International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 3558~3568
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp3558-3568

Finding a suitable threshold value for an iris-based authentication system

Narongrit Wangkeeree[1], Sirapat Boonkrong[2]
[1]Faculty of Information Technology, King Mongkut's University of Technology North Bangkok, Thailand
[2]School of Information Technology, Institute of Social Technology, Suranaree University of Technology, Thailand

Article Info

Article history:

Received Oct 5, 2018
Revised Apr 5, 2019
Accepted Apr 17, 2019

Keywords:

Authentication
Iris-based authentication
Threshold value

ABSTRACT

Authentication is the first line of defense of any information technology systems. One of many popular methods used today is biometric, and iris authentication is gaining popularity. However, the threshold value deemed to be secure and appropriate has not been thoroughly studied. Threshold is a value that defines the acceptable amount of the correct bits of the image before securely passing the authentication process. Therefore, the main aim of this research was to find a secure and suitable threshold value used in iris authentication system, where iris localization was done by using Circle Hough Transform technique. Iris image databases v.4 from the Chinese Academy of Sciences Institute of Automatic (CASIA) were used in this research. The way to find the appropriate threshold was to test for the right balance of the GAR, FRR and FAR values when trying to verify the person's identity. The results of the test revealed that the appropriate threshold had the value of 72.9246 percent of all the available bits of the iris image. Both had a high GAR and very low FAR and FRR values. It can be concluded that the obtained threshold value was suitable and secure.

Corresponding Author:

Narongrit Wangkeeree,
Faculty of Information Technology,
King Mongkut's University of Technology North Bangkok,
Bangkok-10800, Thailand.
Email: s5607011910021@email. kmutnb.ac.th

1. INTRODUCTION

Today, Biometric systems are widely used in authentication process in order to identify an individual. Biometric can be divided into two main methods. The first is physical biometric which includes face, fingerprint palm and iris recognition [1-5]. The second is known as behavioral biometric, which includes walking pattern, typing pattern and hand-written signature recognition [6]. Biometric systems can help enhance the security of identification and authentication mechanisms. It is claimed to be stronger than a password recognition system since passwords can be forgotten, disappeared and stolen [7, 8].

One of the most widely used biometric methods is iris recognition. It is proved to be efficient and comes with promising level of security [9]. In this system, an iris is required in order to verify the person's special characteristics [10]. The part of the iris that is used for identity verification is located between the black center part of the eye (pupil) and the white part of the eyeball (sclera).

Authentication by iris recognition involves extraction of a set of iris images of a given eye. They are then used to generate a final template (iris template) and iris data, in bits, are used in iris test by comparing all points with the template. A chance to match all points is least possible though an iris image belongs to the same person [11]. As a result, the determination of error rate between iris template and iris test for authentication is needed. An accuracy rate used for authentication by iris recognition is 60 percent or using statistical formulas for a comparison [12]. However, in the security aspect, the mentioned accuracy rate cannot be workable as a

chance for error rate is quite high. Other experiments focused on Equal Error Rate (EER) value or threshold value of the intersection of FAR and FRR at the acceptance level of approximately 50 per cent, which is a good for usability but not secure [13]. In this paper, a threshold value by intersection of GAR and FRR will be determined. Consequently, this research paid attention to a threshold value from which an accuracy rate from a comparison of iris template and iris test can be acceptable for authentication in a suitable and secure manner. Contribution of this study is, therefore, to find a suitable threshold value for an iris-based authentication system.

The efficiency of the authentication method using iris recognition can be measured and evaluated by using the followings. Firstly, the False Rejection Rate (FRR) is the proportion of authentic or correct iris that are incorrectly denied. Secondly, False Acceptation Rate (FAR) is the proportion of impostors or fake iris that are accepted by the biometric system. The Genuine Acceptance Rate (GAR) is defined as, GAR = 100 – FRR [14].

In order to measure and evaluate the efficiency and security as said above, a threshold value must be set. A too low threshold value may result in a verification of authentication containing a high value of Genuine Acceptance Rate (GAR) and a low value of False Rejection Rate (FRR), but a high value of False Acceptation Rate (FAR), high performance of usability but it is not secure. With a too high threshold value, it can result in a verification of authentication containing a low value of Genuine Acceptance Rate (GAR) and a high value of False Rejection Rate (FRR), and affects the incorrectness of the error rate for False Acceptation Rate (FAR) to be low accordingly. Though authentication with too high of threshold value can respond to the security aspect, the real application cannot be done as correct data can be filtered at the same time. Therefore, an analysis to find an appropriate threshold value should be concerned about real application with secure aspect [15].

2. BACKGROUND KNOWLEDGE AND RELATED WORK

This paper focuses on the finding of a suitable and secure threshold value for an iris authentication system. In order to acquire an understanding of this technique, related theories and researches including iris recognition system and Circle Hough Transform, and methods for finding threshold values will be explained in this section

2.1. Iris recognition system and circle hough transform

Authentication or identification process using iris recognition system is considered to be the most highly secured biometric technology. The efficiency of detection is based on pupil dilation and image acquisition to be used in the recognition process. Other factors include too low and too bright light that can lead to error in detection. Therefore, before using an eye image for test or recognition, a process to reduce an error of recognition should be done. For example, converting image colors to gray scale so as to eliminate a problem of iris color. An eye image is composed of pupil, iris, sclera, eyelashes, eyebrows and the top part of eye. However, a part that can be used for authentication is the black center part of the eye or iris which is located between pupil and the white part of the eyeball (sclera) [16, 17] as seen in Figure 1.

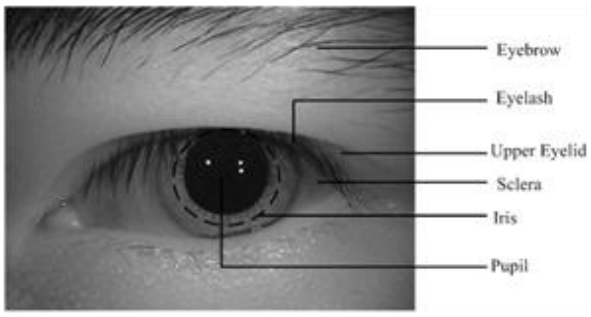


Figure 1. Parts of the human eye

A part of this research is to consider the performance of an iris recognition system implemented by Circle Hough Transform technique to detect an iris image. The iris recognition process can be divided into four parts: eye image acquisition, iris and pupil segmentation, noisy iris image segmentation and feature extraction and encoding.

2.1.1. Eye image acquisition

In this research, images used in iris recognition system are from CASIA Iris Image Database for Biometric Ideal Test [18]. The iris images were captured by a high resolution camera so both dual-eye iris and face patterns were included in the image which made them suitable in this research. Iris images of CASIA were captured with a self-developed close-up iris camera. The most compelling feature of the iris camera is that it has been designed with a circular Near-infrared (NIR LED) array, with suitable luminous flux for iris imaging. Because of this novel design, the iris camera can capture very clear iris images and well-suited for studying. The system allows the user to be anywhere from 1 to 3 feet (0.3 meters) away from the camera that locates the focus on the iris as seen in Figure 2.

2.1.2. Iris and pupil segmentation

The first step is to isolate the actual iris region in a digital eye image. The iris region can be approximated by two circles, one for the pupil/iris boundary and the other one for the iris/sclera boundary. Before detection of these boundaries, the edges of the eye image must be found from pixel intensity. From the edge image, the Circular Hough Transform can be used to detect the centers and radii of the two boundaries according to Daugman Algorithm as seen in Figure 3.

John Daugman proposed Daugman Algorithm, a major part of Iris Recognition System, for segmentation process [13], [14]. The algorithm can be written in a function form as, $Max(r, x_0, y_O)\left|\frac{\partial}{\partial r}G_\sigma(r)^* \int_{r,x,y}\frac{I(x,y)}{2\pi r}ds\right|$. From the Function, $I(x,y)$ is a procedure to find pixel intensity (x,y) from eye images used in a test, r denotes the radius of various circular regions with the center coordinates at (x_0, y_0), σ is the standard deviation of the Gaussian distribution, G_σ denotes a Gaussian filter of scale sigma (σ), (x_0, y_0) is the assumed centre coordinates of the iris, s is the contour of the circle given by the parameters (r, x_0, y_0), Pupil and limbus boundaries are expectation to maximize the contour integral derivative, where the intensity value over the circular borders would make a sudden change. $G_\sigma(r)$ is a smoothing function controlled by σ done by increasing the intensity of the captured image.

Figure 2. Examples of iris images used in this research

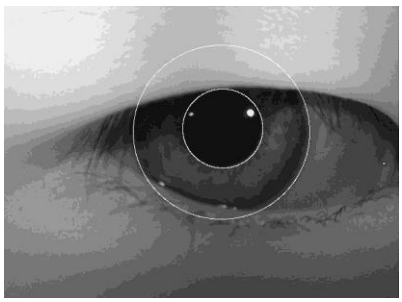


Figure 3. Segmentation Process

2.1.3. Circle hough transform

Circle Hough Transform (CHT) is a feature extraction technique for detecting circles such as eyes by locating circular objects from an input image. Although there are a number of algorithms functioning like Circle Hough Transform, it is more considerably used and effective when compared to others. The quality and color of the image are adjusted before implemented in CHT process. According to Daugman's algorithm, there were some researches relying on the process in detecting eye images for authentication [13, 14] as seen in the (1).

$$\nabla\equiv\left(\frac{\partial}{\partial x},\frac{\partial}{\partial y}\right) and\ G(x,y)=\frac{1}{2\pi\sigma^2}e^{-\frac{(x-x_0)^2+(y-y_0)^2}{2\sigma^2}}.G(x,y) \quad (1)$$

The (1) is a smoothing function by a suitable size of σ from edge detection techniques for iris recognition system.

Edge map is a selection procedure to increase a working efficiency of Circle Hough Transform in order to get more accurate shapes by considering the edge points, as described by the formula; $(x_j, y_j), j = 1,2, \ldots, n, a$ which can be written in the (2) and (3).

$$H(x_c, y_c, r) = \sum_{j=0}^{n} h(x_j, y_j, x_c, y_c, r), \quad (2)$$

Where

$$h(x_j, y_j, x_c, y_c, r) = \begin{cases} 1 \; if \; g(x_j, y_j, x_c, y_c, r) = 0; \\ 0 \; otherwise. \end{cases} \quad (3)$$

An analysis of limbus and pupil which are both modeled as circles and the parametric Function g can be defined in (4).

$$g(x_j, y_j, x_c, y_c, r) = (x_c - y_c)^2 + (y_j - y_c)^2 - r^2. \quad (4)$$

The center of the circle is (x_c, y_c) and Radius is r, when an edge point is out of the circle, the function value is equal to 0and the value of Function g is equal to 1whereas Function h is a basic principle of Circle Hough Transform technique. Even though there are other algorithms proposed for the same purpose such as, but Circle Hough Transform is still deemed appropriate since the algorithm has also been used and applied in [18-22].

2.1.4. The removal of noise factors

In this research, a removal of noise factors that affect an accuracy of the iris recognition system such as upper eyelashes and lower eyelashes in an eye image as the both eyelashes were necessary since they could cause a high number of errors in detection [23] as seen in Figure 4.

2.1.5. Normalization process

It was found that an error in detection could be caused by iris inconsistence/ pupil dilation and light shining into the eyes during data collection as well as an unequal comparison such as a distance of image capture, camera rotation or camera angle, head tilt and eye rolling. Eye normalization process can increase significantly a difference in color level between the black and the white parts of the eye to reduce the error in the detect [24]-[30]. The normalization module uses eye image to transform the iris texture from cartesian to polar coordinates. The process, often called iris unwrapping, yields a rectangular entity.

Figure 5 shows an iris image with detected pupillary and iris boundaries and the normalized region. As seen in Figure 5(b), eyelid occlusion and eyelash presence in the iris region can cause artefacts in the normalization image before feature extraction.

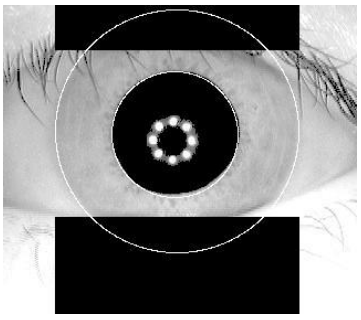
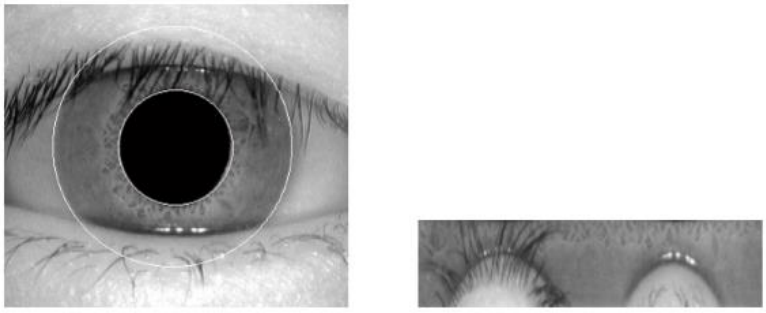


Figure 4. Removal of noise



(a) (b)

Figure 5. Original and normalization iris image, (a) Original Iris Image, (b) Normalization iris image

2.1.6. Feature extraction or data encoding

The system extracted an eye image in a center area between the two circle contours, called the retina, including small black spots in the retina. The data was extracted and transformed into the binary iris by convolving encoding, i.e., bit 0 and bit 1 as seen in Figure 6 [31]. The algorithm for extracting [32] and generating the iris template is as follows.

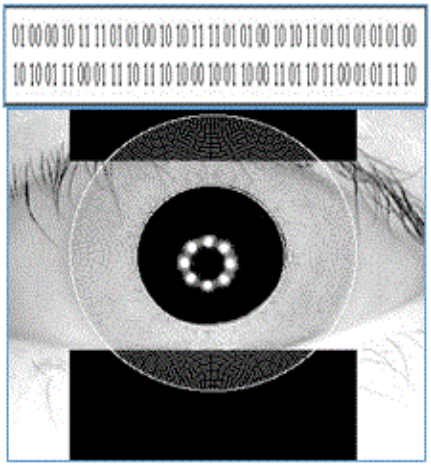


Figure 6. Feature extraction for iris

Feature Extraction Algorithm [32]
length = size (polar_array, 2)*2*nscales
template = zeros (size (polar_array, 1), length)
length2 = size (polar_array, 2)
h = 1: size (polar_array, 1)
mask = zeros (size (template))
For k=1 to nscales **Then**
E1 = E0 {k}
H1 = real (E1) > 0
H2 = image (E1) > 0
H3 = abs (E1) < 0.0001
For i = 0 to (length2-1) **Then**
ja = double (2*nscales*(i))
template (h, ja + (2*k)-1) = H1 (h, i+1)
template (h, ja + (2*k)) = H2 (h, i+1)
mask (h, ja + (2*k)-1) = noise_array (h, i+1) | H3(h, i+1)
mask (h, ja + (2*k)) = noise_array (h, i+1) | H3(h, i+1)
End For
End For
End Algorithm

2.2. Threshold value

Threshold value is a ranging comparison value of data from iris template and iris test. The comparison is done by bit difference at each point and position. The Genuine Acceptance Rate (GAR), False Rejection Rate (FRR) and False Acceptation Rate (FAR) values are also evaluated. Threshold Value has to be in suitable and safe range. If a range of threshold value is too high, it can affect the efficiency of authentication in terms of data filter or data collision of iris data while a correct data might be filtered out at the same time. However, if a range of threshold value is too low, it can result in high efficiency of recognition of correct iris data but increasing data collision of iris data accordingly.

Equal error rate (EER) is a biometric security system algorithm used to predetermine the threshold value for its False Acceptation Rate (FAR) and its False Rejection Rate (FRR). When the rates are equal, the common value is referred to as the equal error rate. The value indicates that the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the higher the accuracy of the biometric system [33] as seen in the Figure 7.

In theory, the correct iris should always value higher than the impostors iris. A single threshold could then be used to separate the correct iris from the impostor's iris [34-36]. Figure 7 shows EER value/Threshold value of the intersection of FAR and FRR at the acceptance level of approximately 50 per cent, which is a good for usability but not secure. In this paper, a threshold value by intersection of GAR and FRR will be determined.

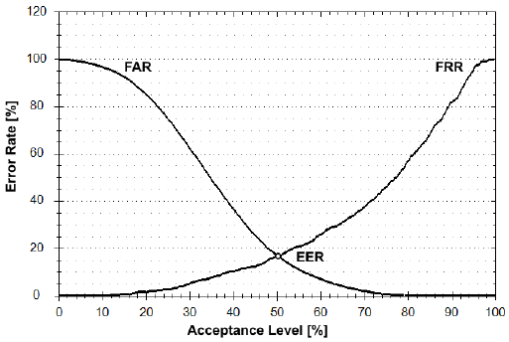


Figure 7. Equal error rate (EER) for FRR and FAR [33]

3. METHODOLOGY

This research used a data set of iris image database from the Chinese Academy of Sciences Institute of Automation (CASIA) which had a total of 22,500 iris images from 1,650 volunteers. All iris images were 8-bit gray-level .JPEG files captured with a circular Near-infrared camera (NIR LED). The iris localization was implemented using Circle Hough Transform technique prior to finding a suitable and secure threshold value. The experimental test was divided into two parts. The first was to use a set of iris images for identifying a threshold value. The second was to use the rest of the iris images to test the validity of the obtained threshold value.

3.1. Data set used to find threshold value

Data set used to find a threshold value contained eyes images from the CASIA V.4 database for Biometric testing. Within that, there was a group of CASIA-Iris-Group1 contained 4,000 iris images from 200 persons.

3.2. Data set used in threshold value testing

The data set that would be used to test the threshold value for the appropriateness contained two groups all of which were from the CASIA V.4 database. The first group of the test data was from the CASIA-Iris-Group3 database which contained iris images created from an algorithm to imitate real eyes. The second group was from the CASIA-Iris-Group2 database. The iris images in this database contained 900 iris images and were gathered from 450 volunteers who took their own images from mobile phone. There were 2,000 iris images in this database. This means that the image quality was not in perfect condition. However, it was decided that this group of images would reflect real-world application more. That was the reason that this database was included in the test dataset. These iris images were used to test the obtained threshold value in terms of accuracy and security. Since an error in authentication from iris recognition partly came from iris images used in a test with regards to brightness, high resolution, and a distance of being away from a camera, these factors were already taken into account when carrying out the test process.

3.3. Threshold value analysis

The analysis threshold value is proposed an overview are divided into two parts: finding a suitable determination and secure threshold value, and testing the threshold value.

3.3.1. Eye images dataset

The eye image datasets used in iris recognition system were from CASIA Iris Image Database V.4 for Biometric Ideal Test. The iris images in the CASIA Iris Image Database V.4 for Biometric Ideal Test were detected or located by the Circle Hough Transform method. The data was then encoded and transformed to create the binary value of the iris by using the algorithm stated in section 2.1.6.

3.3.2. Finding appropriate threshold value

Different ranges and numbers for the threshold values were examined in order to find the appropriate and secure value. The evaluation for the secure threshold value was done by comparing binary bits between the iris template and the iris test. In other words, the binary bits of the iris template and iris test were compared and tested, in both values and positions. Different threshold values were set for the analysis. They were >=50, >=55, >=60, >=65, >=70, >=75 and >= 80 per cent of all the binary bits. Each threshold value was evaluated using three criteria, namely Genuine Acceptance Rate (GAR), False Rejection Rate (FRR) and False

Acceptation Rate (FAR). This was done to determine a suitable and secure threshold value. The process is depicted in Figure 8. The required threshold value should have a high GAR value, low FRR value and the lowest FAR value [35].

Algorithm for Finding the Suitable and Secure Threshold Value This section explains how a suitable and secure threshold value is determined. The algorithm begins with the comparison between the iris template and the iris test. The GAR, FRR and FAR are also determined using the algorithm below. Note that the threshold value in the algorithm is the value set as explained in the previous paragraph.

The comparison is done bit by bit from the first to the nth bit at each point to find the matching percentage. The GAR value is the percentage of the correct iris accepted by the threshold value. The FRR value is a percentage of the correct iris rejected by the threshold value. The FAR value is amount of impostor's irises accepted by the threshold value. Hence, it is necessary that this percentage is as small value as possible so that the impostor's irises are not accepted by the threshold value. The three values can be computed accordingly.

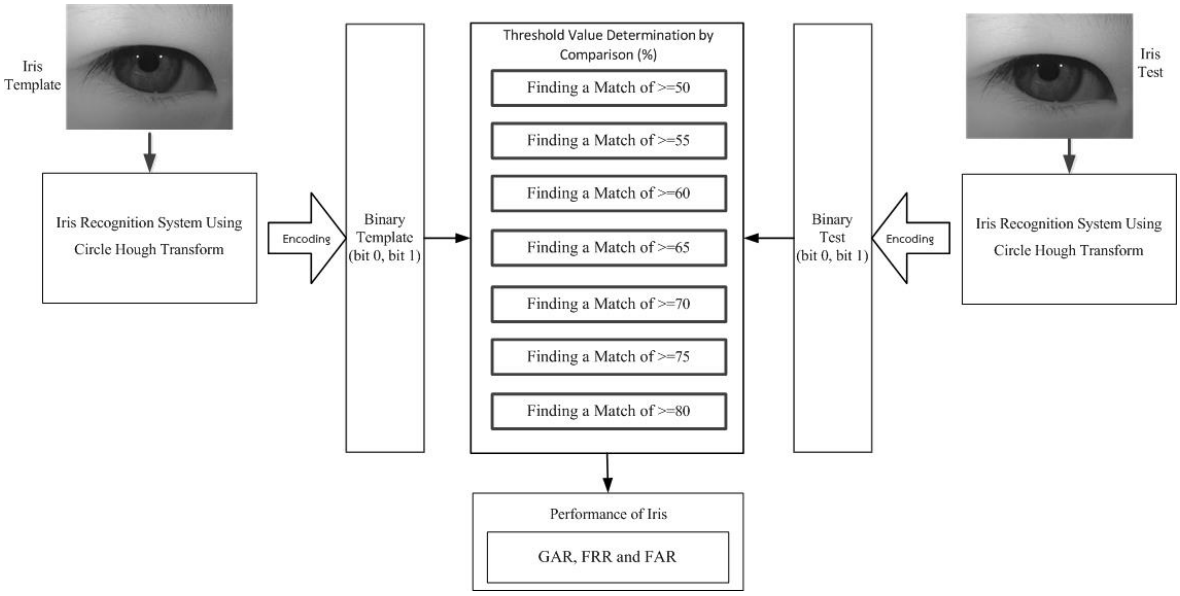


Figure 8. Finding a suitable and secure the threshold value

Bit Comparison Algorithm
Begin
Read IrisTeampate
Read IrisTest
For i=1 to n **Then**
IF IrisTeampate (i) == IrisTest (i) **Then**
Matched Bits = Matched Bits + 1
Else
Unmatched Bits = Unmatched Bits + 1
End IF
End For
Correct = Matched Bits*100/n
IF Compare >=Threshold Value **Then**
Result = Pass
Else
Result = No Pass
End IF
End Compare

4. RESULTS AND DISCUSSION

4.1. Threshold value determination

The threshold value deemed appropriate and secure was found using the method explained in the previous section. In other words, the Circle Hough Transform technique was applied to both the iris templates and the iris test images for localization purposes. The comparisons between the templates and the test images were carried out, having set the values of the threshold. The results that were looked for were the number of the iris test images that passed the specified threshold. The values of GAR, FRR and FAR were obtained as shown Table 1.

Table 1. Results from comparing the iris templates and iris test images against pre-specified threshold values

Performance	Threshold Value						
	>=50	>=55	>=60	>=65	>=70	>=75	>=80
GAR	92.2635	80.6433	72.0825	64.1825	55.4671	44.5329	40.8591
FRR	7.7365	19.3567	27.9175	35.8175	44.5329	55.4671	59.1409
FAR	70.8471	39.2634	24.9367	17.0393	12.6747	9.1360	6.1354

Table 1 shows the comparison results in percentage when evaluating classifier performance of GAR, FRR, and FAR. The aim of this paper was to find a secure threshold value for an iris authentication system. That is, for security purposes, the process was carried out to find the value that gave a low FAR value. Moreover, in terms of correctness, the Acceptance Rate (GAR) value needed to be greater than False Rejection Rate (FRR) value. From Table 1, it can be seen that the threshold values that satisfied the above criteria are the values of >= 70 and >= 75. The threshold value of >= 70 had the values of GAR = 55.4671, FRR = 44.5329 and FAR = 12.6747. The threshold value of >=75 had the values of GAR = 44.5329, FRR = 55.4671 and FAR = 9.1360. The results from Table 1 were then plotted in Figure 9 in order to find a suitable and secure threshold value.

Figure 9 displays three lines of graph. They are the GAR, FRR and FAR values for each of the specified threshold values. The graph showed that the values of GAR and FAR tended to decrease as the threshold value increased. However, the values of FRR went in the opposite direction. In other words, the FRR values increased as the threshold value increased. In reality, a suitable threshold value would be the one that holds a high value of GAR and a low value of FAR. However, it would be difficult to determine an exact value from Table 1. It was, therefore, necessary to include the FRR line into the graph to assist in the determining of the threshold value.

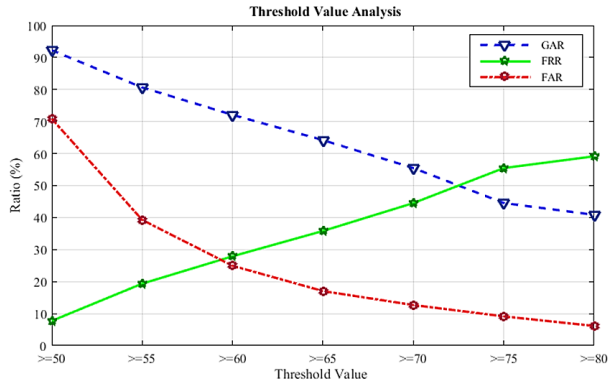


Figure 9. Threshold value analysis

The analysis of threshold ranged with the two-point equation was implemented. In this paper, a threshold value by intersection of GAR and FRR will be determined. Figure 9 shows that the interceptions occurred at two positions. The first was where the FAR line crossed with the FRR line. The second was where the GAR line crossed with the FRR line. The point of interest for the sake of this paper was the intersection of the GAR and FRR lines. This point specified the suitable and secure threshold value because the GAR value was higher than FRR value. At the same time, the FAR value or the false acceptance rate was approximately 10 per cent of all the images, which could be considered suitable and secure [17]. Furthermore, calculated by the two-point equation, the intersection of interest occurred at the threshold value of approximately 72.9246. Our obtained threshold value is higher that those claimed by [13] and [12] whose values are 50 and 60, respectively. Our value would be tested further in the next section.

4.2. Testing the obtained threshold value

The obtained threshold value of 72.9246 per cent of all the available bits was tested for correctness using other data sets as each data set contained different properties according to a condition of data collection. The data sets involved in the test were from two groups of the CASIA V.4 database - CASIA-Iris-Group2 and CASIA-Iris-Group3. Table 2 Shows Data set of test threshold value 72. 9246.

Table 2. Data set of test threshold value 72. 9246

Iris Test	Performance		
	GAR	FRR	FAR
Iris-CASIA-Group2	78.00	22.00	0.00
Iris-CASIA-Group3	77.00	23.00	2.00
Average	77.50	22.50	1.00

From Table 2, the obtained threshold value of 72.9246 was tested against the CASIA-Iris-Group2 database. It was found that 78.00 per cent of the iris test images resulted in acceptance rate (GAR), 22.00 per cent resulted in false rejection rate (FRR), and none fell in the false acceptance rate (FAR) category. This, therefore, can be considered a suitable and safe thresholssd value.

For the CASIA-Iris-Group3 database, it was found that 77.00 percent of all the images resulted in GAR, 23.00 percent of the images resulted in FRR and only 2.00 percent of all the iris images resulted in FAR. Therefore, it can be claimed that the threshold value of 72.9246 is secure since there was no permissible error detected at all.

From the tests on the two databases, it was found that at the threshold value of 72.9246, the average GAR value was 77.50 per cent, the average FRR value was 22.50 per cent and the average FAR value was 1 per cent. It can be seen that the values represent a very small error when compared with other researches such as that of Khan et al. [37] whose false acceptance rate or FAR value was approximately 23 percent.

5. CONCLUSION

An iris authentication system needs a threshold value to analyze an accuracy or rejection of iris images. If the determined threshold value is too high, the error rate of rejecting the genuine iris image can occur. On the other hand, if the determined threshold value was too low, it will result in the error rate of accuracy of incorrect iris images. This research was conducted based on the interest of finding a suitable and secure threshold value on an iris authentication system, with Circle Hough Transform technique used for the localization of the iris. The experimental test of threshold range modeling from the data set of CASIA V.4 iris image database in a group of CASIA-Iris-Group1 revealed that the suitable threshold value was having 72.9246 per cent of the correct bits when compared the iris template with the test iris image. This value of threshold was claimed to be suitable and secure because it provided a higher value of GAR than FRR, while the FAR value was low.

When the obtained threshold value was tested with other data set such as CASIA iris image database version 4.0 in a group of CASIA-Iris-Group2, a total iris images from 1,000 persons, the result revealed that GAR value was 78.00 per cent, FRR value was 22.00 per cent, and FAR value was 0.00 per cent. When tested with the data set of CASIA iris image database version 4.0 in a group of CASIA-Iris-Group3, a total of iris images from 450 persons, it was found that GAR value was 77.00 per cent, FRR value was 23.00 per cent, and FAR value was 2.00 per cent. Therefore, the threshold value at 72.9246 is considered to be the suitable and secure range to be applied for a high security level of authentication method.

REFERENCES

[1] Wu G., Zhao M., Han L. and Li S. "A fingerprint feature extraction algorithm based on optimal decision for text copy detection," *International Journal of Security and Its Applications*, vol. 10(11), pp. 67-78, 2016.

[2] M. M. Mahmoud Musleh, I. I. Ba, K. M. A. Nofal, *et al*., "Improving information security in e-banking by using biometric fingerprint: a case of major bank in Malaysia," *Int. J. Comput. Sci. Inf. Secur*, vol. 10(3), pp. 1–4, 2012.

[3] W. Abdul, A. Alzamil, H. Masri, *et al.*, "Fingerprint and iris template protection for health information system access and security," *J. Med. Imaging Health Inform*, vol. 7(6), pp. 1302–1308, 2017

[4] Ye C., Xiong Z., Ding Y., Zhang X., Wang G., Xu F., and Zhang K. "Parallel joint fingerprinting and encryption for social multimedia sharing based on game of life," *International Journal of Security and Its Applications*, vol. 10(7), pp. 93-102, 2016,

[5] Nandakumar K., Jain A. K., Pankanti S., "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE transactions on information forensics and security*, vol. 2(4), pp. 744-757, 2007.

[6] Jorgensen Z. and Yu T., "On mouse dynamics as a behavioral biometric for authentication," *In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ACM, Mar 2011, pp. 476-482.
[7] Leng L. and Zhang J. "Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security," *Journal of Network and Computer Applications*, vol. 34(6), pp.1979-1989, 2011.
[8] Garg S., Kumar A. and Hanmandlu M., "Biometric authentication using finger nail surface," In 2012 *12th International Conference on Intelligent Systems Design and Applications (ISDA)*, pp. 497-502, Nov 2012.
[9] Zhu W., Zhao Z., and Wu Y., "An algorithm of eyelashes detection for iris recognition," *International Journal of Security and Its Applications*, vol. 10(7), pp. 195-202, 2016.
[10] Rathgeb C., *Iris biometrics: Template protection and advanced comparators*, Salzburg: University of Salzburg, 2011.
[11] Miyazawa K., Ito K., Aoki T., Kobayashi K. and Nakajima, H., "An effective approach for iris recognition using phase-based image matching," *IEEE transactions on pattern analysis and machine intelligence*, vol. 30(10), pp. 1741-1756, 2008.
[12] Daugman J., "How iris recognition works," In *The essential guide to image processing*, Academic Press, 2009, pp. 715-739.
[13] Daugman J., and Downing C., "Effect of severe image compression on iris recognition performance," *IEEE Transactions on information Forensics and Security*, vol. 3(1), pp. 52-61, 2008.
[14] Lee E. C., and Son S. H., "Anti-spoofing method for iris recognition by combining the optical and textural features of human eye," *KSII Transactions on Internet & Information Systems*, vol. 6(9), 2012.
[15] Malik J., Sainarayanan G., and Dahiya R., "Min Max Threshold Range (MMTR) based approach in palmprint authentication by phase congruency features," In *2010 International Conference on Signal and Image Processing*, pp. 388-393, Dec 2010.
[16] Jan F., Usman I., and Agha S., "Reliable iris localization using Hough transform, histogram-bisection and eccentricity," *Signal Processing*, vol. 93(1), pp. 230-241, 2013.
[17] Jan F., Usman I., Khan S. A. and Malik S. A., "Iris localization based on the Hough transform, a radial-gradient operator, and the gray-level intensity." *Optik*, vol. 124(23), pp. 5976-5985, 2013.
[18] Chinese Academy of Sciences Institute of Automation. Casia iris image database Version 4.0. Oct 23, 2016. http://www.sinobiometrics.com
[19] Verma P., Dubey M., Basu S. and Verma P., "Hough transform method for iris recognition-A biometric approach," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1(6), pp. 43-48, 2012.
[20] Pallav P. K. and Granorkar S. R., "Investigation and analysis of Hough-DCT-Hamming distance based method of iris recognition," *International Journal of Innovative Technology and Exploring Engineering*, vol. 3(1), pp. 181-185, 2013.
[21] Mukhopadhyay P. and Chaudhuri B. B., "A survey of Hough Transform," *Pattern Recognition*, vol. 48(3), pp. 993-1010, 2015.
[22] Daugman J., "New methods in iris recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37(5), pp. 1167-1175, 2007.
[23] Min T. H. and Park R. H., "Eyelid and eyelash detection method in the normalized iris image using the parabolic Hough model and Otsu's thresholding method," *Pattern recognition letters*, vol. 30(12), pp. 1138-1143, 2009.
[24] Sulaeman D., Nugroho A. S. and Galinium M., "Iris Segmentation using Gradient Magnitude and Fourier Descriptor for Multimodal Biometric Authentication System," *Journal of ICT Research and Applications*, vol. 10(3), pp. 209-227, 2016.
[25] Sheela S. V. and Vijaya P. A., "Iris recognition methods-survey," *International Journal of Computer Applications*, vol. 3(5), pp. 19-25, 2010.
[26] Proenca H., "Iris recognition: On the segmentation of degraded images acquired in the visible wavelength," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32(8), pp. 1502-1516, 2010.
[27] E. Mohammadi Arvacheh, "A study of segmentation and normalization for iris recognition systems," 2006.
[28] Arvacheh, E. M., "A study of segmentation and normalization for iris recognition systems," 2006.
[29] Proenca H. and Alexandre L. A., "Iris recognition: An analysis of the aliasing problem in the iris normalization stage," In 2006 *International Conference on Computational Intelligence and Security*, vol. 2, pp. 1771-1774. Nov 2006.
[30] Nithyanandam S., Gayathri K. S. and Priyadarshini P. L. K., "A new iris normalization process for recognition system with cryptographic techniques," *arXiv preprint* arXiv:1111.5135, 2011.
[31] Belcher C., and Du Y. "A selective feature information approach for iris image-quality measure," *IEEE Transactions on Information Forensics and Security*, vol. 3(3), pp. 572-577, 2008.
[32] Daugman J., "How iris recognition works," In *The essential guide to image processing*, Academic Press, 2009, pp. 715-739.
[33] Cheng J. M. and Wang H. C., "A method of estimating the equal error rate for automatic speaker verification," In *2004 International Symposium on Chinese Spoken Language Processing*, pp. 285-288, Dec 2004.
[34] Chen Z., Xia X., and Luan F., "Automatic online signature verification based on dynamic function features," In *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Aug 2016, pp. 964-968.
[35] Janratchakool W., Boonkrong S. and Smanchat S., "Finding the optimal value for threshold cryptography on cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6(6), pp. 2979-2988, 2016.
[36] Desmedt Y. and Frankel Y., "Threshold cryptosystems," In *Conference on the Theory and Application of Cryptology* ,Springer, New York, NY, Aug 1989, pp. 307-315.

[37] Khan M. T., Arora D. and Shukla S., "Feature extraction through iris images using 1-D Gabor filter on different iris datasets, In *2013 Sixth International Conference on Contemporary Computing (IC3)*, pp. 445-450, Aug 2013.

BIOGRAPHIES OF AUTHORS

Narongrit Wangkeeree is Ph.D. student at the Faculty of Information Technology, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand. His main area of interesting research is information and network security. He received M.Sc. in Information Technology (Data Communication and Network) from KMUTNB.

Sirapat Boonkrong is an associate professor at the School of Information Technology, Suranaree University of Technology (SUT), Thailand. He received his B.Sc. and Ph.D. in Computer Science from the Department of Computer Science at the University of Bath, UK. His main area of research is information and network security. He is currently a full-time lecturer at the School of Information Technology, SUT, and mainly teaching and researching in the field of information and network security.