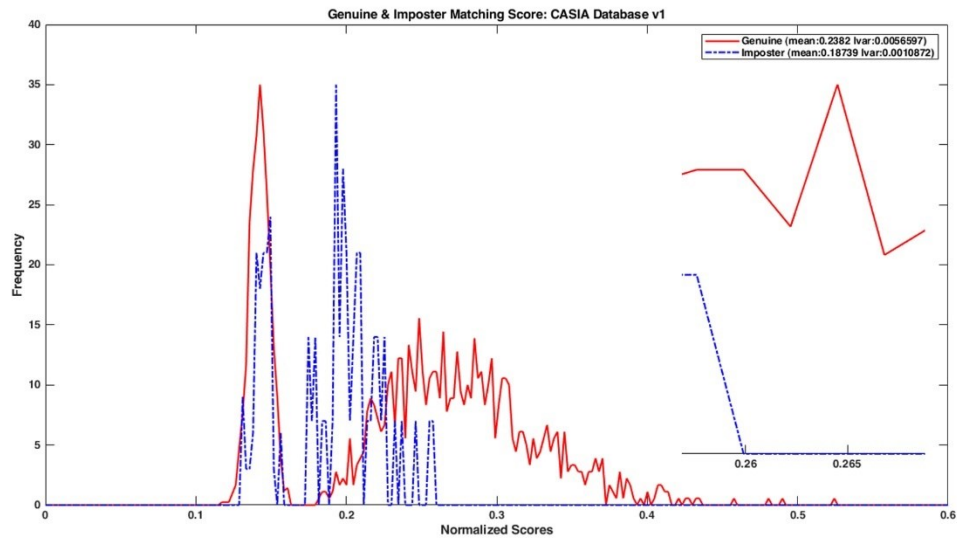


Figure B-3: Genuine and Imposter Matching for CASIA-v1 database

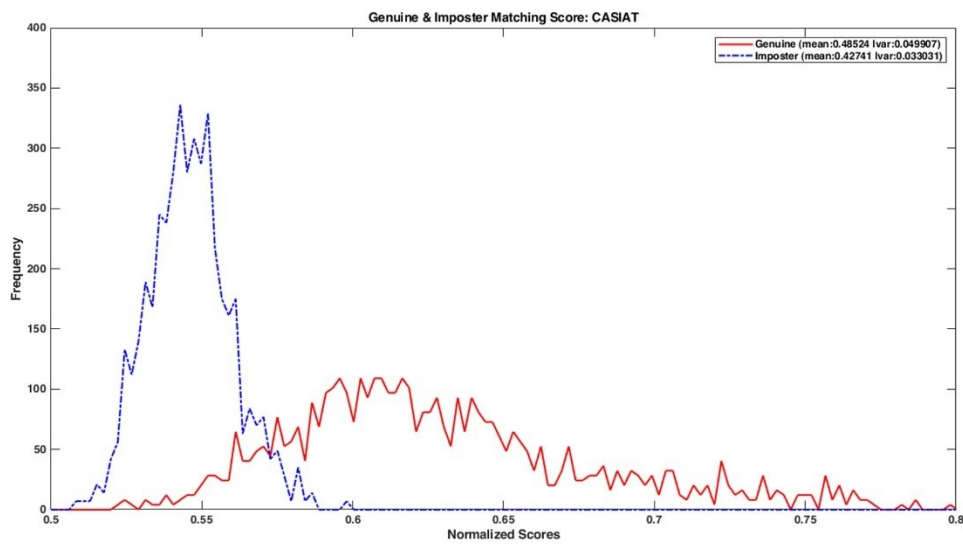


Figure B-4: Genuine and Imposter Matching for CASIA-Iris-Thousands

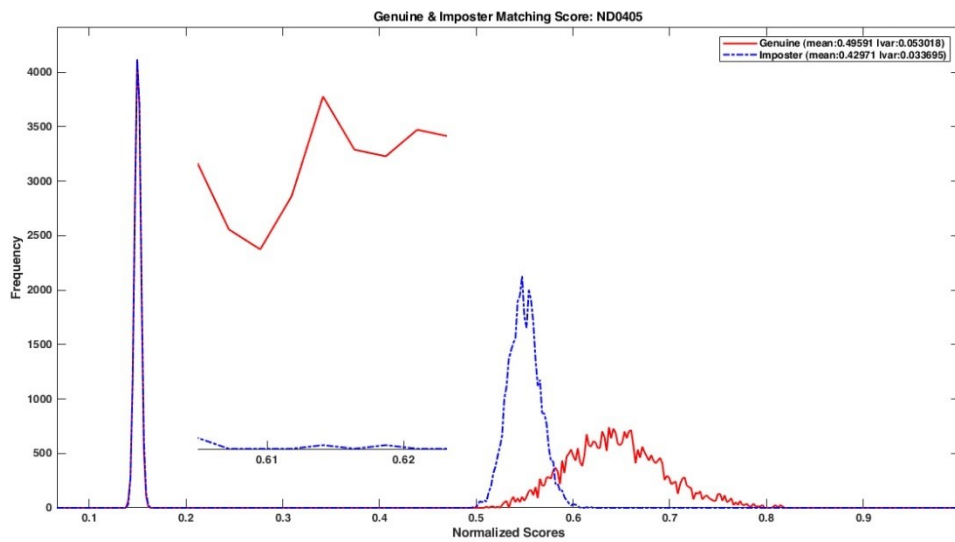


Figure B-4: Genuine and Imposter Matching for ND0405