Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2019) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Adaptive Threshold for Fingerprint Recognition System Based on Threat Level and System Load

Vaibhav B Joshi[a], Mehul S Raval[b]

[a]*Rydot Infotech Ltd, Law Garden, Ahmedabad, 380009, India*
[b]*Pandit Deendayal Petroleum University, Raisan, Gandhinagar, 382007, India*

Abstract

Fingerprint is widely used trait for person recognition in civilian applications. A user is authenticated when matching score is greater than acceptance threshold. The performance of fingerprint system (FS) is evaluated based on false acceptance rate (FAR) and false rejection rate (FRR). Usually the FS is set to work at a rate where FAR and FRR are equal (EER). However, operating at EER allows finite FAR which is risky during critical threat. In response acceptance threshold must shifts towards zero FAR to mitigate threat. This increases FRR, system load and user inconvenience. In civilian application acceptance threshold is set by vendor and currently there is no research attempt to change it dynamically. This is necessary as; 1) system must respond to external parameters like load and threat level; 2) system must balance security and user convenience due to high traffic. This paper describes a method to change acceptance threshold over the interval EER to zero FAR based on system load and threat level. The proposed method is based on fuzzy inference system (FIS) and artificial neural network (ANN).

Keywords: Adaptive; Biometrics, Fingerprint System; Security, Threshold

1. Introduction

In 21st century, fingerprint is most popular biometric used for providing access to a user. The performance of fingerprint recognition system depends on the several factors like, sensor characteristics, indoor and outdoor temperature, humidity, lighting conditions etc. [1]. Such conditions play a very vital role during segmentation and classification [2, 3]. The internal and external factors cause intra and inter class variation generating error in person recognition [4]. Hence, instead of looking for a 100% match, authentication is given when a matching score between

* Corresponding author. Tel.: +91-79-2327-5397 ; fax: +91-79-2327-5030.
E-mail address: mehul.raval@sot.pdpu.ac.in

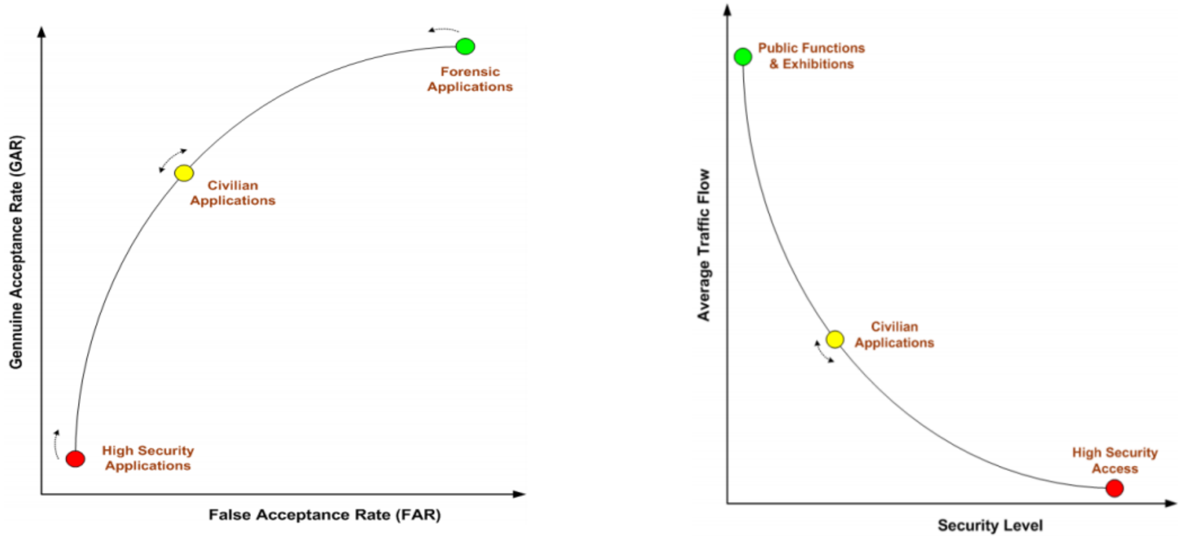

Fig. 1: Security level, traffic flow and false acceptance rate for different class of applications [5]

enrolled and test fingerprint is greater than an acceptance threshold. It is a pre-decided matching score used to distinguish genuine user and impostor. Like any pattern recognition system FS also has false rejection (type I error) and false acceptance (type II error). They are defined as follows:

$$FAR = \frac{\#Impostor\ accepted\ as\ a\ genuine\ user}{total\ no.\ of\ impostor} \tag{1}$$

$$FRR = \frac{\#genuine\ user\ treated\ as\ impostor}{all\ genuine\ users} \tag{2}$$

Based on FAR and FRR accuracy is defined as follows:

$$Accuracy(\%) = 100 - \frac{FAR(\%) + FRR(\%)}{2} \tag{3}$$

Due to large number of application scenarios, it is difficult to generalize acceptance threshold. Fig. 1 shows security level, traffic flow and FAR for different applications [5]. Depending on application acceptance threshold is varied to balance user convenience [6] and security [1]. For example, a fingerprint based entry system at Disney world prefers low FRR [1] because of high traffic flow, moderate security and better user experience. The FS deployed at such places balance user inconvenience and security. As result acceptance threshold is set at equal error rate (EER). However, acceptance threshold must change based on FAR and FRR [7]. In 2004 NIST [8] studied the matching performance of the US-VISIT IDENT system using flat fingerprints. Authors analyzed effect of different acceptance threshold on false rates. They recommended periodic changes in threshold for improving FS performance. In [9] author shows the change in acceptance threshold based on security requirements and its effect on FAR and FRR. An adaptive fingerprint system [4, 10] has been introduced to handle intra class variation with respect to user inconvenience. The aim is to continuously adapt the fingerprint system to intra class variation of input data. Optimal acceptance threshold detection techniques [7, 11] has been introduced to handle inter class variation. In [7], authors use Bayesian approach for classification and then use student-t distribution to reduce the cost of false acceptance and rejection. In [11], authors defines cost function based on FAR and FRR which is minimized using gradient descent technique. Due to external parameters and environmental conditions matching accuracy of a minutiae based fingerprint system changes. The authors in [12, 13] suggested dynamic thresholding for fingerprint recognition system. In [13], for each enrolled fingerprint authors find maximum and minimum matching score to decide dynamic range of operating point. In [12] authors introduce a context user factor (CUF) which is based on historical usage override and generic usage override conditions. A new acceptance threshold is decided based on the updated CUF. The generic usage override conditions are due to location, temperature and humidity and ambient light. Historical usage override condition contains an FRR score for last Q samples of the user. Authors in [5] discuss dynamic threshold for multi-modal biometric system. It is assumed that multi-modal biometrics increase security with increase in FRR. The authors defines cost associated with FRR during high traffic to derive optimal threshold. The total cost is calculated as a linear combination of cost associated with FAR and FRR. The weight are optimized using particle swam optimization (PSO). All methods for dynamic thresholding in [7, 12, 13, 11, 4, 10] compensate effects on biometric samples as well as on system features. Similarly authors in [5, 14] suggested dynamic threshold for multi modal biometric system. However, above approaches do not consider impact of parameters like threat level and system load while dynamically changing acceptance threshold. This is a very practical problem and needs solution during fingerprint system deployment. For example, in a cricket stadium with fingerprint based access, system operates at EER for user convenience during entry or exit hours. Also the threshold must change automatically based on threat advisory. Therefore, this paper propose a method to adaptively find an acceptance threshold for balancing security and user convenience. The system finds a threshold that lies between EER to zero FAR. This ensures that during critical alert security overrides user convenience. The proposed method is based on fuzzy inference system (FIS) which takes parameters; system load and threat level as inputs and suggests an optimal FRR^*. This in turn is applied to ANN which generates FAR^*. Using FRR^* and FAR^* optimal acceptance threshold is found.

2. Preliminaries

It is important to understand the relationship between threat level, FAR, FRR and system load while deriving acceptance threshold.

2.1. Relation between threat level and FAR

This paper envisage a fingerprint system deployed at civilian premises. The security agency issue advisory which is designed to give a likelihood of attack. The threat levels are as follows [15]; LOW means an attack is unlikely; MODERATE means an attack is possible, but not likely; SUBSTANTIAL means an attack is a strong possibility; SEVERE means an attack is highly likely; CRITICAL means an attack is expected imminently. Based on such advisory acceptance threshold of FS must evolve. As the threat level moves from LOW to CRITICAL the acceptance threshold shifts from EER to zero FAR. Fig. 2 shows the relationship between FAR/FRR vs. threshold. Based on Fig. 2 various relationships are defined as follows:

$$\begin{gathered} Threatlevel \propto \frac{1}{FAR} \\ FRR \propto \frac{1}{FAR} \\ \therefore Threatlevel \propto FRR \end{gathered} \tag{4}$$

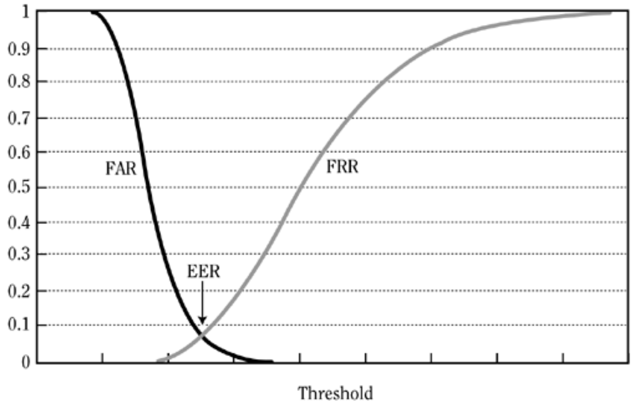

Fig. 2: FAR and FRR vs. acceptance threshold [16]

2.2. *Relation between FRR and system load*

The load on fingerprint system can be well understood using queuing model (M/G/1) [17].

2.2.1. *Analogy between fingerprint system and M/G/1 queuing model*

In general any fingerprint system can be modeled as a single server which processes incoming query to identify individual. It is safe to assume that incoming queries are random and independent of each other. During peak hours the number of incoming queries increases exponentially (c.f. Fig. 3) and then reduces. Such incoming queries can be well modeled by Poisson distribution. The time required for identification is constant and independent to number of queries in the queue. Analogous to fingerprint system, in M/G/1 model 'M' shows incoming query follows Poisson distribution with arrival rate λ, '1' indicates single server and 'G' is independent service time.

2.2.2. *M/G/1 queuing model*

M/G/1 queuing model can be well explained using following equations.

$$\begin{aligned} \rho &= \frac{\lambda}{\mu} \\ E[X] &= \frac{1}{\mu} \\ W &= \frac{\rho}{2\mu(1-\rho)} \\ T &= W + E[X] \\ N &= \lambda T \end{aligned} \tag{5}$$

where, X is a random variable, λ is arrival rate, μ is service rate, ρ is line utilization, T is average time spent by user in system, W indicates average time spent by user in queue and N denotes average number of users in the system. From eq. 5 one can see that line utilization is proportional to λ and inversely proportional to μ. Hence reduction in service rate, increases line utilization. Any system with λ greater than μ is overloaded and service queue tends to infinity. Due

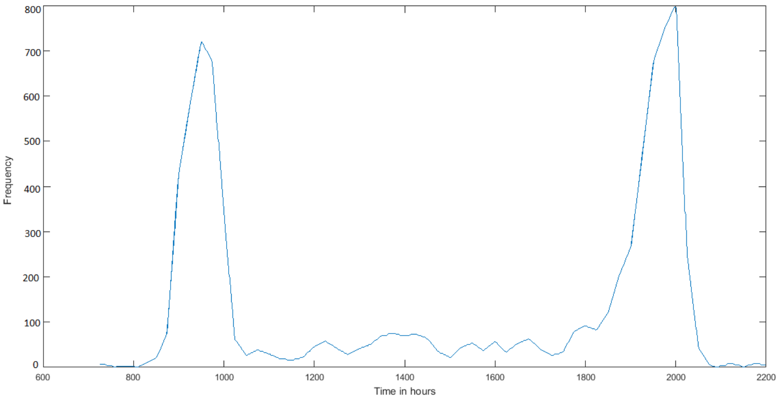

Fig. 3: Number of queries arriving at fingerprint system with respect to time

to a false rejection person will retry authentication request and number of queries increases exponentially in unit time. This increases line utilization and system load. The effect of FRR on line ρ' is modeled as follows.

$$\rho' = \left(\frac{\lambda}{\mu}\right)^{(1-FRR)} \tag{6}$$

2.3. A case study of fingerprint system

A biometric attendance system deployed by Government of India (GoI) is studied in order to gather real statistics to model arrival rate, service time, number of queries and line utilization. The GoI started Aadhaar Enabled Biometric Attendance System (AEBAS) [18] for its employees. The details of their attendance on a day to day basis is made available to public. The portal [18] provides information about organizations, number of registered employees, number of active devices and attendance statistics. Fig. 3 shows a snapshot analogous to attendance at Prasar bharati [19] on a typical day. It has around 1000 registered employees for biometric attendance with average in-time for office at 09.43 am and average out time at 06.18 pm. The average response time per biometric authentication request is 1.58 sec (service time). The peak traffic window is from 08.00 am to 10.00 am and 06.00 pm to 08.00 pm. The biometric terminals for fingerprint collection is tablet, desktop and finger print reader. The tablet and desktop is integrated with fingerprint scanner which has in-built template extractor compatible to Android platform [20]. A typical fingerprint scanner has following specifications; sensor resolution 500 ± 10 [PPI], platen area of $16mm(x) \times 18mm(y)$, operating temperature -20^0C to 60^0C, operating humidity RH 10 to 90 % and supports WSQ compression, $ISO19794-2/4$, ANSI 378 and NFIQ standards. As shown in Fig. 3 average number of queries arriving at system per hour is around 1000 during peak hours. This constitutes an arrival rate $(\lambda) = 1000/3600$ query per second. The average time required for one to many fingerprint verification and identification is $\approx$ 1.5 seconds [19]. Hence, the service rate (μ) is $1/1.5$ query per second. Using these values of λ, μ and eq. 6 the plot of line utilization ρ' vs. FRR is as shown in Fig. 4. It is clear that with increase in FRR the line utilization and system load increases. Therefore, by controlling FRR system load can be moderated for user convenience.

3. Method for Adaptive Threshold

The proposed method considers FS used for civilian application. Simplified block diagram of the method for adaptive threshold is shown in Fig. 5. Function f_L calculates the load L. Then the threat level from intelligence agency

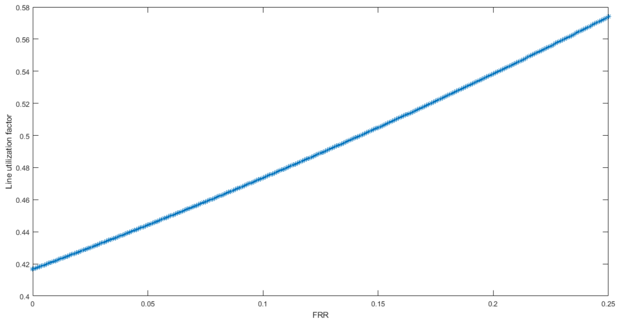

Fig. 4: Line utilization vs. FRR

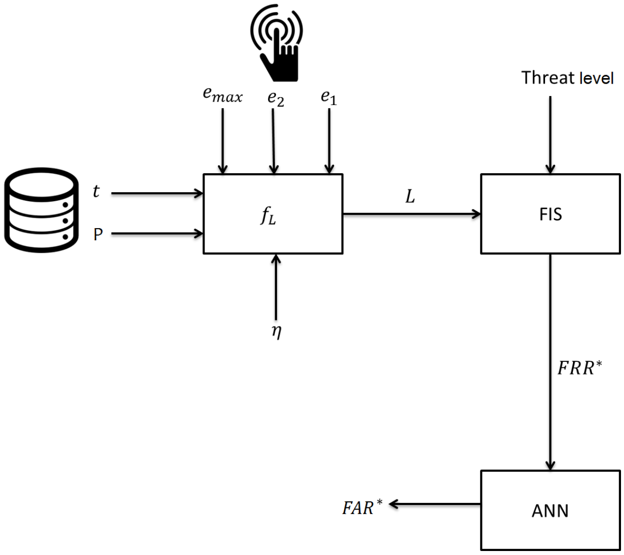

Fig. 5: Basic block diagram of the acceptance threshold recommender

and system load are used as an input to fuzzy inference system which generate FRR^* as output. The FRR^* is given to a trained artificial neural network (ANN) to get an optimal FAR^*. Using FRR^* and FAR^* optimal threshold (TH^*) is computed.

3.1. Query Load Predictor

The f_L computes a load L on the fingerprint system. It depends on two attributes; 1) arrival rate; 2) number of registered users. The traffic rise and fall exponentially during peak hours and it is constant rest of the time. Accordingly $L \geq 1$ signifies critically-balanced or over-load condition. The $L < 1$ indicates under-load during non peak hours. The number of registered user forms another attribute for the system load. Also in Government office temporary registrations are required for visitors on a particular day. Therefore, the load equation must incorporate current and peak arrival rate along with the permanently and temporarily registered users. The load on system is defined as follows [21]:

$$L = \frac{e_1}{e_{max} - (4e_1 - e_2)} + \eta \frac{t}{P + t} \tag{7}$$

where, L is current load, e_1, e_2 are the arrival rate in last 15 minutes and last 1 hour respectively. The e_{max} represents maximum rate in 15 minutes over last twenty four hours. P, t and η are number of permanently registered users, number of temporary registrations and weight parameter respectively. In eq. 7 value of L is affected by size of a window representing *current* time frame. It should neither be too small nor too large. This paper considers time frame of last 15 minutes for measuring current load. In eq. 7 $4e_1$ represent queries equivalent to generated in an hour based on current load and therefore $4e_1 \geqslant e_2$. During peak hours λ for last 15 minutes and last hour is approximately similar i.e. $4e_1 \approxeq e_2$. Similarly when load is very low during non peak hours once again $4e_1 \approxeq e_2$. The eq. 7 in such cases reduces to $L = \frac{e_1}{e_{max}} + \eta\frac{t}{P+t}$. The $L \in [0, 1]$ is normal load while $L > 1$ indicates over load which can occur in two conditions; 1) $e_1 > e_{max}$ and 2) $e_1 = e_{max}$. In second case number of temporary registrations decides the overload magnitude. During non-peak hours even though $4e_1 \approxeq e_2$, will not cause $L > 1$ as $e_{max} > e_1$.

3.2. Fuzzy Inference System (FIS)

The FIS infers FRR^* for the load L and given threat level. The FIS quantifies threat level linguistic terms like ‘low’, ‘moderate’, etc. and load category like ‘low’,‘medium’ and ‘high’. The proposed method use Takagi-Sugeno-Kang (TSK) fuzzy inference because it models non linear system as interpolation over multiple linear models and guarantees continuity in output space [22]. The TSK system also act as a universal approximator for a known function with a guaranteed upper bound on error [23]. The design of FIS implies choosing number of fuzzy membership functions, their shape and the rule base. A fuzzy membership function maps input to its membership value. The proposed method use Gaussian membership function as it is smooth, non zero at all the points and monotonic. A typical rule in TSK fuzzy model has a linear form and the final output is weighted average of all the rules. In the proposed method a rule has following generic form.

$$FRR^* = \alpha_0 + \alpha_1 X_1 + \alpha_2 X_2 \tag{8}$$

where, α_0 is the initial bias required for the output to be in certain range. In the present case $\alpha_0 = EER$ as the output FRR^* must lie between [EER, FAR$_{min}$], where FAR$_{min}$ is value of FRR at minimum FAR. This also form the output range of FIS. The variables X_1 and X_2 are fuzzy sets representing threat level and system load respectively. In eq. 8 α_1 and α_2 are parameters deciding significance of each input. The proposed method emphasize more on the security thereby constraining $\alpha_1 > \alpha_2$. The fuzzyfication of the load is done using three Gaussian fuzzy functions; low, medium, high. The low load spans the range [0, 1], medium load spans [1, 2] and $L > 2$ covers high load range. As per MI5 security recommendation the threat level is fuzzyfied using five Gaussian membership functions namely; low, moderate, substantial, severe and critical.The premiss while building the fuzzy rules are; 1) at low threat level system is tuned to improve user convenience; 2) at moderate threat level output is medium but lowered at high load; 3) when threat level is substantial then with low load, output is held high. It is lowered for medium and high load; 4) at severe threat level output is held high at low and moderate load. It is lowered to medium when load is high; 5) for critical threat level output is held high irrespective of load. With formulation of eq. 8, α_0, fuzzy sets and constrains fuzzy rules are listed in Table 1. Surface plot of proposed FIS rulebase is shown in Fig. 6. The output of FIS has three triangular fuzzy membership functions: low, medium and high. De-fuzzyfication of output using centroid method gives FRR^*.

3.3. Artificial Neural Network (ANN)

The FRR^* should be mapped by a suitable function to find FAR^*. The receiver operating characteristics (ROC) provides one such suitable mapping function. Fig. 7 of FS shows relationship between FAR and FRR. It is a non-linear relation hence fitting a linear function will not work. One can also use a lookup table for mapping discrete FAR - FRR pairs. But it is difficult to estimate number of pairs required for inverse mapping in advance. Therefore, a multilayer neural network is used to learn relationship between FRR and FAR. It consists of four layer and neurons of input and hidden layers have sigmoidal activation. function whereas, the output neuron has a linear activation function. This fully connected neural network is trained using back-propagation learning algorithm. The training pairs of [FRR,

Table 1: Fuzzy rules.

Threat level	Load	Output
low	low	low
	med	low
	high	low
moderate	low	med
	med	med
	high	low
substantial	low	high
	med	med
	high	med
severe	low	high
	med	high
	high	med
critical	low	high
	med	high
	high	high

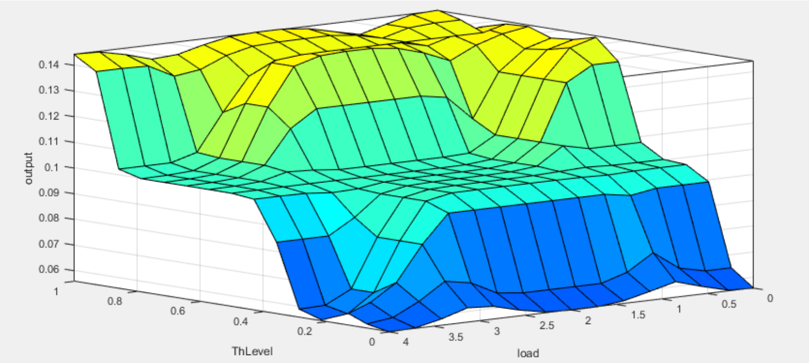

Fig. 6: Surface plot of FIS rulebase

FAR] are extracted from ROC as shown in Figure 7. After learning, ANN is capable of mapping FRR^* to a FAR^*. Then one can find TH from plot of FAR vs threshold.

4. Experimental Results

The proposed method is tested on a FS characterized by Fig. 7. This hybrid technique [24] use minutiae and ridges flow information for fingerprint matching. The fingerprints of 160 persons were captured using veridicom sensor producing 300×300 pixels images at 500 dpi. The reasons for selecting FS in [24] are; the system has 1280 registered users, response time of 1.5 seconds and generates fingerprint images which is analogous to the practical system in subsection 2.3. In the first session, each person gave two impression of four different fingers. A set of 1280 (160×4×2) images were collected in this way. During the second session few week later another 1280 images were obtained. On average FS took 1 second to extract minutiae, 0.3 second for ridge extractio and 0.2 second for fingerprint identification in database. The hybrid technique performs well over a wide range of FAR as shown in Fig. 7. For example, at a FAR of 0.1%, the genuine acceptance rate (GAR) is around 84% or in another words FRR is around 16%. The equal error rate is around 4%. Considering ROC of [24] in the proposed method output range of the FIS is set to [0.04 to 0.16]. The ANN trained over the FRR and FAR using error back-propagation method yields an MSE of 0.00006. Based on threat level and system load, FRR^* and FAR^* given by system are indicated in Table 2. It is easy to visualize that the FIS give FRR^* such that FAR^* lies between minimum value (∼ 0.1%) to EER (∼ 4%). This means the proposed

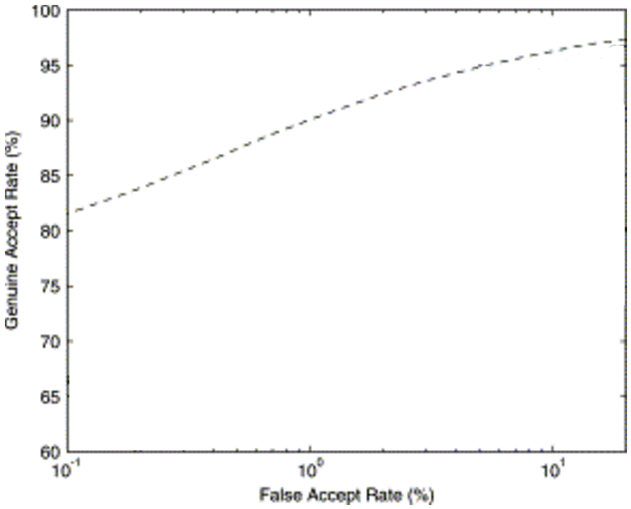

Fig. 7: ROC of a fingerprint system [24]

Table 2: FRR^*, FAR^*, FS accuracy and line utilization (ρ') for different inputs.

Threat level	Load	FRR^*	FAR^*	Accuracy (%)	ρ'
low	low	0.0627	0.0338	95.17	0.4402
	medium	0.0589	0.0352	95.29	0.4387
	high	0.0589	0.0352	95.29	0.4387
moderate	low	0.1178	0.0156	93.35	0.4619
	medium	0.1160	0.0174	93.65	0.4612
	high	0.0965	0.0223	94.21	0.4534
substantial	low	0.1456	0.0109	92.44	0.4733
	medium	0.1124	0.0158	93.36	0.4598
	high	0.1089	0.0173	93.61	0.4583
severe	low	0.1612	0.0037	91.86	0.4800
	medium	0.1548	0.0050	91.75	0.4771
	high	0.1245	0.0173	93.57	0.4646
critical	low	0.1616	0.0028	91.75	0.4800
	medium	0.1616	0.0025	91.73	0.4800
	high	0.1596	0.0045	91.85	0.4791

method dynamically moderates threshold as per load - threat level combination to improve user experience without compromising security. It is also important to note the effect of FRR^* and FAR^* on the recognition accuracy. The proposed method is designed such that it does not change accuracy significantly (c.f. accuracy column in the Table 2) but at the same time modulate FRR for better user experience. The highest accuracy is achieved when system operates at EER. In case of critical threat level one can see from the Table 2 that the accuracy is decreasing which is due to deviation of FRR^* and FAR^* from EER. Contribution to reduction in accuracy is more due to increased FRR as FAR is almost constant and tending to zero. This means that reduction of accuracy doesn't lead to increased chance of impostor breaking the security. As evident from Table 2, when threat level is low or moderate there is a high variation in FRR^*/FAR^* and system is flexible. When threat level is substantial or severe FRR^*/FAR^* variation is moderate and the system flexibility reduces. During critical threat level system becomes conservative and FRR^*/FAR^* is almost constant. One must note that, the proposed method tries to enhance the security as the suggested FAR^* moves from EER to ($\sim 0.1\%$ FAR) as threat level increase. Table 2 also reflects change in line utilization for a given threat level and load. When threat level is low, moderate or substantial the sytem exhibit flexibility i.e. FAR^* varies to reduce ρ' at all types of load. During severe threat level ρ' is almost similar for low and medium load while it reduces at high load. During critical threat level system does not enter into load balancing and ρ' is almost similar at all loads. The system becomes conservative as line utilization increases with rise in threat level. This phenomenon is observed across all types of load and it is due to security concern overriding user convenience.

5. Conclusion

This paper propose an adaptive acceptance threshold for fingerprint system. From Table 2 and the fuzzy rules it is easy to visualize that the proposed method suggest an optimum FRR^* and FAR^* for a given threat level and system load. It adjust FAR^* to effectively balance user experience without compromising security. Currently proposed method is tuned to a specific FS and its generalization capabilities needs to improve. The fully automated system needs exhaustive training on many ROC's and load-threat level scenarios. This also forms future direction for this work. Till the time proposed method achieves generalization, authors envisage it to operate in semi automatic mode i.e. with an operator in loop. A value of recommended threshold is a suggestion for operator who may over rule it and rely on personal experience.

References

[1] A. K. Jain, J. Feng, K. Nandakumar, Fingerprint matching, Computer 43 (2) (2010) 36–44.

[2] C. Parmar, M. Joshi, M. S. Raval, M. Zaveri, Automatic image inpainting for the facial images of monuments, in: Centenary Conference-Electrical Engineering, IISc Bangalore, IISc Bangalore, 2011, pp. 415–420.

[3] A. Parikh, M. S. Raval, C. Parmar, S. Chaudhary, Disease detection and severity estimation in cotton plant from unconstrained images, in: 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), IEEE, 2016, pp. 594–601.

[4] N. Poh, A. Rattani, F. Roli, Critical analysis of adaptive biometric systems, IET biometrics 1 (4) (2012) 179–187.

[5] A. Kumar, Dynamic security management in multibiometrics, Cambridge, UK: Cambridge Univ. Press.

[6] A. K. Jain, A. Ross, Learning user-specific parameters in a multibiometric system, in: Image Processing. 2002. Proceedings. 2002 International Conference on, Vol. 1, IEEE, 2002, pp. I–57.

[7] R. M. Diez, C. Conde, E. Cabello, Automatic detection of the optimal acceptance threshold in a face verification system, in: International Workshop on Biometric Authentication, Springer, 2004, pp. 70–79.

[8] C. L. Wilson, M. D. Garris, C. I. Watson, Matching performance for the us-visit ident system using flat fingerprints, in: National Institute of Standards and Technology Internal Report 7110, Citeseer, 2004.

[9] A. S. Patrick, Fingerprint concerns: Performance, usability, and acceptance of fingerprint biometric systems, National Research Council of Canada.

[10] N. Poh, R. Wong, J. Kittler, F. Roli, Challenges and research directions for adaptive biometric recognition systems, in: International Conference on Biometrics, Springer, 2009, pp. 753–764.

[11] Y. Makihara, M. A. Hossain, Y. Yagi, How to control acceptance threshold for biometric signatures with different confidence values?, in: Pattern Recognition (ICPR), 2010 20th International Conference on, IEEE, 2010, pp. 1208–1211.

[12] Y. Li, P. Ramadas, Context aware biometric authentication, uS Patent 8,255,698 (Aug. 28 2012).
URL https://www.google.com/patents/US8255698

[13] P. Lo, Dynamic thresholding for a fingerprint matching system, uS Patent 7,257,241 (Aug. 14 2007).
URL http://www.google.co.in/patents/US7257241

[14] A. Kumar, V. Kanhangad, D. Zhang, A new framework for adaptive multimodal biometrics management, IEEE transactions on Information Forensics and Security 5 (1) (2010) 92–102.

[15] MI5 security agency business security advice, https://www.mi5.gov.uk/business-security-advice, accessed: 2016-07-1.

[16] Biometrics for network security, prentice hall series in computer networking and distributed, http://flylib.com/books/en/4.400.1.71/1/, accessed: 2017-03-21.

[17] M/G/1 queue massachusetts institute of technology, http://web.mit.edu/modiano/www/6.263/lec8.pdf, accessed: 2016-07-01.

[18] Aadhaar enabled biometric attendance system, http://attendance.gov.in/, accessed: 2019-08-31.

[19] Doordarshan directorate general (prasar bharati), http://ddg.attendance.gov.in/, accessed: 2019-08-31.

[20] On-boarding manual for organizations to install aadhaar-enabled biometric attendance system, http://attendance.gov.in/assets/doc/Phase-II_of_BAS.pdf, accessed: 2019-08-31.

[21] V. B. Joshi, M. S. Raval, D. Gupta, P. P. Rege, S. K. Parulkar, A multiple reversible watermarking technique for fingerprint authentication, Multimedia Systems 22 (3) (2016) 367–378.

[22] P.-C. Chang, C.-H. Liu, A tsk type fuzzy rule based system for stock price prediction, Expert Systems with applications 34 (1) (2008) 135–144.

[23] A. H. Sonbol, M. S. Fadali, S. Jafarzadeh, Tsk fuzzy function approximators: Design and accuracy analysis, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 42 (3) (2012) 702–712.

[24] A. Ross, A. Jain, J. Reisman, A hybrid fingerprint matcher, Pattern Recognition 36 (7) (2003) 1661–1673.