國立臺灣大學管理學院資訊管理研究所

碩士論文

Graduate Institute of Information Management

College of Management

National Taiwan University

Master Thesis

基於雙重門檻決策的循序型多重生物辨識認證系統

A Serial Multi-modal Biometrics Authentication System Based on Double Threshold Decisions

鄭立民

Li-Min Zheng

指導教授：林永松　博士

Advisor: Frank Yeong-Sung Lin, Ph.D.

中華民國 105 年 1 月

January, 2016

謝誌

從進入研究所，懵懵懂懂地學習如何做研究，到完成論文的這兩年來，面臨各式各樣的困難與挑戰，也受到很多人的支持與鼓勵。對那些幫助過我的父母、兄姊、口試委員、研究所的各位同儕，在此獻上我十二萬分衷心的感謝。將此論文獻給所有曾幫助我的人，尤其是我的父母與指導教授。

首先要感謝我的家人。我是家中的老么，也是唯一念到研究所的。父母對我有所期望，供應學費讓我唸研究所，以及在半夜挑燈夜戰時，為我準備的每一杯咖啡還有聽我遭遇挫折時忍不住的碎念，對於家人的感謝，為人兒女的，無法用區區文字表達。還有兄姊一路上的關愛與支持，紓解我一路上不少的壓力。

再來最要感謝的是我的指導教授—林永松教授，在我的論文題目以及解題技巧上給予大大的啟發，可以說沒有教授就沒有今日我的與我的論文。不得不佩服我深思好幾個禮拜都不得其解的問題，在教授手上就如庖丁解牛一樣簡單。但願未來能成為像教授一樣具有如此學術風範的人士，無論是多年來學術的經驗與知識，以及其謙卑的態度與研究精神，著實令小弟我萬分的欽佩與感激。

論文得以完善，必須感謝撥空來參加我的論文口試給予寶貴建議的委員們。包括台大資管系孔令傑教授、台北大學資工系莊東穎教授、輔仁大學資工系呂俊賢教授以及台灣科技大學電機系鍾順平教授。感謝各位教授對論文的建議以及各種細節上的修改與修正，能夠順利完成這份論文，各位教授功不可沒。

最後要感謝研究所的學長姊、同儕們以及學弟妹，尤其是博班的猶順學長以及邱漢學長對於論文上的指點，還有一路上互相扶持，一起歡笑，互相吐苦水的家榮、鈺雯還有燕芬，沒有這群好夥伴我是不可能走到今天的。研究所台大資管各位幫助過我的同仁，族繁不及備載，也在此獻上我十二萬分的感謝。

鄭立民 謹識

民國一零五年一月

于國立台灣大學資訊管理研究所

論文摘要

論文題目：基於雙重門檻決策的循序型多重生物辨識認證系統

作者：鄭立民

指導教授：林永松 博士

資訊安全近年成為企業組織十分重視之領域，透過網路處理任何資料型態，不論是結構化或是非結構化，log 紀錄檔、照片、聲音、通訊紀錄或是電子郵件，包括使用者之隱私資訊，對該資訊之保護更是不可忽略。隱私資訊被竊取或濫用，對於商譽等無形資產之損害更是難以想像。例如：iCloud 的名人照片被駭客攻擊竊取之事件，暴露出一般身份驗證機制不足，但是蘋果手機 iPhone 5s 以上其實已具備了多重辨識技術服務，包括人臉辨識、語音辨識、指紋辨識、或鍵盤輸入間隙辨識等生物認證技術，只是沒有一個良好生物辨識技術得以將其整合應用，故本研究為了貼近實際應用，擬提出多輪迴方式驗證方式，透過使用多重辨識技術融合(如帳號、密碼 、指紋 、瞳孔及人臉)之特徵值驗證防範不當連線。設計最佳化演算法達成一個高準確率及低誤判率的多重生物辨識認證系統，且對於驗證時間希望能在一定時間內完成,動態地依據安全性需求提供最佳的生物辨識組合方案，本計畫針對下列議題進行深入研究：

議題 I：一個高準確率的多重生物辨識認證系統；

議題 II：能夠動態的依據安全性需求提供最佳的生物辨識組合方案；

上述議題將運用數學式建立相關模型成目標式和多項限制式，依使用者只要在循序式的生物辨識機制的其中一個回合，能夠達到第一門檻即可通過，若是低於第二門檻則直接拒絕，若是位於其中，才會需要進行下一階段的生物辨識機制。如此一來，使用者只有在最糟糕的情形下才會需要使用所有系統所提供的生物辨識機制。計畫中除了運用數學模式來描述外，運用現有最佳化技術與自行開發優化演算法來進行分析和驗證，發展以幾何規劃為基礎的集中式與啟發式演算法，且執行相關參數驗證，依此設計一系列實驗、數值分析計算出最佳解或近似最佳解以最有效率及有效果之方式設計該多重生物辨識系統，結合理論與實務應用。

關鍵字: 多重生物辨識系統、幾何規劃、雙重門檻、最佳化、循序生物辨識系統

Thesis Abstract

Thesis Title:

A serial multi-modal biometrics authentication system based on double threshold decisions

Author: Li-Min Zheng

Advisor: Yeong-Sung Lin, Ph.D.

In recent years, business organizations highly regarded in information security issues. We process any type of data whether structure or non-structure through the internet, such as log files, photographs, Voices, Communication records and e-mail. All these data has personal privacy information, so the protection of these data can not be ignore. The stealing and misuse of privacy information will harm company’s goodwill and the loss is hard to evaluate. For example, the hacker attack event in stealing celebrity photos on iCloud shows the insufficient of general identity authentication mechanism. Actually, iPhone 5s could provide several biometrics services include face recognition, voice recognition, fingerprint recognition and keystroke recognition, but there hasn’t exist a good way to intergrate all these biometrics services. Therefore, this paper propose a multi-modal biometrics authentication modal with serial verification in practical applications to avoid improper connection to the systems. This paper design an optimal algorithm to produce an optimal solution of biometrics combination with dynamic security requirements for a shortest authentication time, high-accuracy and low false reject multi-modal biometrics authentication systems. In our paper, we focus on the two issues:

Issues 1: A high-accuracy multi-modal biometrics system

Issues 2: An optimal combination solution of biometric modality according to dynamic security requirements.

Issues of above will use mathematical formula to establish the relevant model to the objective function and constraints. In our model, if user achieve the pass threshold, the system will accept the user; if user can not achieve the, the system will reject the user; only if user between pass threshold and reject threshold have to carry on the next level biometric authentication. User need to use all the biometric mechanism which provided by systems only in the worst-case situation. In addition to use mathematical formula to establish our model, we use exist optimization techniques and self-developed centralized and heuristic optimization algorithm based on Geometric Programming to analysis and verification. According to the design of series experiments and numerical analysis, we want to calculate optimal or near-optimal solutions in most efficiency and effectiveness way for the multi-modal biometrics systems which integrate theory with practice.

Keywords: Multi-Biometrics System, Geometric Programming, Double Thresholds, Optimization , Serial Biometrics System

Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

In recent years, more and more government departments invest in building biometric-based indentity management sysytems for ID cards, passports, visas, drivers's license, border control, public monitoring, access control etc. The practical example like: United States Visitor and Immigrant Status Indicator Technology(US-Visit) in USA[1]; National ID in United Kingdom[2]; Aadhaar/Unique ID project in India[3]. On the other hand, because of the information security issue from growing cloud services, the promotion of "Personal Information Protection Act", the rise of personal privacy and access control for sensitive business data, some private stakeholders who has security requirements also adopt biometric-based indentity management systems. Due to the requirement and investment form government and private departments, the market share of biometric technology grows year by year. A market research report made by Global Information Inc shows that the average annual growth rate of global biometrics market is about 21% [4].

Using biometric technology for identity management compared to traditional identity management method such as password has many advantages[6]. First, there is no need to remember anything, biometric attributes cannot be lost, transferred or stolen. Second, biometrics attributes are very difficult to forge so it could effectively reduce the risk of spoofing.

In the past years, many researchers study and work hard in biometrics systems. The development of biometrics technology becomes more mature. Many biometrics modality has been tested and used, such as fingerprint recognition, hand geometry recognition, face recognition and Iris recognition etc[5][6]. The performane of recognition system based on single modality is easily impacted by 1) Noisy data, 2) intra-calss variations, 3) distinctiveness, 4) non-universality, 5) spoof attacks. Therefore, some researchers begin studing in multi-modal biometric systmes. Although multi-modal systems need additional costs of different kinds of sensors and matching algorithm, it provides better accuracy [7]. There is a simple example to understand how multi-modal system has better accuracy in section 2-1.

1.2 Motivation

With biometric technology is gradually being accepted by the market, national and public security level biometric system began to build and utilize. These middle - large size systems databases has 100,000 to millions data. How to development a high efficiency, high reliability biometric systems is an issue needs to be studied.

Multi-modal biometrics system has been verified that its accuracy is better than uni-modal biometrics system. In the early year, there is lack of cooperation between the biometrics technology providers due to unestablished uniform standards and considerations of building cost. As technology advances, sensor's upgrated ability and lower cost, and establishment of Biometric technology standards make the mulit-modal biometrics system could realize. For example, smart phone is a general device which could provide serveral biometrics technology services. Its touch screen can use for fingerprint biometrics, signature biometrics and keystroke biometrics; its camera can use for face biometrics and Irist biometrics; its recorder can use for voice biometrics. In summory, the basic infrastructure that mulit-modal biometrics system need has reached a fairly high level.

Along with trends in big data and cloud computing services, access control for the government and bussines become more complicated. There are lots of type of data in the database, and data's confidentiality and value are dissimilar. If access contorl is relaxed, system will faces the risk of leakage of confidential information. If access control is strict, the usability and potential value of data is sacrificed. Therefore, how to provide a proper access control mechanism is an important issue.

As previously mentioned, this parper propose a serial multi-modal biometrics authentication system based on double threshold decisions (refer to section 2.1). We expect this modol could achieve:

(1) A high-accuracy multi-modal biometrics system

(2) An optimal combination solution of biometric modality accroding to dynamic security requirements.

In our modol, if user achieve the pass threshold, the system will accept the user; if user can not achieve the pass threshold , then system reject the user; only if user between pass threshold and reject threshold have to carry on the next level biometric authentication. User need to use all the biometric mechanism which provided by systems only in the worst-case situation.

Based on dynamic security requirements to produce an optimal combination solution of biometric modalities has high potentail application value such as confidential file management system, and area access control in military. We could give an optimal comination solutiion based on how confidentail the file user want to aceess or which level the authority that the area need.

1.3 Related Work

In this chapter, we describe the baisc knowledge need to know in biometric academia including the architecture of biometric systems, the modes of oprations, the peformance measurement and the literature survey we do for this paper. In the end, we will discuss multi-modal biometric systems in its operation modes and fusion method. Most information refer to reference[6].

1.3.1 Architecture of Biometric Systems

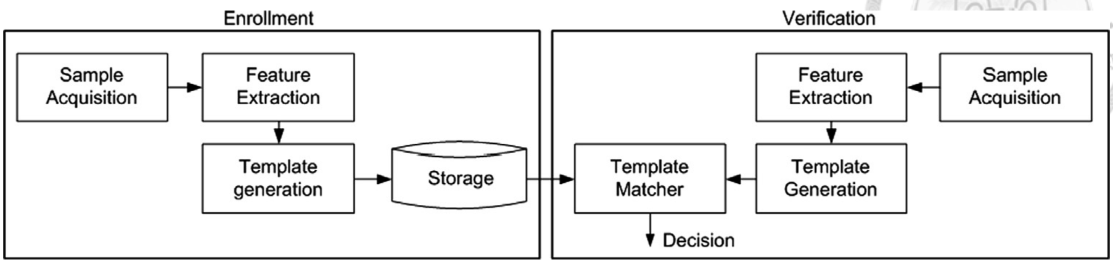


Figure1-1. architecture of biometric systems [6]

According to reference[6], the architecture of biometric systems include the following four module:

(1) Image acuisition module:

This acquires the image of a biometric trait and submit to the system for further processing. This process needs sensor supports such as fingerprint reader, video camera, keyboard, infra-red light camera, recorder etc.

(2) Feature extration module:

Processes the acquired image thereby extracting the salient or discriminatory features such as the line of fingerprint, the distance between eyebrow, the branch of vein, the acceleration bewteen keystroke etc.

(3) Matcher module:

Matchs the extracted features of probe image with those of gallery image to obtain a match score whereas, an embedded decision making module verifies or rejects the claimed identity based on match score.

(4) Database module:

Saves the digital representation of previously acquired samples very often termed as templates for future matching use. If user wants to use this system, the user must enroll, and system will generate template and save in database.

1.3.2 Modes of Operations

According to reference [6], a biometric system operates in one of the following modes:

(1) Authentication/Verification:

This is very often referrd as positive recognition. User need to claims a particular identity before execute the image acuisition process. After system extract the feature and generate template, the matching module will compare between the template and enrolled template with particular identity that the user claim before. If user meet the qualification which system decided, system verify the user. If not, reject the user.

(2) Identification:

This is very often referrd as negative recognition. User don’t need to claim identity before image acuisition process. System compare the generated template with all the enrolled template in the database to find the most likely one the user is. Compare to authentication, indentification needs more cost to matching all the template. In practical, system usually use soft biometrics like gendor or skin color to classify in the beginning of system to reduce the matching time of system.

(3) Screening:

This is an extension to identification. The process is the same, but the ojective of this mode is to assure a particular individual does not belong to a watch list.

The practical applicaion of above three operation modes is show in table 1-1.

Table1-1 applicaion of three operation modes of biometric system

Modes	Applications
Authentication/ Verification	Computer logins, ATMs, e-commerce, access control and user authentication on mobile devices.
Identification	Issuance of ID cards, passports, riving licenses, border crossing and welfare disbursements.

Screening	Airport security, surveillance activities, public place and public events security etc.

1.3.3 Peformance Measurement

In this sector, we will introduce some indicators often used to measure the performance of a biometric system:

(1) False Accept Rate, FAR:

Means the probability that system let imposters pass the system. The higher rate of FAR means the higher risk of system. System needs high security requirements will focus on this indicator.

(2) False Reject Rate, FRR:

Means the probability that system reject the real one who should pass the system. The higher rate of FRR means the worse user experience. System needs high usability will focus on this indicator.

(3) Equal Error Rate, ERR:

Means the rate that system's FAR equal to FRR. This rate usually used to compare the algorithm performance of biometric systems. The lower rate of ERR means the better accuracy of the system.

(4) Receiver Operating Characteristic, ROC:

ROC is a grapical plot that illystrates the performance of a binary classifiery system as its dicscrimination threshold is varied. In biometric system, the curve shows the visual characteristic of trade off between FAR and FRR. Most of biometric system will decide a threshold to determine how similar between user and enroll template the system could accept. If the threshold decrease, we have lower FRR but higher FAR. On the contrary, if the threshold increase, we have lower FAR but higher FRR. ROC curve shows the relation of trade off between FAR and FRR.

(5) Cumulative Match Characteristic, CMC

This curve used in indentification. An indentification system return just one result usally have high recognition error. In practical, such system will return the top k results rather one result. Top k also known as Rank-k. Let rank-k be the horizontal axis and le the probability that top-k results include the real one be the vertical axis, we could draw the CMC curve for indentification system.

1.3.4 Literature Survey

We survey many paper about multi-modal biometrics system in past 4 years. Related literature survey list in Table 1-2.

Table 1-2. Related Literature Survey

Author	***Literature descriotions and features***	***Year***
NormanPoh, ThirimachosBourlai, JosefKittler[9]	Consider the system quality, user characteristics, cost sensitivity as a benchmark. Based on similarity scores multi-modal biometrics authentication systems. Evaluate using pulic database such as face recognition, fingerprint recognition, Iris recognition.	2009
Amioy Kumar, M.Hanmandlu, H.M.Gupta[10]	Based on similarity scores, proposed an authentication biometric system using fuzzy binary decision tree(FBDT) algorithm. According fuzzy gini coefficient and fuzzy entorpy to determine the route in tree. Using Iris recognition system to experiment and evaluate.	2012
Y.J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M. Goh[11]	They propose to fuse multiple biometric modalities at the feature level in order to obtain an integrated template and to secure the fused templates using a hybrid template protection method. The proposed method is made out of a feature transformation technique known as Random Tiling and an equal-probable 2N discretization scheme.	2012
NormanPoh , ArunRoss , WeifengLee , JosefKittler[12]	This study investigates a relatively new fusion strategy that is both user-specific and selective. authors advance the state of the art in user-specific and selective fusion in the several ways. Fifteen sets of multimodal fusion experiments carried out on the XM2VTS score-level benchmark database show	2013

	that even though our proposed user-specific and -selective fusion strategy, its performance compares favorably with the conventional fusion system that considers all information.	
Anne M.P. Canuto, Fernando Pintro, Joao C. Xavier-Junior[13]	Referred to 'Cancellable', means biometrics consist of applying functions (generally not invertible) in the original biometric data in order to obtain transformed or intentionally distorted biometric data. This paper provide three kinds of cancellable transformations for two different biometric modalities (voice and iris).	2013
Suresh Kumar Ramachandran Nair, BirBhanu, SubirGhosh, Ninad S. Thakoor[14]	Based on similarity scores, using statistical method to predict the placement location of match scores. System indentify the user accroding to previous prediction. This paper propose GM modol and GMM modol.	2014
Salman H.Khan, M.AliAkbar, FarrukhShahzad, MudassarFarooq, ZeashanKhan[15]	This paper isn't an algorithm reseach. It focuses on how to keep the template safely to avoid hacker easily access for spoofing attack. This paper adopt hash and password based method trying protect the template without infulence performance of system.	2014

We find that more and more researcher pay attention to the protection of biometrics data in recent year.[13][15] And more and more gait and behavior biometric system survey which is not most popular in biometric academic fields in the past. Lots of interesting fusion method for multi-biometrics has been proposed.[10][14] Except paper, lots of article shows there is another trend that the mobility biometrics systems is more and more important in pratical use.

1.3.5 Operation Modes and Fusion Method of Multi-Modal Biometric Systems

According section 1.2, Multi-modal biometrics system has been verified that its accuracy is better than uni-modal biometrics system, and the basic infrastructure that mulit-modal biometrics system need has reached a fairly high level. Therefore, more and more researchers start studing in multi-modal biometrics. In this sector, we will discuss multi-modal biometric systems in its operation modes and fusion method. Accroding to reference [6], the operation modes of multi-modal biometric systems could classify in two categories:

(1) Serial/cascaded mode:

The acquired multiple traits are processed one after another. The output of one trait serves as an input to the processing of next trait. Within the frame of this scheme, the first modality is normally used as an index to narrow down the search space before the next modality is processed which in turn results in the reduction of recognition time.

(2) Parallel mode:

Multiple modalities are processed simultaneously and the obtained results are combined together to obtain a final match score. This architecture provides better accuracy but requires more time to establish the identity.

Serial and parallel mode architectures are illustrated in Figure 1-2.

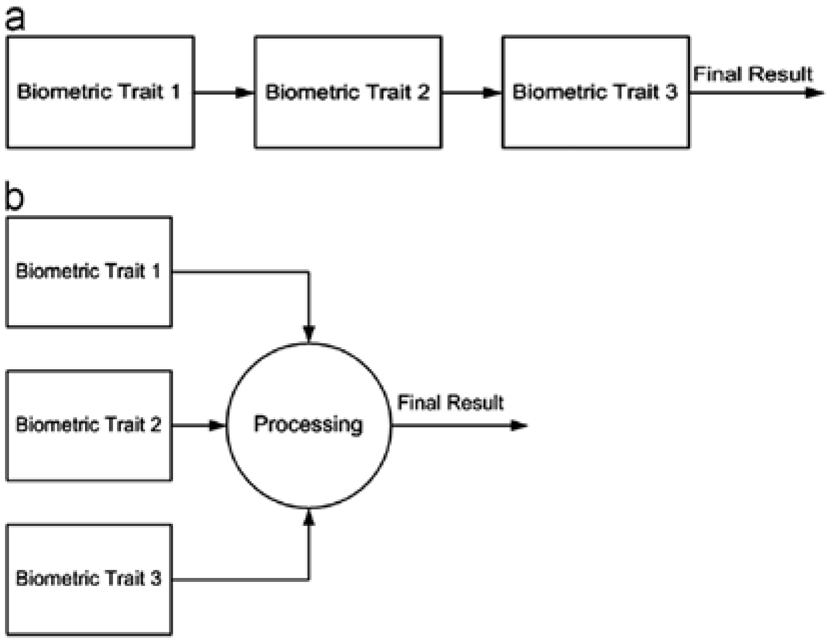


Figure 1-2 Multi-modal system architectures:(a) serial architecture (b) parallel architecture. [6]

There is a problem: how could we fuse different kinds of biometrics modality? According to reference [6], the authors classify the fusion mechanism of multi-modal biometric system into four categories:

(1) Sensor-level fusion:

Each biometric modality has different sensor. Acquisition image from all these sensor will assemble together to generate a new image data. System extraction feature from the new image and generate template for future matching use. For example, Microsoft Kinect has both 3D depth sensors and RGB camera, it combines two sensor data to more correctly identify the user.

(2) Feature-level fustion:

Each biometric modality extract the feature of their own image from sensor. After, system will combine the feature set to a whole new feature set for generating template.

(3) Score-level fusion:

Each biometric modality generate its own scores after their own matching module. After, system combine the score set to one score for future decisions.

(4) Decision-level fusion:

Each biometric modality generate its own result that accept or reject the user. After, system intergrate the results to generate the final result. For example, if there is over half modalities accept the user, the system will accept the user; if not, system reject the user.

The model proposed in this paper is a serial multi-modal biometric system with distinctive decision fusion.

2. Problem Formulation

This paper proposed a serial multi-modal biometric authentication systems based on double threshold decisions. In this chapter, we will describe our modol and the issues we focus on.

2.1 The multi-modal Biometrics Modol with Double Thresholds

Compare to identificaion mode, authentication mode is easier and don’t need lots of time in matching user with all the enrolled template. So this paper choose the authentication mode to research. Maybe we will research the usefulless of this modol in indentificaion mode systems in the future.

The operation merchanism of Identity authentication in our modol illustrate in Figure 2-1. To complete the authentication function, user need finish two processes:

(1) Enroll process:

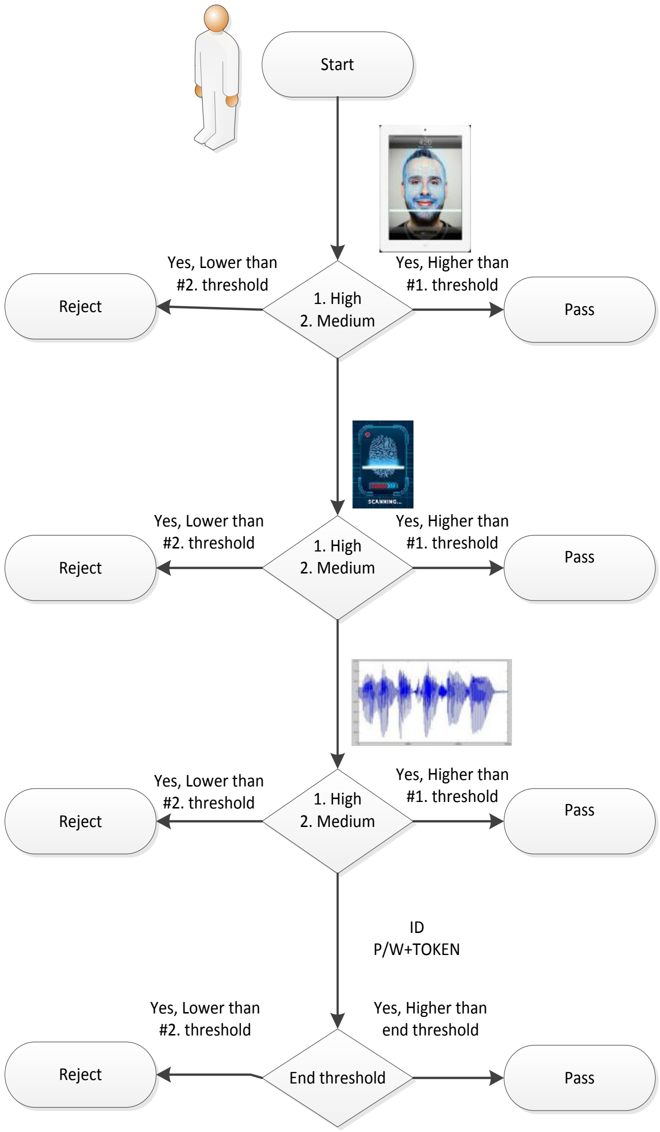
First, user need to provide sample for all kinds of biometric modality which systems provided. After, all of the modality extract the feature and generate template then saving templet into database which calls enroll template.

(2) Authentication process:

When user has identity authentication requirements, user have to claim who the user is. And then, system will ask user to test by first level biometrics modality. After system matching the template between user and the template in database which user claimed, system generates a score. System will take act based on the double threshold decision.

- If the score achieve pass threshold: System accept the user.
- If the score lower than reject threshold: System reject the user.
- If the score between first and reject threshold: system will ask user to do next

level biometrics authentication.



Accroding the situation of next level, system will take different act:

- If this level isn’t the last level in the model: Do as the same in previous level.
- If this level is the last level in the model: In this situation, system must determine to accept or reject the user. Due to the reason, system only have one threshold in this level, i.e. the pass threshold equal to reject threshold. In the end, if score higher than threshold, system accept the user; if score lower than threshold, system rejects the user.

Figure 2-1: Schematic diagram of authentication process in our modol

2.2 Problem Description

Based on the model we proposed in previous chapter, we hope to reduce the user authentication time. User need to use all the biometric mechanism which provided by systems only in the worst-case situation. The problem is how to find the optimal solution that the minimum worst-case authentication time and fulfill the security and usability requirements. Consider the problem, we focus three issues below:

(1) The Combination and Permutation of Biometrics Modalities:

The modol proposed in this paper is serial. Each iteration has it own biometric mechanism. Different kinds of biometric modalities has it own advantage and disadvantage. We think that the accuracy of our model will affected by the permutation of different kind combinations of biometrics modality.

(2) Double Threshold Decisions:

These are the most importance kernal decision variables. These variables will increase along with the level of biometric mechanism. If there is N-level in our modol, the decision variables number of thresholds is 2N-1.

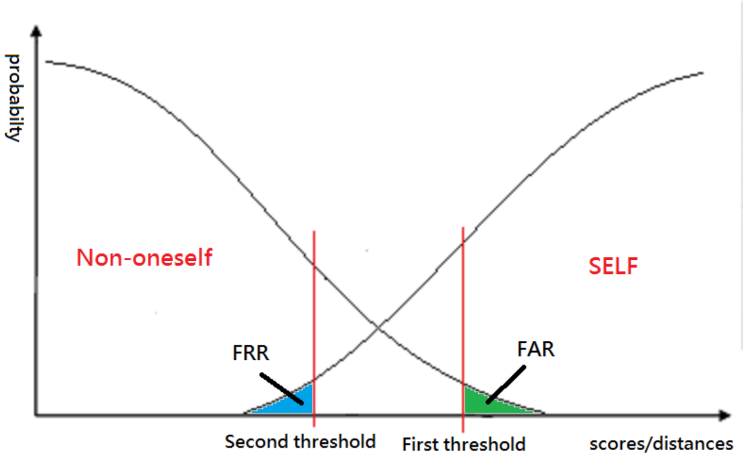


Figure 2-2: Schematic diagram of double threshold decision

Figure 2-2 shows the user himself and imposter's score and probability distribution. The higher score means the system has more confidence that you are the correct one who should pass the authentication. In our modol, we need to decide where the pass threshold and reject threshold is. When we decided pass threshold just like the figure, the green area presents the FAR in this-level with pass threshold we determined. When we decided reject threshold just like the figure, the blue area presents the FRR in this-level with reject threshold we determined. If we increase the pass threshold, the lower FAR we got in this level. If we decrease the reject threshold, the lower FRR we got in this level. Except the final level, we all have to decide pass threshold and reject threshold. It directly affects our modol's final FAR & FRR.

In Figure 2-2, we can easily know that multi-modal system has better accuracy than uni-modal in our model. Suppose there are two biometric systems that have different self and non-oneself distribution in our modal. Whichever in level 1,we could set pass threshold in FAR = 0 with minimum FRR and set reject threshold in FRR = 0 with minimum FAR. If we do that, the next level biometrics mechanism must performance better accuracy than itself when use uni-modal.

(3) User authentication time:

In our modol, some user will finish the authentication process in first level, because their scores is high enough to pass the pass threshold or just so low to achieve the reject threshold. Some user will finish in the final level that is the worst case. We want to find the optimal solution of biometric modalities combination and permutation which can minimum the worst-case authentication time. This issue is very important due to friendly user experience.

2.3 Mathematical Formulation

Given parameters and decision variables relate to our problem list in table 2-1:

Table 2-1 Decision variable

Decision variables	
Notation	Description
t_{b1}	First sensitivity set for method $b \in B$
t_{b2}	Second sensitivity set for method $b \in B$
x_{bs}	1 if method $b \in B$ is employed at stage $s \in S; x_{bs} \in \{0,1\}$
$\alpha(t)$	FAR with threshold t
$\gamma(t)$	FRR with threshold t
a_{s1}	FAR for stage $s \in S$ when the first sensitivity is set $[a_{s1} = \sum_{b \in B} \alpha(t_{b1}) x_{bs}]$
a_{s2}	FAR for stage $s \in S$ when the second sensitivity is set $[a_{s2} = \sum_{b \in B} \alpha(t_{b2}) x_{bs}]$
r_{s1}	FRR for stage $s \in S$ when the first sensitivity is set $[r_{s1} = \sum_{b \in B} \gamma(t_{b1}) x_{bs}]$
r_{s2}	FRR for stage $s \in S$ when the second sensitivity is set $[r_{s2} = \sum_{b \in B} \gamma(t_{b2}) x_{bs}]$

Table 2-2 Given parameters

Given parameters	
Notation	Description
B	The index set of available biometric verification methods.
S	{1,2,…,J} the index set of stage considered in the cascade verification process
T_b	The average authentication time for method $b \in B$
α	System's FAR requirement.
β	System's FRR requirement.

Objective Function is:

$$Z_{NLP} = \min \sum_{\forall s \in S} T_b x_{bs}, \forall b \in B \qquad \text{(NLP 1)}$$

Subject to:

$$t_{b2} \le t_{b1}, \forall b \in B \qquad \text{(NLP 1.1)}$$

$$\sum_{s=1}^{J} (\prod_{1}^{s} a_{s-1,2}) \Box a_{s1} \le \alpha, \forall s \in S \qquad \text{(NLP 1.2)}$$

$$\sum_{s=1}^{J}(\prod_{1}^{s} r_{s-1,1})\square r_{s2} \le \beta, \forall s \in S \qquad \text{(NLP 1.3)}$$

$$x_{bs} = \text{ 0 or 1}, \forall s \in S, \forall b \in B \qquad \text{(NLP 1.4)}$$

$$\sum_{\forall b \in B} x_{bs} \le 1, \forall s \in S \qquad \text{(NLP 1.5)}$$

$$\sum_{\forall s \in S} x_{bs} \le 1, \forall b \in B \qquad \text{(NLP 1.6)}$$

The overall FAR=

$$a_{11} + (a_{12} - a_{11})a_{21} + (a_{12} - a_{11})(a_{22} - a_{21})a_{31} + ... + (a_{12} - a_{11})(a_{22} - a_{21}) ...... (a_{J-1,2} - a_{J-1,1})a_{J,1}$$

$$\approx a_{11} + a_{12}a_{21} + a_{12}a_{22}a_{31} + ... + a_{12}a_{22}a_{32......}a_{J-1,2}a_{J1}$$

$$= \sum_{s=1}^{J}(\prod_{1}^{s} a_{s-1,2})\square a_{s1}$$

The overall FRR=

$$r_{12} + (r_{11} - r_{12})\mathrm{r}_{22} + (r_{11} - r_{12})(r_{21} - r_{22})r_{32} + ... + (r_{11} - r_{12})(r_{21} - r_{22}) ...... (r_{J-1,1} - r_{J-1,2})r_{J,2}$$

$$\approx r_{12} + r_{11}r_{22} + r_{11}r_{21}r_{32} + ... + r_{11}r_{21}r_{31......}r_{J-1,1}r_{J2}$$

$$= \sum_{s=1}^{J}(\prod_{1}^{s} r_{s-1,1})\square r_{s2}$$

The ojective function(NLP) is our goal that to find the minimum worst case authentication under the FAR/FRR constraints(NLP1.2,1.3). NLP 1.1 and NLP 1.4 are variable range restriction. NLP1.5 means every biometric only use once. We can not repeatly choose the same biometric for several levels. The intention here is to lower the influence from dependency of same biometric. In our model, we assume that every biometrics is iid with each other. Previous level's result does not influence the next level. NLP1.6 means each level can only have one biometric.

3. Solution Approach

In this chapter, we suggest our preliminary conception of problem solving. There are two sectors in the chapter, 1) Permutations and Combinations of Biometrics, 2) Finding the Optimal solution which can fulfill the FAR/FRR constraints.

In initialization phase, some parameters need to give is: 1)serveral biometric modalities and 2) user himself and imposter's score and probability distribution for every biometric modalities, and 3)the average authentication time of these modalities.

3.1 Permutations and Combinations of Biometrics

First, we need to find out all the posibile permutations and combinations of biometrics. After that, we can start finding the optimal permutation and combination solution which can fulfill the FAR/FRR constraints with the minimum authentication time.

In this phase, we have to do four steps:

(1) Combination:

First, we list all possible combination of biometric modalities. Assume there are three modalities in our modol: A, B, C. Then, all possible combination are: A, B, C, AB, AC, BC, ABC.

(2) Sorts by the authentication time of combination:

Third, we sort the set of combination from previous results by the authentication time of combination. Assume the authentication time for A = 10s, B=5s, C=7s. After sorting, the set of combination are: B,C, A, BC,AB, AC, ABC.

(3) Permutation:

Finally, we extends all the possible permutation form the previous results of combination. After permutation, the results are: B,C, A, BC,CB,AB,BA, AC,CA, ABC,ACB,BCA,BAC,CAB,CBA,.

The thinking in here is if we sequentially test the combination from the lowest authentication time. The first one we found that could fulfill the FAR/FRR constraints, then this one is one of the optimal solutions we need. (We say “one of” here because maybe there is another one which has the same authentication time can fulfill the constraints.) If this one couldn’t achieve the goal, then we try the next one.

3.2 Finding the Optimal Solution which can Fulfill the FAR/FRR Constraints

In this phase, we have to verify whether a combination fulfill the FAR/FRR constraints. This problem can express in objective function below:

$$Z_{NLP2} = \min \sum_{s=1}^{J} \left(\prod_{1}^{s} r_{s-1,1}\right) \square r_{s2}, \forall s \in S \tag{NLP 2}$$

Subject to:

$$t_{b2} \le t_{b1}, \forall b \in B \tag{NLP 2.1}$$

$$\sum_{s=1}^{J} \left(\prod_{1}^{s} a_{s-1,2}\right) \square a_{s1} \le \alpha, \forall s \in S \tag{NLP 2.2}$$

To solve this problem effectively, we decide to adopt Geometric Programming to modeling the problem.

3.3 Geometric Programming

In this section, we will introduce the Geometric Programming and describe the basic form of a GP, and give a brief discussion of how GPs are solved. Most of the contents are refer to book, **‘Convex Optimization’**(S.Boyd, L.Vandenberghe)[16] and survey paper,**’ A Tutorial on Geometric Programming’**[17].

A geometric programming(GP) is a type of mathematical optimization problem characterized by objective and constraint functions that have a special form.The term geometric program was introduced by Duffin, Peterson, and Zener in their 1967 book on the topic (Duffin et al. 1967). It’s natural to guess that the name comes from the many geometrical problems that can be formulated as GPs. But in fact, the name comes from the geometric-arithmetic mean inequality, which played a central role in the early analysis of GPs.

The main motivation for GP modeling is the great efficiency with which optimization problems of this special form can be solved. To give a rough idea of the current state of the art, standard interior-point algorithms can solve a GP with 1000 variables and 10000 constraints in under a minute, on a small desktop.

3.3.1 GP modeling

Here, we describe the basic form of a GP. There are two special mathematics proper nouns we need to know, monomail and posynomail.

Let $x_1, \ldots, x_n$ denote n real positive variables, and $x = (x_1, \ldots, x_n)$ a vector with components x_i . A real valued function f of x, with the form

$$f(x) = cx_1^{a1}x_2^{a2}...x_n^{an} \qquad \text{(monomial)}$$

where $c > 0$ and $a_i \in \mathbf{R}$, is called a monomial function, or more informally, a monomial. Any positive constant is a monomial, as is any variable. Monomials are closed under multiplication and division: if *f* and *g* are both monomials then so are *fg* and *f/g*. A monomial raised to any power is also a monomial.

A sum of one or more monomials, i.e., a function of the form

$$f(x) = \sum_{k=1}^{k} c_k x_1^{a1k} x_2^{a2k} ... x_n^{ank} \qquad \text{(posynomial)}$$

where $c_k > 0$, is called a posynomial function or, more simply, a posynomial (with K terms, in the variables (x1, . . . , xn). The term ‘posynomial’ is meant to suggest a combination of ‘positive’ and ‘polynomial’. Any monomial is also a posynomial. Posynomials are closed under addition, multiplication, and positive scaling. Posynomials can be divided by monomials (with the result also a posynomial): If *f* is a posynomial and *g* is a monomial, then *f/g* is a posynomial. If *γ* is a nonnegative integer and *f* is a posynomial, then *f γ* always makes sense and is a posynomial.

$$\text{Minimize} \quad f_0(x)$$

$$\text{subject to} \quad f_i(x) \le 1, \mathrm{i}=1,\ldots,\mathrm{m} \qquad \text{(GP optimization problem)}$$

$$g_i(x)=1, \mathrm{i}=1,\ldots,\mathrm{p}$$

In a standard form GP, the objective must be posynomial, the equality constraints can only have the form of a monomial equal to one, and the inequality constraints can only have the form of a posynomial less than or equal to one.

3.3.2 Remodeling for the GP form

Our previous objective function and mainly constraints of FAR are monomial at first glance, but in fact, those decision variables such as a_{b1},a_{b2} is decided by two thresholds in each-level in our model. Since the special form of GP, monomial and posynomial only support few mathematical operation like add, multiply and Exponentiation. If we wand to caculate the decision variables of FAR/FRR in every level in our model from two thresholds we may choose, we very possibly need to face minus operation or others. If we want to use GP to solve our problem, we need to avoid this problem.

There is a simple way to drop the two thresholds decision variables, we could just let the FAR/FRR be our mainly decision variables. In practice, this is very reasonable. The man who design the biometrics authentication system always try every threshold to investigate that FAR and FRR trade off, and choose a proper FAR/FRR then push back to find the corresponding threshold. For the sake of simplicity, we suppose that FAR multiply FRR equal to a constant. If the tail distribution of score and probability distribution of oneself and non-oneself is exponential distribution, this assumption will set up. In most case, it's similar to exponential distribution. To avoid the assumption cause deviation in our model. The constants in our model will be given proper values. ($<\sqrt{0.01}$;The Square of the constant is the ERR of the biometrics system in our assumption. In general, if a biometrics system is worthy of use, it's ERR usually smaller than 1%) In fact, the real FAR and FRR curve will intersect in (0,1) and (1,0), but it's will intersect in (0,constant) and (constant,0) under our assumption. For our estimate of overall FAR and FRR, we are strict, means that we perform better in fact.

As follows is the new model under the assumption: (con_b means the contstant of biometrics b that FAR*FRR is, which we previously assumed.)

$$Z_{NLP2} = \min \sum_{s=1}^{J} (\prod_{1}^{s} r_{s-1,1}) \square r_{s2} \qquad \text{(GP)}$$

Subject to:

$$a_{b1} \leq a_{b2} \qquad \text{(GP1)}$$

$$r_{b2} \leq r_{b1} \qquad \text{(GP2)}$$

$$\sum_{s=1}^{J} (\prod_{1}^{s} a_{s-1,2}) \square a_{s1} \leq \alpha \qquad \text{(GP3)}$$

$$r_{b1} == a_{b1} \wedge (-1) * \mathrm{con}_b, \forall b \in B \qquad \text{(GP4)}$$

$$r_{b2} == a_{b2} \wedge (-1) * \mathrm{con}_b, \forall b \in B \qquad \text{(GP5)}$$

3.3.3 Solving the GP problem

The main trick to solving a GP efficiently is to convert it to a nonlinear but convex optimization problem, i.e., a problem with convex objective and inequality constraint functions, and linear equality constraints. Efficient solution methods for general convex optimization problems are well developed.

The conversion of a GP to a convex problem is based on a logarithmic change of variables, and a logarithmic transformation of the objective and constraint functions. In place of the original variables x_i , we use their logarithms, $y_i = \log x_i$ (so $x_i = e^{y_i}$).

Instead of minimizing the objective f_0, we minimize its logarithm log f_0. We replace the inequality constraints $f_i \leq 1$ with log $f_i \leq 0$, and the equality constraints $g_i = 1$ with log $g_i = 0$. This results in the problem

$$\begin{array}{ll} \text{Minimize} & \log f_0(\mathrm{e}^{y}) \\ \text{subject to} & \log f_i(\mathrm{e}^{y}) \leq 0, \mathrm{i} = 1, \ldots, \mathrm{m} \qquad \text{(Convex optimization problem)} \\ & \log g_i(\mathrm{e}^{y}) = 0, \mathrm{i} = 1, \ldots, \mathrm{p} \end{array}$$

with variables $y = (y_1, \ldots, y_n)$. Here we use the notation e^y , where y is a vector, to mean componentwise exponentiation: $(e^y)i = e^{yi}$.

This new problem doesn't look very different from the original GP ; if anything, it looks more complicated. But unlike the original GP, this transformed version is convex, and so can be solved very efficientl. We won't go deep into more details of GP's mathematical theory. Reference[17] shows that user who use GP do not need to know how GP problem solved. We could pretend the GP solver is a reliable black box which solve all the problem form in GP. In our model, we use the GP solver which reference [18] provide. It's based on Interior point methods just like most GP solver.

Interior point methods is a kind of algorithm to solve linear or non-linear convex optimization problem. It was invented by the John von Neumann. He propose a new method solving the linear programming by using Gordan's homogeneous system.

In addition to being fast, interior-point methods for GPs are also very robust. They require essentially no algorithm parameter tuning, and they require no starting point or initial guess of the optimal solution. They always find the (true, globally) optimal solution, and when the problem is infeasible (i.e., the constraints are mutually inconsistent), they provide a certificate showing that no feasible point exists. General methods for NLP can be fast, but are not guaranteed to find the true, global solution, or even a feasible solution when the problem is feasible. An initial guess must be provided, and can greatly affect the solution found, as well as the solution time. In addition, algorithm parameters in general purpose NLP solvers have to be carefully chosen.

4. Computational Experiments

4.1 Experimental Enviroment

Hardware:
ASUS notepad with 64-bits win8 Operating system and Intel(R) Core™ i5-3337U CPU @ 1.8GHz 1.8 GHz. Memory size 4GB.
Software:
Matlab2015a, Version 8.5.
'GGPLAB', a matlab toolbox for specifying and solving geometric programs.[18]

4.2 Experimental data

According to remodeling model in section 3.3.2. The only parameter of our input of several biometrics authentication systems is the constant which FAR multiply FRR is. Most of the biometrics database only provide original data such as biometrics sample or score set. Data related to the FAR and FRR curve is hard to find. Although we could design or use exist biomertrics system to produce the data we need, it's need lots of works. For convenience, we design five supposed biometrics system carefully refer to exist biometrics systems. Its effectiveness in turn from the bad to the good. With the better the performance, which has a higher authentication time (it may need more accurate and stable sampling procedures or more complex back-end calculation).

ID	FAR*FRR	ERR	Authentication Time
1	0.000081	0.009	1s
2	0.000064	0.008	2s
3	0.000049	0.007	3s
4	0.000036	0.006	4s
5	0.000025	0.005	5s

Refer to section 3.2, we total have $P_1^5+P_2^5+P_3^5+P_4^5+P_5^5=5+20+60+120+120=325$ kinds of biometrics permutations and combinations.

4.3 Result

Our experiment can divided into three parts. First, in our origin idea, we want to provide an optimal combination solution of biometric modality which has the shortest authentication time according to dynamic security requirements. Second, we want to know the performance of our model. Third, we want to know the influences of different permutations in the same combination.

4.3.1 Focus on authentication time(Experiment 4-1)

Experiment 4-1: We try to ajust the FAR and FRR requirements from 0.0009 to 0.0002 with interval 0.0001. We try to list a table to show that the combination of biometrics authentication system which can fulfill the constraints and have the shortest authentication time. The results show in Table 4-1:

Table 4-1: The combination and shortest authentiacation which can fufill different α、β constraints (top:combination;bot:authentication time)

α β	**0.0009**	**0.0008**	**0.0007**	**0.0006**	**0.0005**	**0.0004**	**0.0003**	**0.0002**
0.0009	[1,2,3]	[1,2,3]	[1,2,3]	[1,2,3]	[1,2,3]	[2,3,1]	[4,1,2]	[5,1,2]
	6s	6s	6s	6s	6s	6s	7s	8s
0.0008	[1,2,3]	[1,2,3]	[1,2,3]	[1,2,3]	[2,1,3]	[3,1,2]	[4,1,2]	[5,2,1]
	6s	6s	6s	6s	6s	6s	7s	8s
0.0007	[1,2,3]	[1,2,3]	[1,2,3]	[1,3,2]	[2,3,1]	[4,1,2]	[5,1,2]	[5,3,1]
	6s	6s	6s	6s	6s	7s	8s	9s
0.0006	[1,2,3]	[1,2,3]	[1,3,2]	[2,3,1]	[3,2,1]	[4,1,2]	[5,1,2]	[5,4,1]
	6s	6s	6s	6s	6s	7s	8s	10s
0.0005	[1,2,3]	[2,1,3]	[2,3,1]	[3,2,1]	[4,1,2]	[5,1,2]	[5,3,1]	[3,4,1,2]
	6s	6s	6s	6s	7s	8s	9s	10s
0.0004	[2,3,1]	[3,1,2]	[4,1,2]	[4,1,2]	[5,1,2]	[5,2,1]	[5,4,1]	[4,3,2,1]
	6s	6s	7s	7s	8s	8s	10s	10s

0.0003	[4,1,2]	[4,1,2]	[5,1,2]	[5,1,2]	[5,3,1]	[5,4,1]	[4,2,1,3]	[5,3,2,1]
	7s	7s	8s	8s	9s	10s	10s	11s
0.0002	[5,1,2]	[5,2,1]	[5,3,1]	[5,4,1]	[3,4,1,2]	[4,3,2,1]	[5,2,3,1]	[4,3,5,2,1]
	8s	8s	9s	10s	10s	10s	11s	15s

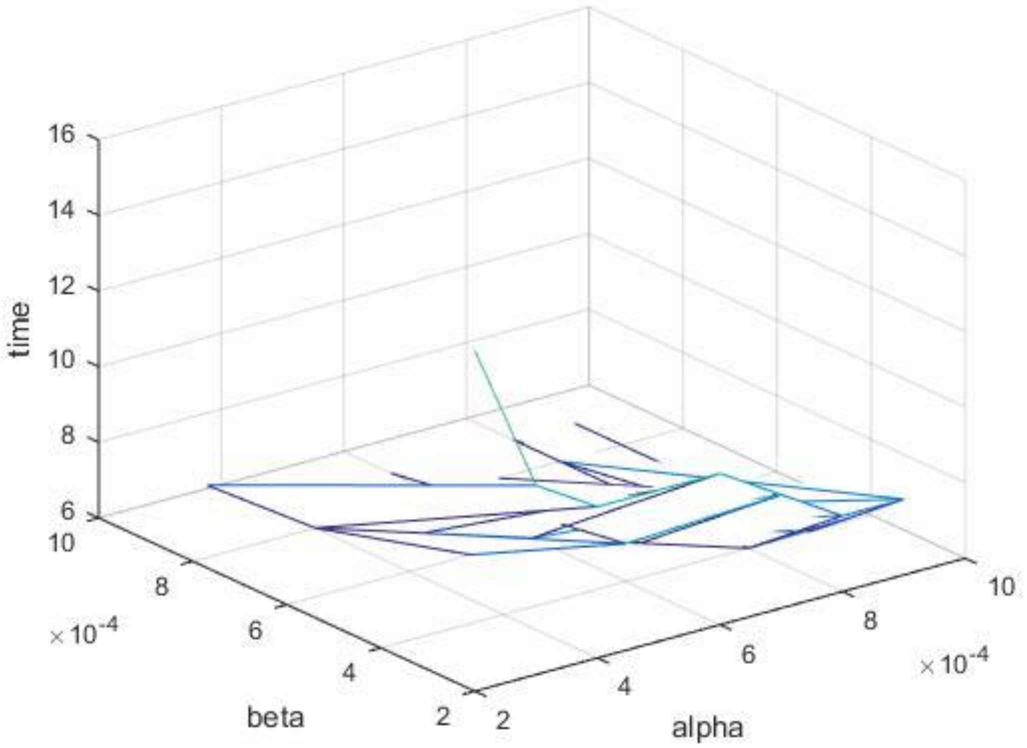


Figure4-1: Three dimension Figure x,y,z = (α 、 β 、Authentication Time)

We try bigger α and β in advance, and find that the value we set in experiment 4-1 is just right consists of three,four,five-level of combinations and touch the bound that don’t have a feasible solution. In performance view, altough we evaluate FAR and FRR strictly at first, we still have high-accuracy that the error rate is under 0.0002 in the best combination. It illustrate that using our model to combine several kinds biometrics authentication system can improve the accuracy rate effectively. Figure 4-1 shows that when we have more stirctly α and β, the authentication time is more longer.

Experiment 4-1 took 542 seconds by using the common desktop. It proves the effectiveness of GP. If there isn’t lots of biometrics system, we could provide an optimal combination solution of biometric modality which has the shortest authentication time according to dynamic security requirements in a short time.

4.3.2 Focus on performance(Experiment 4-2,4-3)

Experiment 4-2: This part we focus on the system performance. We set α =0.0005 to observe the change of FRR. The result shows in Figure 4-2:

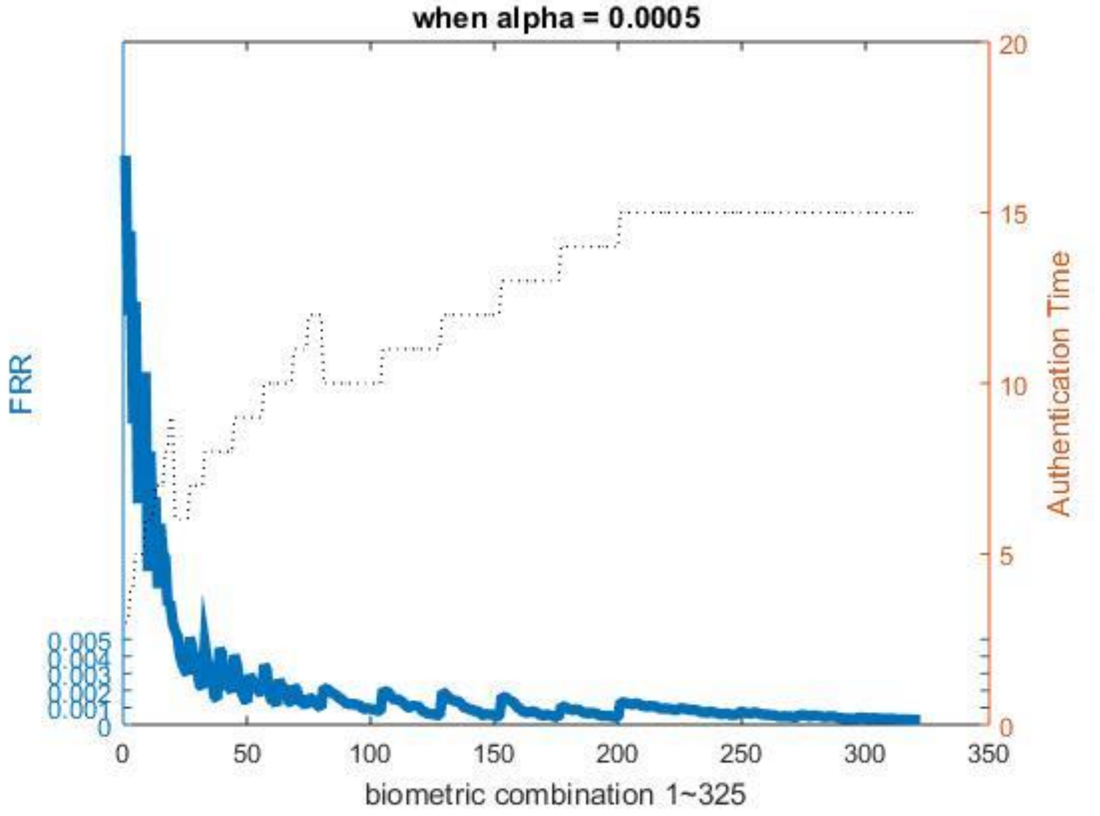


Figure4-2:when α =0.0005，320 kinds of biometrics combination2's minimum FRR and it's authentication time

In figure 4-2, combinations 0~20 are two-level ,40~80 are three-level, 80~120 are four-level, others are five level. On the left, we can obviously discover that the change of FRR is mostly in the interval of two-level combinations. Like expected, more level we use have more accuracy in average. It is noteworthy that the FRR twists and turns dramaticly because even the same conbination of biometrics, the permutation will influence the perfromance hardly. We will experiment later in experiment 4-3 and 4-3. Experiment 4-2 took 133 seconds.

4.3.3 Focus on permutation(Experiment 4-3,4-4)

In this part of experiment, we want to know we should put one biometrics system in preceding level or the last level can improve the performance? We choose the combination[1,3,5] which is most different from each other (Experiment 4-3)and the best of four combination[2,3,4,5] (Experiment 4-4) to experiment. Experiment 4-3 tooks 63 seconds and experiment 4-4 took 326 seconds. The results show in Table 4-3,4-4,Figure4-3,4-4,4-5:

Table 4-3 cobination[1,3,5]' FRR performance when alpha = 0.001:-0.0001:0.0002

Alpha/BIO	[1,3,5]	[1,5,3]	[3,1,5]	[3,5,1]	[5,1,3	[5,3,1]
0.0009	0.000356	0.000301	0.000277	0.000207	0.000167	0.000148
0.0008	0.000401	0.000339	0.000312	0.000232	0.000188	0.000166
0.0007	0.000458	0.000387	0.000356	0.000266	0.000215	0.00019
0.0006	0.000535	0.000452	0.000416	0.00031	0.000251	0.000221
0.0005	0.000641	0.000542	0.000499	0.000372	0.000301	0.000266
0.0004	0.000802	0.000678	0.000624	0.000465	0.000377	0.000332
0.0003	0.001069	0.000904	0.000832	0.00062	0.000502	0.000443
0.0002	0.001604	0.001355	0.001247	0.00093	0.000753	0.000664

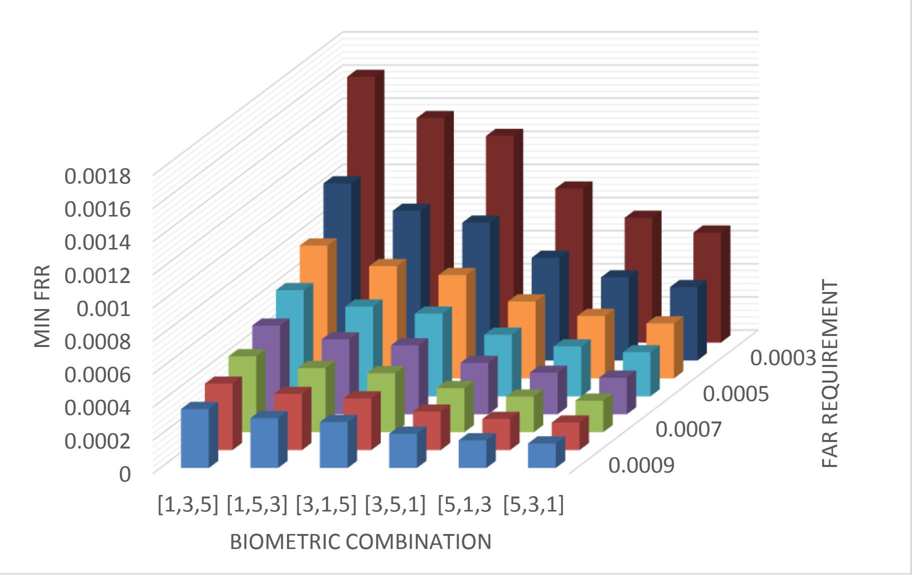


Figure4-3 cobination[1,3,5]' FRR performance when alpha = 0.001:-0.0001:0.0002

Table4-4 cobination[2,3,4,5]' FRR performance when alpha = 0.001:-0.0001:0.0002(10^-3)

Alpha/BIO	[2,3,4,5]	[2,3,5,4]	[2,4,3,5]	[2,4,5,3]	[2,5,3,4]	[2,5,4,3]
0.0009	0.1166	0.112	0.1091	0.1021	0.0983	0.0957
0.0008	0.1305	0.1247	0.121	0.1122	0.1074	0.1042
0.0007	0.1491	0.1425	0.1381	0.1269	0.1207	0.1165
0.0006	0.174	0.1662	0.1611	0.1481	0.1405	0.1352
0.0005	0.2088	0.1995	0.1933	0.1777	0.1686	0.1622
0.0004	0.261	0.2494	0.2416	0.2221	0.2108	0.2028
0.0003	0.348	0.3325	0.3222	0.2962	0.281	0.2704
0.0002	0.522	0.4987	0.4833	0.4443	0.4215	0.4056
	[3,2,4,5]	[3,2,5,4]	[3,4,2,5]	[3,4,5,2]	[3,5,2,4]	[3,5,4,2]
0.0009	0.1015	0.097	0.0884	0.0802	0.079	0.075
0.0008	0.1142	0.1091	0.0989	0.0884	0.087	0.0819
0.0007	0.1305	0.1247	0.113	0.1005	0.0986	0.0919
0.0006	0.1523	0.1455	0.1319	0.1172	0.115	0.107
0.0005	0.1827	0.1746	0.1582	0.1407	0.138	0.1284
0.0004	0.2284	0.2182	0.1978	0.1759	0.1725	0.1605
0.0003	0.3045	0.2909	0.2637	0.2345	0.23	0.214
0.0002	0.4568	0.4364	0.3956	0.3517	0.345	0.3211
	[4,2,3,5]	[4,2,5,3]	[4,3,2,5]	[4,3,5,2]	[4,5,2,3]	[4,5,3,2]
0.0009	0.0805	0.074	0.0753	0.0672	0.0598	0.0583
0.0008	0.0906	0.0833	0.0848	0.0754	0.0661	0.0642
0.0007	0.1036	0.0952	0.0969	0.0861	0.0753	0.0728
0.0006	0.1208	0.1111	0.113	0.1005	0.0878	0.0849
0.0005	0.145	0.1333	0.1356	0.1206	0.1054	0.1019
0.0004	0.1812	0.1666	0.1695	0.1507	0.1317	0.1274
0.0003	0.2416	0.2221	0.226	0.201	0.1756	0.1699
0.0002	0.3625	0.3332	0.339	0.3015	0.2634	0.2548
	[5,2,3,4]	[5,2,4,3]	[5,3,2,4]	[5,3,4,2]	[5,4,2,3]	[5,4,3,2]
0.0009	0.0585	0.0563	0.0548	0.051	0.0488	0.0473
0.0008	0.0659	0.0634	0.0616	0.0573	0.0549	0.0531
0.0007	0.0753	0.0724	0.0704	0.0655	0.0627	0.0607
0.0006	0.0878	0.0845	0.0821	0.0764	0.0732	0.0708
0.0005	0.1054	0.1014	0.0986	0.0917	0.0878	0.0849
0.0004	0.1317	0.1267	0.1232	0.1147	0.1098	0.1062
0.0003	0.1756	0.169	0.1643	0.1529	0.1464	0.1415

0.0002	0.2634	0.2535	0.2464	0.2293	0.2195	0.2123

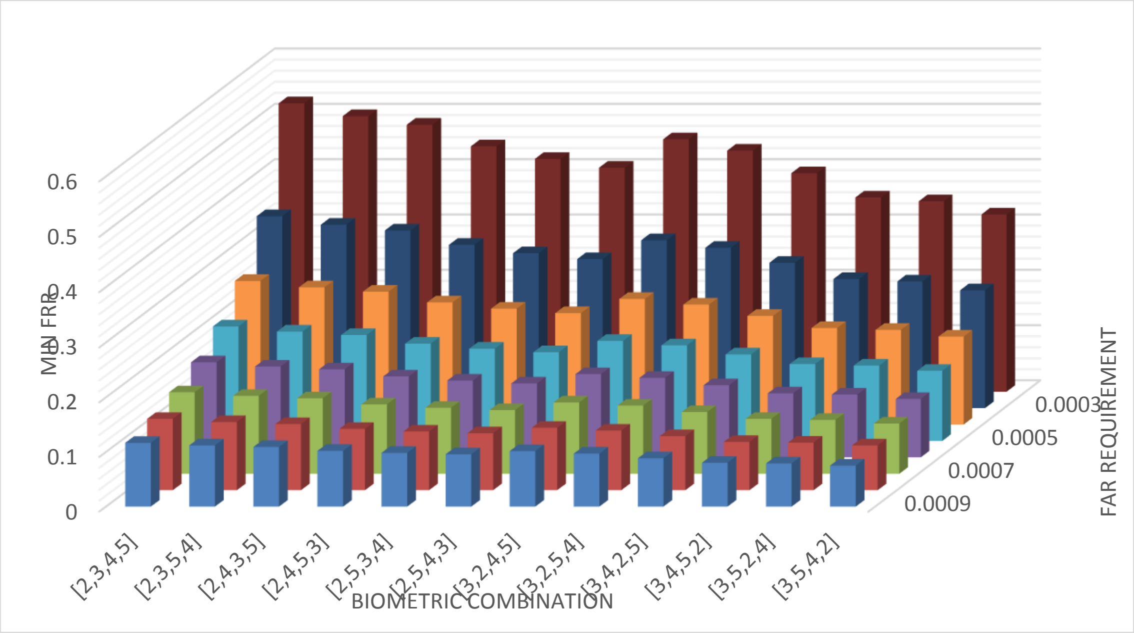


Figure 4-4 cobination[2,3,4,5]' FRR performance when alpha = 0.001:-0.0001:0.0002 part1

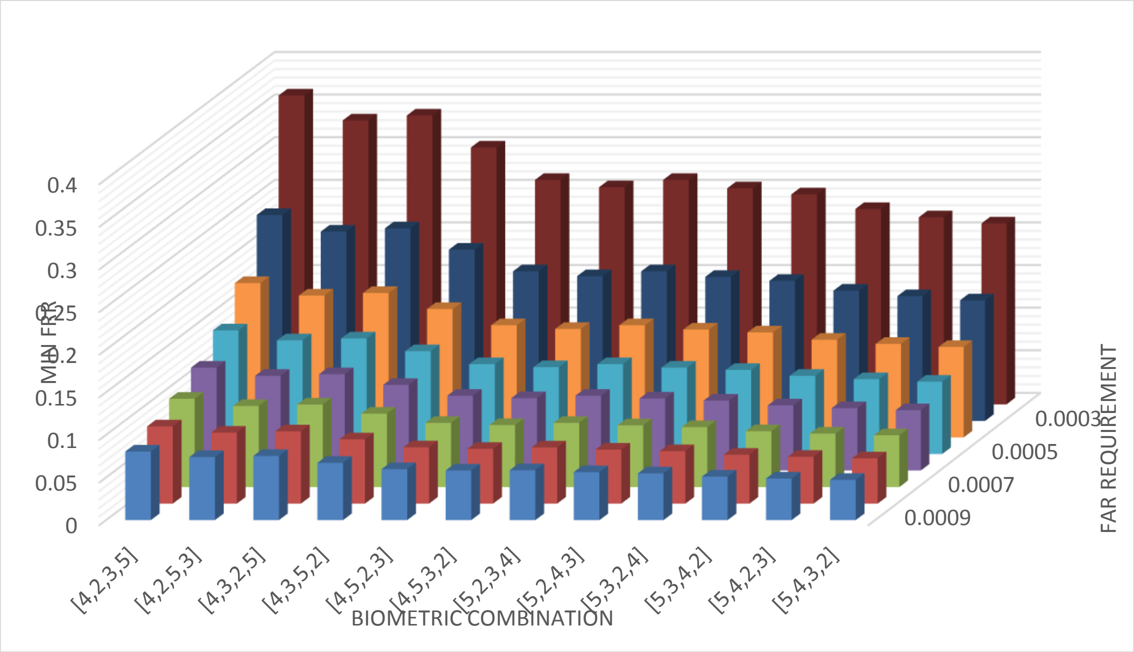


Figure 4-5 cobination[2,3,4,5]' FRR performance when alpha = 0.001:-0.0001:0.0002part2

From experiment 4-3 and 4-4's data, we could summed up that when the biometrics are the best performance in its combination. You should put it in the first-level to maximize the performance. Maybe the inference can cover more situation: if biometrics A is totally better than B, A in the level in front of B can get better performance. If the inference can be proved. It will give a lot of advantage in providing an optimal combination solution of biometric modality according to dynamic security requirements.

5. Future Work

There is lots work we can study based on our theis:

1) We could use 'cost' replace the 'time' in our model to transform an optimal problem into a design problem easily.
2) In pratical, sample acuisition in different biometrics systems can sampling at the same time. For example, system cam take your face picture and you can sign on the electronic board at the same time. If do so, the authentication time can cut down the sampling time.
3) In our model, the more biometric systems we have, the more better performance we get. If we take no notice of the authentication time and back-end algorithem cost, can we develop a near-perfect system?
4) Try to prove the inference: if biometrics A is totally better than B, A in the level in front of B can get better performance. This will give a big advantage in our model and experiment.
5) Find a way to estimate the dependency between biometrics mechanisms that we ignore in our thesis. It can help FAR/FRR results of our model become more accurate. In addition to, we could try to choose the same biometrics mechanism in several level to look what different from results in our thesis.

6. Conclusion

To provide an optimal combination solution of biometric modality according to dynamic security requirements is the main purpose in this thesis. The double threshold decisions based model we proposed can simply combine several kinds of biometrics authentication systems. We solve the NLP problem with the Geometric Programming that Great enhance the computing speed. Because the speed, providing an optimal combination solution of biometric modality according to dynamic security requirements is not a dream. In practical, we could produce the table such as our experiment 4-1 in advance. When user need authentication, we can quickly find the optimal biometrics combination under FAR/FRR requirement which system need by the table. When there is a new biometrics systems, we can add and update table in a short time. Overall, we purpose an effective method to combine biometric mechanisms and to find the opitimal combination under the FAR/FRR requirement in an efficient way by using Geometric Programming.

Reference

[1] Robert A. Mocny, Direcetor US-VISIT, “Biometrics Standards Requirements for US-Visit”

[2] Tracey Caldwell, “National ID cards in the UK: the role of biometrics”, Biometric Technology Today , Volume 2013, Issue 7, July 2013, Pages 7–8

[3] Bigthink editors, “World's Biggest Biometrics ID Scheme”

[4] RNCOS E-Services Pvt. Ltd., Biometric Market Forecast to 2014

[5] Ariana-Michele Moore, “Biometric technologies — an introduction”, Biometric Technology Today, Volume 15, Issue 1, January 2007, Pages 6–7

[6] J.A.Unar , Woo Chaw Seng, Almas Abbasi, “A review of biometric technology along with trends and prospects”, Pattern Recognition, Volume 47, Issue 8, August 2014, Pages 2673-2688

[7] K. Bowyer, K. Chang, P. Flynn, X. Chen, “Face recognition using 2-D, 3-D, and infrared : is multi modal better than multi sample?”, Proc. IEEE’94, November 2006, Pages 2000–2012

[8] Biometrics.gov, the central source of information on biometrics-related activities of the Federal government, “Biometrics Technology and Standards Overview”

[9] Norman Poh, Thirimachos Bourlai, Josef Kittler, “A multimodal biometric test bed for quality-dependent, cost-sensitive and client-specific score-level fusion algorithms”, Pattern Recognition, Volume 43, Issus 3, March 2010 ,Pages 1094-1105

[10] Amioy Kumar, M.Hanmandlu, H.M.Gupta, “Fuzzy binary decision tree for biometric based personal authentication”, Neurocomputing, Volume 99, 1 January 2013, Pages 87-97

[11] Y.J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M. Goh, “Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion” , Information Fusion Volume 18, July 2014, Pages 161–174

[12] NormanPoh , ArunRoss , WeifengLee , JosefKittler, “A user-specific and selective multimodal biometric fusion strategy by ranking subjects” , Pattern Recognition Volume 46, Issue 12, December 2013, Pages 3341–3357

[13] Anne M.P. Canuto, Fernando Pintro, Joao C. Xavier-Junior, “Investigating fusion approaches in multi-biometric cancellable recognition” , Expert Systems with Applications Volume 40, Issue 6, May 2013, Pages 1971–1980

[14] Suresh Kumar Ramachandran Nair, Bir Bhanu, Subir Ghosh, Ninad S. Thakoor, “Predictive models for multibiometric systems”, Pattern Recognition, Volume 47, Issue 12, December 2014, Pages 3779-3792

[15] Salman H.Khan, M. Ali Akbar, Farrukh Shahzad, Mudassar Farooq, Zeashan Khan, “Secure biometric template generation for multi-factor authentication”, Pattern Recognition, Volume 48, Issue 2, February 2015, Pages 458-473

[16] Convex Optimization (S.Boyd, L.Vandenberghe) Cambridge University Press, 2004 , ISBN-13:978-0521833783 , ISBN-10: 0521833787

[17] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, “A Tutorial on Geometric Programming”, Optimization and Engineering, Volume 8, Issue 1, March 2007, Pages 67-127

[18] GGPLAB’, a matlab toolbox for specifying and solving geometric programs.