JOIV : Int. J. Inform. Visualization, 6(2-2): A New Frontier in Informatics - August 2022 531-539

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

An Improved Approach to Iris Biometric Authentication Performance and Security with Cryptography and Error Correction Codes

Sim Hiew Moi [a,*], Pang Yee Yong [a], Rohayanti Hassan [a], Hishammuddin Asmuni [a], Radziah Mohamad [a], Fong Cheng Weng [b], Shahreen Kasim [c]

[a] *Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, 81300 Skudai, Johor, Malaysia*
[b] *Faculty of Computing and Information Technology, Tunku Abdul Rahman University College, Johor, Malaysia*
[c] *Faculty Sains Komputer Dan Teknologi Maklumat, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia*

*Corresponding author: *hiewmoi@utm.my*

***Abstract*— One of the most challenging parts of integrating biometrics and cryptography is the intra-variation in acquired identifiers between the same users. Due to noise in the environment or different devices, features of the iris may differ when it is acquired at different periods. This research focuses on improving the performance of iris biometric authentication and encrypting the binary code generated from the acquired identifiers. The proposed biometric authentication system incorporates the concepts of non-repudiation and privacy. These concepts are critical to the success of a biometric authentication system. Iris was chosen as the biometric identifier due to its characteristics of high accuracy and permanent presence throughout an individual's lifetime. This study seeks to find a method of reducing the noise and error associated with the nature of dissimilarity acquired by each biometric acquisition. We used Reed Solomon error-correction codes to reduce dissimilarities and noise in iris data. The code is a block-based error correcting code that can be easily decoded and has excellent burst correction capabilities. Two different distance metric measurement functions were used to measure the accuracy of the iris pattern matching identification process: Hamming distance and weighted Euclidean distance. The experiments were conducted with the CASIA 1.0 iris database. The results showed that the False Acceptance Rate is 0%, the False Rejection Rate is 1.54%, and the Total Success Rate is 98.46%. The proposed approach appears to be more secure, as it can provide a low rate of false rejections and false acceptances.**

***Keywords*— Biometric; iris; error correction codes; cryptography; encryption; decryption.**

Manuscript received 15 Dec. 2021; revised 20 Jan. 2022; accepted 18 Apr. 2022. Date of publication 31 Aug. 2022.
International Journal on Informatics Visualization is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

I. INTRODUCTION

Recently, there have been several interesting studies on the interaction between biometrics and Error Correction Codes (ECC). Biometrics is categorized into two diverse types: the physiological or biological characteristics of a human body, including fingerprints, iris, retina, voice, face, etc. [1], [2]. The biometrics are unique to each individual and are highly reliable. The first computer-based authentication mechanisms relied on something that has been known, such as passwords and PINs. Passwords are only reliable if they are not guessed or divulged to others. It has been shown that humans can remember only short passwords [3], and most users tend to choose passwords that are easily guessed by brute force or dictionary attacks [4]. Biometric authentication offers an inextricable link between the authenticator and its owner, which cannot be achieved with passwords or tokens since they cannot be lent or stolen. Additionally, biometrics has the advantage of detecting and preventing multiple identities.

However, security has been a major concern in the conventional automated biometric authentication system. In most conventional biometric authentication work, the biometric templates are stored directly in the database [5]. The match is performed directly by comparing iris biometric templates stored in the database to the acquired biometric templates. Storage and biometric authentication of this kind are not secure and do not provide adequate privacy. There can be serious consequences if the biometric templates are lost. The physiological biometrics of an individual cannot be altered once the image templates are stolen. In order to address the issues above, researchers have been investigating the interaction between biometrics and cryptography. Biometric data is unique to each individual, but it is difficult for us to use it directly as an encryption key. Each image captured during authentication can cause different bits to

appear in the generated template. There have been several attempts by previous researchers to combine biometrics and cryptography [6]–[8].

Every new biometric sample is different by nature, so biometric templates are always variable. The unreliability bits in biometric templates pose the biggest challenge to biometrics [5]. Various noises and errors may be present in the captured iris image due to burst, background error, CCD camera pixel noise, iris distortion, and eyelashes and eyelids obscuring the image. Thus, the template generated from the same iris always differs during each authentication. Differences between iris templates from the same person during every authentication are known as intra variance, while inter variance is the variation of iris templates between two different individuals. This research aims to create an ideal biometric authentication system that meets non-repudiation, privacy, and security criteria. The key element to achieving these criteria is incorporating error correction codes into the iris biometric approach. Error Correction Codes help correct errors on the genuine identification, leading to smaller threshold values, thus improving the user separation of the impostor identification. For matching the iris, we used Hamming Distance and Weighted Euclidean Distance.

A. Biometric Technologies

According to Greek origins, the term "biometrics" means "the measurement of life". Recently, there have been numerous methods for identifying and authenticating your identity, which generally requires something you have (keys, smartcards, ID badges) as well as something you know (passwords, PINs, security questions). Security professionals, however, still believe that biometrics (determining who a person is) are the "best" way to identify and authenticate. There are two different categories in biometrics which are physiological and behavioral [9]. Physiological biometrics is concerned with the distinct traits most people possess, usually determined by their genes, whereas behavioral biometrics is concerned with a person's distinct actions.

Fig. 1 illustrates the various types of biometrics. The term overt biometric refers to the biometrics taken when the user is aware that he is being authenticated by a biometric. In contrast, a biometric is considered covert if data is captured without the consent or knowledge of the user. Including iris biometrics, most biometrics are overt. The user's active participation ensures that the overt biometric has a better accuracy rate and a lower error rate [10]. Some examples of covert biometrics are facial and voice recognition. Faces and voices are two types of biometrics that can be used to determine a person's identity from a distance without the user even realizing it. As these two types of biometrics do not require user consent, they are known as covert biometrics.

Jain et al. [11] identified seven factors for determining biometric strength and weakness. Based on the seven factors below, we will be able to determine the best biometric characteristic. Having these biometric characteristics helps to identify which biometrics are better suited to a given application. Study the effect of the different human fields of view on the behavior of the retina of the people's eye. A comparison was done between these results and the results obtained from Liou and Brennan model lenses).

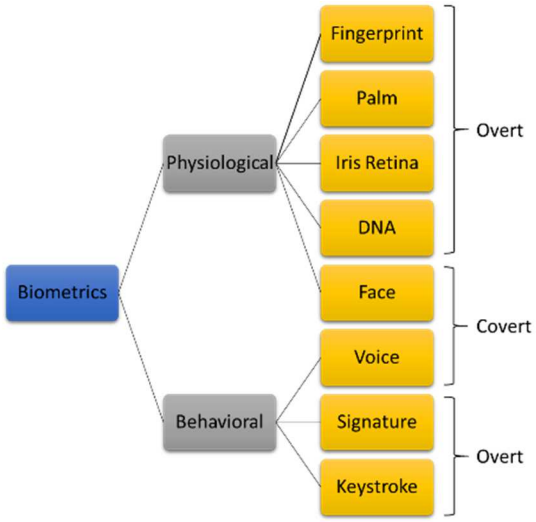

Fig. 1 Different types of biometrics

- Universality: every person accessing the application should possess the trait.
- Uniqueness: the trait should be sufficiently different from that of other users.
- Permanence: A biometric trait must remain constant over time concerning the matching algorithm.
- Measurability: the biometric trait should be able to be acquired, digitized, and processed to extract representative feature sets using devices that do not inconvenience the user.
- Performance: the accuracy of the biometrics recognition
- Acceptability: the willingness to provide their biometric traits information.
- Circumvention: robust enough to withstand a fraud attack.

The following table illustrates the comparison of various biometric technologies concerning the seven factors. In an ideal biometric, the metrics listed below would be well measured. Comparing the various biometrics listed in the table and comparing each of their characteristics, it has become apparent that iris biometrics possess the best biometric characteristic. An iris is characterized by high universality, uniqueness, permanence, high-level performance, and high circumvention [12]. Its high uniqueness provides the iris with a high level of inter-class variability of its feature values. A high permanence and performance level ensured the system or application would receive the most accurate result. A high degree of circumvention also contributes to the robustness of the iris.

TABLE I
COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES [11]

Biometric	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystroke	Low	Low	Low	Medium	Low	Medium	Medium
Hand veins	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice	Medium	Low	Low	Medium	Low	High	Low
Facial thermograph	High	High	Low	High	Medium	High	High
Odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Ear Canal	Medium	Medium	High	Medium	Medium	High	Medium

B. Iris Recognition

The iris pattern is absolutely unique. The state of the art of iris recognition technology captures approximately 249 degrees of freedom [13]. Recognition of the iris is regarded as one of the best biometrics available. It has been reported by Wayman et al. [14] that iris recognition is the most accurate form of biometrics for identifying humans and is suitable for large-scale identification applications. A human being's iris pattern will remain the same throughout his or her lifetime, starting from the fifth week of birth. The pioneer scientist, John Daugman, is credited with creating the first algorithm for iris recognition [15]. A new correlative algorithm for iris verification based on the Hough Transform has been proposed by Wilddes [16]. Most of the algorithms proposed by previous researchers on iris verification utilize this scheme shown in Fig. 2. A biometric system involves collecting biometric data or images, followed by enrolment and verification. Initially, an iris recognition system captures an image of the subject's eye. Next, the iris is segmented and normalized for feature extraction. The iris segmentation process is intended to determine an iris image's outer and inner boundaries. A normalization process involves transforming the iris into polar coordinates, a process known as unwrapping, and a feature extraction process comes after determining the segmented normalized image. A one-dimensional Gabor filter is used for extracting the features of iris in our approach. The feature extraction procedure is to generate binary strings from the normalized iris images. Some researchers used Gabor filters in two dimensions which are relatively more complex than the algorithm of using one dimension. Fig. 3 shows the example segmentation of iris for the CASIA version 1.0 database. The rubber sheet model shown in Fig. 4 and Fig. 5 is used in normalization. The bitwise template shown in Fig. 6, which contains the bits information, will be produced after the feature extraction codification.

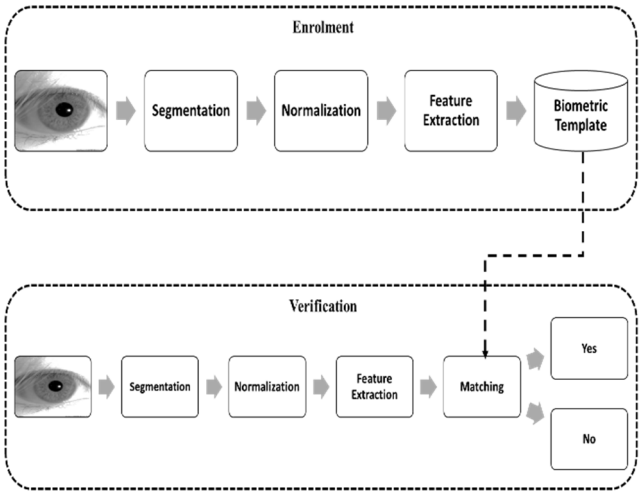

Fig. 2 Iris Biometric Process Block Diagram

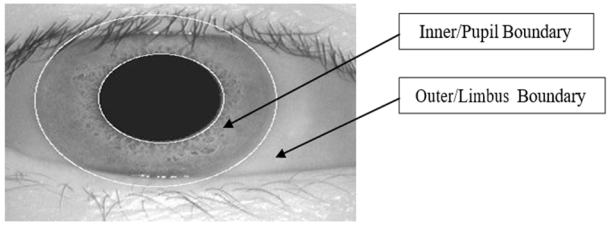

Fig. 3 Iris Segmentation for CASIA Database version 1.0

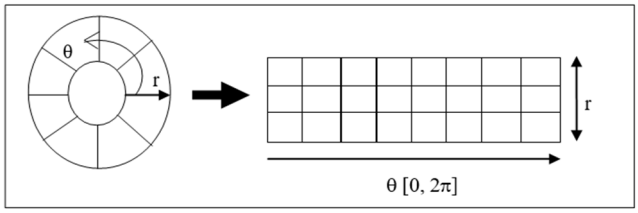

Fig. 4 Rubber sheet model (concentric circle)

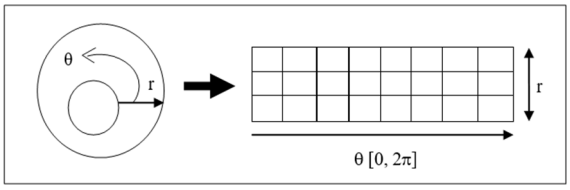

Fig. 5 Rubber sheet model (non-concentric circle)

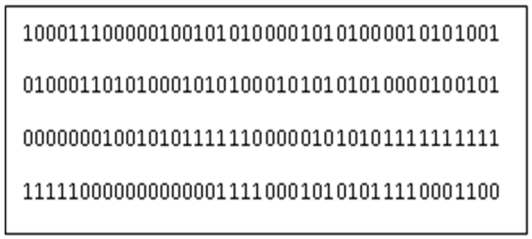

Fig. 6 Iris Code Template

C. Error Correction Codes (ECC)

The main purpose of Error Correction Codes (ECC) is to fix errors that occur in the transmission over some noisy channels. In the cryptography concept, it may be impossible to read the plaintext whenever a bit is changed in the ciphertext. Therefore, there is a need to detect and correct errors. ECC has been suggested to deal with the noise in biometric data. Depending on the type of errors found on the biometric identifier, error correction codes were used to eliminate any differences between enrollment and verification readings. [17]. Error correction codes address variability between the iris patterns. Instead of correcting errors in iris codes, they eliminate the error in codewords caused by the biometric data. It is used to correct the error in the test iris sample compared to the reference sample. The performance of the authentication approach can be significantly improved when this ECC is used properly. Irving Reed and Gus Solomon introduced the Reed Solomon Code on January 21, 1959 in their paper "Polynomial Codes over Certain Finite Fields" [18]. The Reed Solomon Code is a block-based error-correcting code that can be easily decoded and has good burst-correction capabilities. A tuple (n,k,t) describes this block code: n,k,t, where n denotes the length of Reed Solomon codes, k the length of the message, and t the number of correct errors. Table II shows the basic idea of error correction codes, while Fig. 7 shows the block diagram showing the error correction codes for biometrics. k is the check bits, c is the encoded codeword, c' is the corrupted codeword and k' is the regenerated key. Using Error Correction Codes, we will get a smaller hamming distance value which means that the difference between the two iris codes is relatively smaller. Table III shows the example calculation of the error correction code with the check bits. XOR operation is performed on the incoming data bits; the results will return wrong (Logical False) if an error occurs. If there are no errors in the incoming data bits, the result will return correct (Logical True). The error will be detected first and is corrected by inverting it.

$$HD(b, b') \geq HD(b, b1')$$

b = biometric during enrolment
b' = biometric for verification without using ECC
b1'= biometric for verification after using ECC to correct errors

TABLE II
BASIC IDEA OF ERROR CORRECTION CODES

Number of errors	Read data	Decoded data
0 errors	000	0
	111	1
1 error	00<u>1</u>	0
	0<u>1</u>0	0
	<u>1</u>00	0
	11<u>0</u>	1
	1<u>0</u>1	1
	<u>0</u>11	1

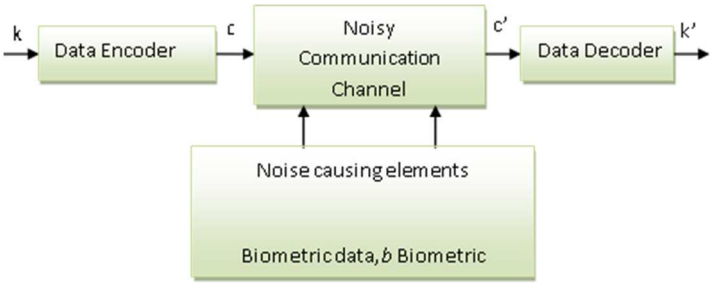

Fig. 7 Block Diagram showing the Error Correction Codes for Biometrics.

TABLE III
ERROR CORRECTION CODES CHECKING BIT

	Incoming Data Bits				Check Bits		
	A	B	C	D	E	F	G
1	0	0	0	0	0	0	0
2	0	0	0	1	0	1	1
3	0	0	1	0	1	0	1
4	0	0	1	1	1	1	0
5	0	1	0	0	1	1	0
6	0	1	0	1	1	0	1
7	0	1	1	0	0	1	1
8	0	1	1	1	0	0	0
9	1	0	0	0	1	1	1
10	1	0	0	1	1	0	0
11	1	0	1	0	0	1	0
12	1	0	1	1	0	0	1
13	1	1	0	0	0	0	1
14	1	1	0	1	0	1	0
15	1	1	1	0	1	0	0
16	1	1	1	1	1	1	1

D. Template Matching

Different types of template matching methods can be used for pattern recognition. A distance metric compares binary bits between two patterns in an image. Several methods can be used for images in biometric recognition. Manhattan Distance, Euclidean Distance [19], Absolute Distance [20], Standard Related Coefficient [16], [19], [20], Neural Network [21], Weighted Euclidean Distance, and Hamming Distance are examples of feature matching methods. Different distance metrics use different formulas and have different matching characteristics, which can affect the matching accuracy between the two templates and the computation time involved in the matching process. A good template distance metric similarity measure will consider the overall data's statistical characteristics before deciding its suitability for the system. Hamming Distance and Weighted Euclidean Distance are template distance metrics that have the advantage of simpler formulas in measurement and are therefore suitable for iris

biometric authentication. Thus, only Hamming Distances and Weighted Euclidean Distances are evaluated in this study.

E. Past Works

Daugman wrote the first history of iris biometrics. Researchers in this field use Daugman's concept as a standard reference model [22]. Several recent studies have integrated cryptography into biometrics. In biometric cryptography, the main concern is variability in the images captured by the same users during each biometric acquisition. Cryptography methods such as RSA, AES, and DES are not suitable for storing biometric templates in encrypted form and matching them directly. The result of the encrypted feature can be greatly affected by changing just a few bits of the feature set extracted from the biometric. This issue has been addressed in some studies.

A novel secure iris verification system based on BCH codes was proposed by Yang et al. [23]. In the research, hash functions are used to compare iris images. There is a downside to BCH codes in that they provide non-uniform error correction. They mentioned that their results reduced from 6% to 0.8% but did not specify how many iris images were tested or what database was used.

Hao et al. [5] and Kanade et al. [24] proposed using concatenated codes as their error correction codes. Concatenated codes may produce better results in terms of accuracy, but they are harder to tune and require more computation time. In a real-time application, the authentication system would be much slower. The results obtained by Hao et al. [5] are 0.47% FRR and 0% FAR. Kanade et al. [24] propose to use concatenated codes by combining Hadamard and Reed Solomon codes. By testing with NIST-ICE database, they obtained a result of 0.055% FAR and 1.04% FRR. However, the system still has some weaknesses in terms of security [25]. For Error Correction Codes, Bringer et al. [26] proposed an optimal iris fuzzy sketch based on Reed Muller and Product Codes. Their approach is based on a minimum sum iterative decoding method. They tested their approach using the NIST-ICE database. Their authentication result is 5.62% of FAR and 10-5 of FRR respectively.

We propose a secured iris biometric authentication approach that uses iris biometrics and passwords together in order to increase the security and overall success rates of our iris biometric authentication approach. In our approach, we use ECC to minimize the signal noise of biometric data and reduce the variability. The details of our approach are described in Section 3.

II. Material and Method

In this section, we discuss the overall iris biometric verification process. These phases include the enrollment process and the verification process. This section will also discuss the experimental datasets and the template matching distance metric. In Sections 4.2.1 and 4.2.2, the steps of the enrollment and verification processes are described.

A. Datasets

This experiment utilized the CASIA Iris Database Version 1.0. The CASIA Iris Database Version 1.0 contains 256 grayscale iris images from 108 candidates, each of which has seven images collected during two sessions. This image was captured specifically for iris recognition research and for educational purposes using special digital optics from the National Laboratory for Pattern Recognition in China. Each iris image is an 8-bit gray-level JPEG collected under near-infrared illumination.

B. Enrolment Process

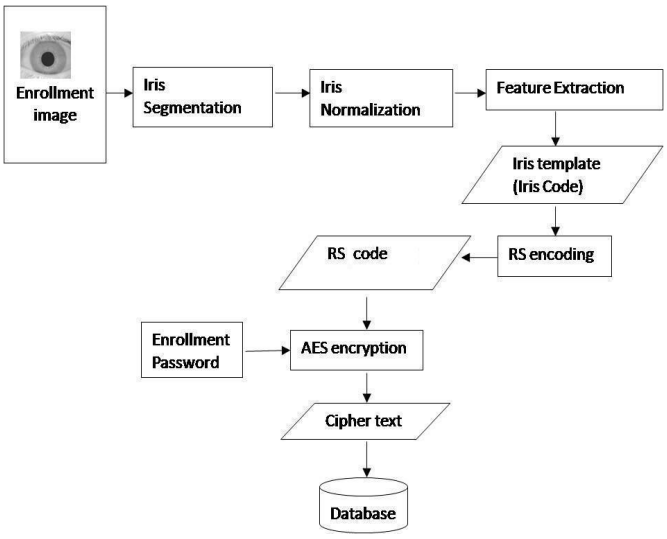

Fig. 8 Enrolment Process Diagram

Fig. 8 illustrates how the enrollment process works. Following is a description of each step.

Step 1: An iris is extracted through iris segmentation, iris normalization, and feature extraction processes, and from these processes, an iris template and iris binary code are generated.

Step 2: The second step in the process is to encode the binary code for the iris image using the Reed Solomon Code Encoding Process.

Step 3: In step three, once the enrollment process has been completed, you will receive your RS Code.

Step 4: To generate a cipher text, the RS Code is then encrypted by using the Advanced Encryption Standard Cryptography Algorithm with the enrolment password, as described in Step 3.

Step 5: The generated cipher text is then stored in the database as step five.

C. Verification Process

The verification process is illustrated in Fig. 9, and the steps are outlined below.

Step 1: Using iris segmentation, normalization, and feature extraction, the iris binary code and the iris template of a tested iris image are obtained.

Step 2: As part of Step 2, a password is required for user authentication, and this password is the same as the enrollment password used to decode the cipher text obtained from the database using AES decryption process to obtain the RS code.

Step 3: Using the Reed Solomon decoding process, the RS code is then used to decode the testing iris template code to obtain the enrolled iris template code. During this process,

Reed Solomon decoding is also used to correct the error of the testing iris template code.

Step 4: The two iris template codes are then matched using a Distance Metric Function (Hamming Distance, Weighted Euclidean Distance).

Step 5: If the iris template matches the threshold value, the user will be authenticated, otherwise, the system will exit.

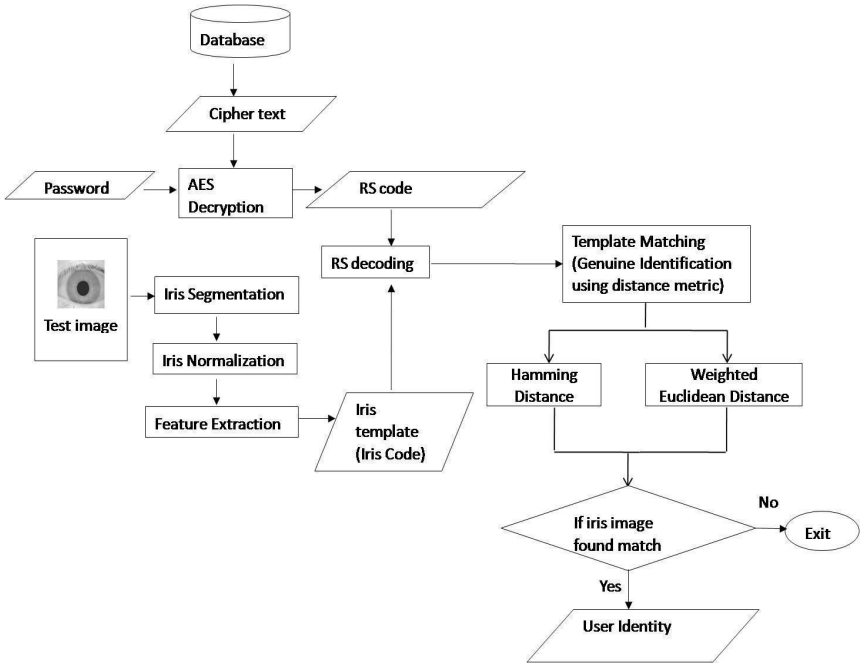

Fig. 9 Verification Process Diagram

D. Reed Solomon Codes

Fig. 10 shows a diagram of the Reed Solomon Error Correction Process for Iris Verification. During the decoding process, the difference bit of the two iris images is considered a corrupted codeword (noisy code). The Reed Solomon Coding algorithm has several important parameters, including number of bits per symbol, m; length of Reed Solomon Codes, n; message length, k; and a number of errors to be corrected, t.

m =? (Number of bit per symbol)
$n = 2^m - 1$
$k = n - 2t$

n represent the length in RS codes
k represents the message length
t represents the number of errors to be corrected.

In our research,
$n = 2^{10} - 1 = 1023$, t =250, k= 523.

Therefore, (1023, 523,250) RS coding algorithm is selected.

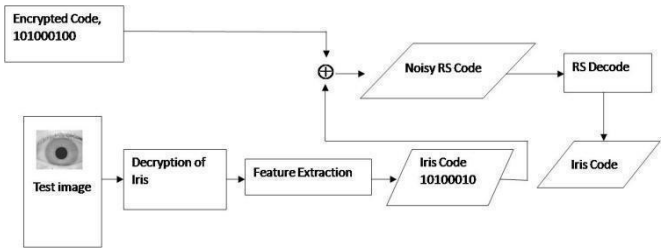

Fig. 10 Diagram of Reed Solomon Error Correction Process on Iris Verification

E. Template Matching Distance Metric

Pattern recognition can be performed using many different template matching methods. In this study, two distance metrics are being applied to iris recognition. There are two distance metrics used: Hamming Distance and Weighted Euclidean Distance

1) Hamming Distance (HD): Hamming Distance (HD) measures how many of the same bits occur between two-bit patterns. In the case of the bit patterns A and B, HD equals the total number of different bits over the total number of bits in the bit pattern, n. The formula for this is shown in Equation 1.

$$HD = \frac{1}{n}\sum_{i=1}^{n} \quad A_i \oplus B_i \tag{1}$$

The Hamming Distance between two patterns derived from the same iris should be close to zero. This is because both patterns are highly correlated, and iris codes should agree on bits. There will be some variation when comparing two intra-class iris templates due to the noise and error detected. Therefore, Hamming Distance 0,0 cannot occur in practice.

2) Weighted Euclidean Distance (WED): Weighted Euclidean Distance is another distance measurement metric used in this study for pattern matching. We determine whether two iris patterns match based on the Weighted Euclidean Distance. The equation for the weighted Euclidean distance is shown in Equation 2.

$$WED = \sum_{i=1}^{n} \quad \frac{(B_i - A_i)^2}{(\delta A_i)^2} \tag{2}$$

F. Performance Measure

The performance of the authentication approach must be quantified in order for us to measure its success. We also need a statistical method to measure the effectiveness and efficiency of this research approach. These measures are:

- FAR (False Acceptance Rate)
- FRR (False Rejection Rate)
- TSR (Total Success Rate)

1) False Rejection Rate (FRR): False Rejection Rate (FRR) can be described as the probability that an individual enrolled in a program will not be identified by the system. It represents the probability that a user is being rejected despite making a true claim about their identity. There are two possible causes for the false rejection rate. The first is the setting of the matching threshold that is too low. A second reason is that the biometric feature presented differs significantly from the enrolled template or is not close enough. In order to ensure a higher level of reliability of the results, as well as to obtain a high probability that the FRR we calculate is significant, we perform 648 (108*6) genuine identifications on every user. Calculating the FRR is generally straightforward. It is calculated by counting the number of times a particular user has failed to authenticate and then dividing by the number of times the user has attempted authentication. The formula for determining the FRR is shown in Equation 3.

$$FRR = \frac{Number\ of\ False\ Rejection}{Number\ of\ Enrollee\ Verification} \quad (3)$$

2) False Acceptance Rate (FAR): False Acceptance Rate (FAR) refers to the probability of identifying an individual as someone else. In other words, it's possible for a user to make a false claim about his/her identity but still be able to be verified as that false identity. In order to ensure a high probability that the FAR calculated is statistically significant, we would have to combine all the users we have. Because of this, we do 80892 (108×107×7) imposter or FAR testing for the CASIA database. The number of 80892 comes from 108 users multiplied by 107 other users, with 7 iris images. The formula involves calculating the total number of falsely authenticated users and dividing it by the total number of users. The formula is shown in equation (4).

$$FAR = \frac{Number\ of\ False\ Acceptance}{Number\ of\ Imposter\ Verification} \quad (4)$$

3) Total Success Rate (TSR): Another performance metric is the Total Success Rate (TSR). Calculating TSR can only be done after calculating FAR and FRR. It can be defined as or represent the verification rate of the overall iris cryptography system. TSR can be affected directly by either the FAR or the FRR [22]. The formula of TSR is shown in equation (5).

$$TSR = \left(1 - \frac{FAR+FRR}{Total\ number\ of\ accesses}\right) \times 100\% \quad (5)$$

III. Results And Discussion

To show the False Rejection Rate (FRR) and False Acceptance Rate (FAR) with its corresponding threshold value, we conducted 648(108*6) genuine identifications and 80892(108*107*7) imposter checks. The approach was implemented, and the results were analyzed using MATLAB. Images used for testing were obtained from CASIA Database version 1.0. This study has been conducted on two approaches which are iris authentication without Error Correction Codes and also iris authentication with Error Correction Codes (ECC) for comparison in order to show the difference between both approaches.

A. Result Analysis for Approach without Error Correction Codes and with Error Correction Codes using Hamming Distance

Table IV shows the results of experiments using Hamming Distance as the distance metric measurement without Error Correction Codes for different threshold values. As a result of the analysis, 0.37 provides the best FAR and FRR and is therefore selected as the threshold value for the proposed iris authentication system. Even though the threshold value of 0.4 gives results of a higher total success rate, it is not chosen because the system did not allow successful decryption from an imposter. Therefore, the FAR is 0%, and the FRR obtained from the result is 18%. A total success rate of 82% was achieved.

TABLE IV
EXPERIMENT RESULT FOR DIFFERENT THRESHOLD VALUES USING HAMMING DISTANCE FOR APPROACH WITHOUT ERROR CORRECTION CODES

Threshold value	False Acceptance Rate, FAR%	False Rejection Rate, FRR%	Total Success Rate, TSR%
0.2	0	99	1
0.25	0	88	22
0.3	0	55	45
0.35	0	26	73
0.36	0	22	78
0.37	***0***	***18***	***82***
0.38	0.01	15	85
0.39	0.01	13	87
0.4	0.02	11	89
0.41	0.11	9	90.9
0.42	0.38	7	92.6
0.43	1.21	6	92.8
0.44	3.68	4	92.3
0.45	10.21	2	87.8
0.5	99.37	0	0.63

Table V shows the experimental results using Hamming Distance as the distance metric measurement. These results were obtained by integrating Error Correction Codes (Reed Solomon Codes) into the iris authentication system. The result shows that 0.37 is also the best threshold value for FAR and FRR. According to the result, the FRR is 1.54%, and the FAR is 0%. The overall success rate (TSR) achieved is 98.46%.

TABLE V
EXPERIMENT RESULT FOR DIFFERENT THRESHOLD VALUES USING HAMMING DISTANCE FOR APPROACH WITH ERROR CORRECTION CODES

Threshold value	**False Acceptance Rate, FAR%**	**False Rejection Rate, FRR%**	**Total Success Rate, TSR%**
0	0	100	0
0.05	0	93.17	6.83
0.1	0	77.19	22.81
0.15	0	55.55	44.45
0.2	0	33.52	66.48
0.25	0	15	85

0.3	0	6.43	93.57
0.35	0	2.92	97.08
0.36	0	2.47	97.53
0.37	***0***	***1.54***	***98.46***
0.38	0.006	1.23	98.77
0.39	0.007	0.77	99.23
0.4	0.028	0.39	99.58
0.45	10.2	0	89.8
0.5	99.4	0	0.6

G. Histogram Comparison between Approach without Error Correction Codes and Approach with Error Correction Codes using Hamming Distance.

Fig. 11 shows the comparison between approaches without Error Correction Codes and approaches with Error Correction Codes for genuine iris testing. Hamming Distance is used as the distance metric in this experiment.

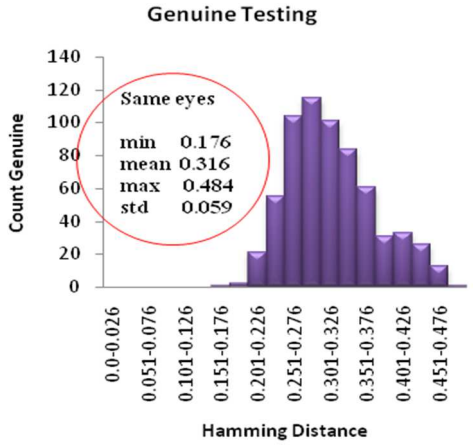

Fig. 11 Histogram Comparison for Approach without ECC and Approach with ECC on Iris Genuine Testing

Fig. 11 shows that the matching threshold value becomes smaller when Error Correction Codes (ECC) are incorporated into the iris biometric authentication process. Both the approach of iris biometric verification without ECC and the approach of iris biometric verification with ECC were examined using 648(108*7) genuine iris patterns. The upper side of the figure shows the histogram for genuine testing without ECC, while the lower side shows the histogram for genuine testing with ECC. As a result, the mean of the overall distribution of the genuine testing with ECC becomes 0.169, which is significantly smaller than the approach before the integration of ECC into iris verification, which is 0.316. This is due to the powerful capability of the ECC to correct the noise in the iris code and the ability to reduce the threshold value, which reduces intra variances and increases inter variances of the iris.

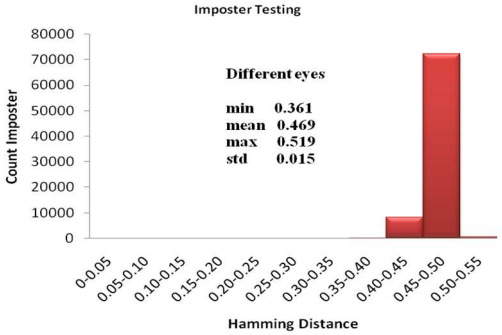

Fig. 12 Hamming Distance between Iris Code for Imposter Testing

H. Comparison between approach using Hamming Distance and Approach using Weighted Euclidean Distance

Table VI and Table VII below provide the FAR and FRR for measurement using Hamming Distance and Weighted Euclidean Distance at different thresholds. According to the results, 0.37 is the ideal threshold value compared to other threshold values using Hamming Distance measurement metric. In contrast, using Weighted Euclidean Distance as a measurement method, the best FAR and FRR value is 32. Comparing results obtained using different metric measurements, Hamming Distance with a Total Success Rate of 98.46% is slightly better than Weighted Euclidean Distance with a Total Success Rate of 96.8%.

TABLE VI
EXPERIMENT RESULT FOR DIFFERENT THRESHOLD VALUES USING WEIGHTED EUCLIDEAN DISTANCE FOR APPROACH WITH ERROR CORRECTION CODES

Threshold value	False Acceptance Rate, FAR%	False Rejection Rate, FRR%	Total Success Rate, TSR%
0	0	98.6	1.4
10	0	49.85	50.15
15	0	23.3	76.7
20	0	15.28	84.72
25	0	7.72	92.28
30	0	4.01	96
31	0	3.70	96.3
32	*0*	*3.20*	*96.8*
33	0.0025	2.10	97.2
34	0.03	2.40	97.5
35	0.12	2.16	97.72
40	4.24	1.24	94.52
45	19.66	1.08	79.26
50	40.85	0.77	58.38
55	59.39	0.31	40.3
60	73.43	0.15	26.42
65	82.13	0	17.87
70	88.13	0	11.87
75	92.22	0	7.78
80	94.9	0	5.1
85	96.89	0	3.11
90	97.86	0	2.14
95	98.52	0	1.48
100	98.96	0	1.04

For imposter testing versus genuine testing for the approach with ECC, the overall mean value obtained for imposter testing is 0.469 (Fig. 12), which shows a large gap compared to the mean for genuine testing, which is only 0.169. The large range of threshold values is easier to distinguish between genuine and imposter. As a result, we obtain a higher accuracy result that results in low false rejection rates (1.54%) and zero false acceptance rates.

TABLE VII
SPEED ANALYSIS OF PROCESSES IN THE IRIS RECOGNITION APPROACH

Critical steps in Iris Recognition	Average Time
Image Processing of Iris Image, Segmentation, Normalization, and Feature Extraction	47.504 second
Template Matching Metric (Hamming Distance)	0.0424 second
Template Matching Metric (Weighted Euclidean Distance)	34.2169 second

The speed analysis of the Iris recognition process is shown in table V. Image processing of the iris image, segmentation, normalization, and feature extraction takes around 47.504

seconds. The verification process for the iris recognition approach using Template Matching Metric (Hamming Distance) usually takes 0.0424 seconds, which is much faster than the verification process for the iris recognition approach using Template Matching Metric (Weighted Euclidean Distance), which takes 34.2169 seconds on average. A better accuracy rate and higher verification speed can be achieved using Hamming Distance based on results obtained from both accuracy rates and time spent.

IV. Conclusion

This research is aimed at producing a robust and reliable iris recognition method by minimizing the intra variance (FRR) and maximizing the inter variance of the iris. The templates in the conventional biometric systems are stored directly in the database, so if stolen, they will become unusable in that system and other systems that rely on that biometric. Error correction codes, or ECCs, help reduce the variability and noise in biometric data. Reed Solomon Codes were used in this study to correct errors. There is no doubt that Reed Solomon Codes are very powerful error correction codes. In addition to iris biometric authentication, they can also be used to eliminate burst errors caused by undetected eyelashes or reflections from flash or lighting. Using Reed Solomon Codes, the FRR is reduced from 18% to around 1.54%, dramatically impacting iris recognition. In order to separate genuine identification from imposter identification, hamming distance and Weighted Euclidean Distance are the distance metrics used. The smaller the threshold value, the greater the similarity between the two patterns. The performance of the two distance metric functions is nearly the same. We found that Hamming Distance performed better than Weighted Euclidean Distance among the two distance functions. In parts of the research, AES has been used. It is used in order to ensure a more secure transaction of the password. With the combination of password usage and iris biometric authentication, the level of security has also increased. AES has been a world standard algorithm for many years to protect sensitive information.

No single biometric can satisfy all the requirements imposed by all applications, such as accuracy, practicality, cost, etc. In the future, multimodal schemes or hybrid schemes that provide a higher level of security and more benefit to the template can be proposed. In addition, another suggestion for future research is to examine low-cost devices that can capture iris images. The cost of the iris scanner equipment is one of the main reasons for the low acceptability of iris biometrics. Therefore, developing iris authentication using low-cost devices such as webcams or mobile phones will greatly benefit society.

Acknowledgment

This work was supported/funded by the Ministry of Higher Education under the Fundamental Research Grant Scheme (FRGS/1/2020/ICT02/UTM/03/1).

References

[1] M. Al Rousan, and B. Intrigila, "A Comparative Analysis of Biometrics Types: Literature Review," Journal of Computer Science, vol. 16, no. 12, pp. 1778-1788, 2020.

[2] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," *International Journal of Applied Engineering Research,* vol. 13, no. 5, pp. 2276-2297, 2018.

[3] C. Kuo, S. Romanosky, and L. F. Cranor, "Human selection of mnemonic phrase-based passwords." pp. 67-78.

[4] B. Brumen, "Security analysis of Game Changer Password System," International Journal of Human-Computer Studies, vol. 126, pp. 44-52, 2019/06/01/, 2019.

[5] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE transactions on computers, vol. 55, no. 9, pp. 1081-1088, 2006.

[6] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication." pp. 45-52.

[7] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice." pp. 202-213.

[8] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," International journal of Information security, vol. 1, no. 2, pp. 69-83, 2002.

[9] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, pp. 4-20, 2004.

[10] M. L. Ali, J. V. Monaco, C. C. Tappert, and M. Qiu, "Keystroke Biometric Systems for User Authentication," Journal of Signal Processing Systems, vol. 86, no. 2, pp. 175-190, 2017/03/01, 2017.

[11] A. Jain, R. Bolle, and S. Pankanti, Biometrics: personal identification in networked society: Springer Science & Business Media, 1999.

[12] A. Ahire, A. Jambhale, T. Patil, M. Chavan, A. Nerurkar, and R. V. Deolekar, "Comparative Analysis of Biometric Systems." pp. 895-901.

[13] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE transactions on pattern analysis and machine intelligence, vol. 15, no. 11, pp. 1148-1161, 1993.

[14] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Biometric systems: Technology, design and performance evaluation: Springer Science & Business Media, 2005.

[15] J. Daugman, "Iris recognition," Handbook of biometrics, pp. 71-90: Springer, 2008.

[16] R. P. Wildes, "Iris recognition: an emerging biometric technology," Proceedings of the IEEE, vol. 85, no. 9, pp. 1348-1363, 1997.

[17] S. Ziauddin, and M. N. Dailey, "Robust iris verification for key management," Pattern Recognition Letters, vol. 31, no. 9, pp. 926-935, 2010.

[18] I. S. Reed, and G. Solomon, "Polynomial codes over certain finite fields," Journal of the society for industrial and applied mathematics, vol. 8, no. 2, pp. 300-304, 1960.

[19] P. Ariyapreechakul, and N. Covavisaruch, "An improvement of iris pattern identification using radon transform," ECTI Transactions on Computer and Information Technology (ECTI-CIT), vol. 3, no. 1, pp. 45-50, 2007.

[20] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, "A system for automated iris recognition." pp. 121-128.

[21] C.-H. Chen, and C.-T. Chu, "Low complexity iris recognition based on wavelet probabilistic neural networks." pp. 1930-1935.

[22] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," Computer vision and image understanding, vol. 110, no. 2, pp. 281-307, 2008.

[23] S. Yang, and I. Verbauwhede, "Secure iris verification." pp. II-133-II-136.

[24] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris." pp. 59-64.

[25] X. Wu, N. Qi, K. Wang, and D. Zhang, "A novel cryptosystem based on iris key generation." pp. 53-56.

[26] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor, "Optimal iris fuzzy sketches." pp. 1-6.