Biometric Authentication Based on Hash Iris Features

Dalal N. Hammod *dalal_hammod@yahoo.com*
University of Al-Nahrain
College of Science
Computer Science Department
Baghdad/Iraq

Abstract

With an increasing emphasis on security, automated personal identification based on biometrics has been receiving extensive attention since its introduction in 1992. In this study, authentication system contained two parts: registration part and matching part. In both parts, iris image is used for personal identification. Localization of inner boundary only, extracted a region from the iris (without eyelashes problem), a feature vector is deduced from the texture of the image. The feature vector is used for classification of the iris texture, then it's treated by the hash function to produce the hash value (authentic value of a person). In matching part, produced hash value searched in the authorized person's database for taking a decision (success or fail) of the authentication. The method was evaluated on iris images takes from the CASIA iris image database version 1.0 [15]. The experimental results show that the vector extracted by the proposed method has very discriminating values that led to a recognition rate of over 100% on iris database. Also, authentication system is very accurate because it's used a secure method of authentication that iris-biometric and a hash function for avoiding stealing data from database.

Keywords: Biometric, Iris Features, Laplace Mask, Authentication System, Hash Function.

1. INTRODUCTION

Pin numbers, email passwords, credit card numbers, and protected premises access numbers all are sort of identity usually used to identify persons but these are the traditional methods of security. Unfortunately, all these identities have some common shortcoming; i.e. they can easily be stolen or guessed. This leads to some logical problems: i.e. people tend to forget multiple, lengthy and varied passwords, therefore, they use one strong password for everything but, unlike, this allows the successful thief to gain access to all the protected information. However, the written identities may be replaced with some of the physical traits used by biometric authentication program [1].

In recent years, personal identification methods used the computers and intelligent software. A good biometric is characterized by the use of features that are highly unique (so that the chance of any two people having the same characteristic will be minimal), easily captured, prevent misrepresentation of the feature, and stable (i.e. Features do not change over time) [2]. The stability conditions are biological behaving which could be classified as [3]:

I- Physiological characteristics: including fingerprint, hand geometry, eye (iris and retina) patterns, and facial features.
II- behavioral characteristics: including voice and signature.

Biometrics, refers to identifying individual physiological or behavioral characteristics, has the capability to reliably distinguish between an authorized person and an imposter [2]. Or A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual [4]. Today, biometric authentication methods are widely used in the areas that need to be highly secure; e.g. banks, computer networks, government, and law enforcement agencies. Current biometrics methods: eye scanning (iris, retina), face recognition, fingerprint scanning, hand geometry, finger geometry and signature recognition [5].

Among all the biometric indicators, iris has one of the highest levels of reliability [6].

Using iris for identification has many advantages: highly protected internal organ of the eye, the limited genetic pen trance of iris patterns, and encoding and decision-making are tractable:

Image analysis and encoding time: few milliseconds

Search speed: approximately one million Iris Codes per second

But the disadvantages of using the Iris for Identification: first, moving target and Located behind a curved, wet, reflecting surface, this problem can solve by using one position and one direction to take capture to the iris. Second, obscured by eyelashes, lenses, reflections that reflections regions are characterized by high intensity value close to 255 (A high threshold value can be used to separate the reflection noise) [7]. In this study, we develop a biometric system for Authentication. The system uses features extracted from the texture of iris image (after applying some preprocessing on the original iris image). Classification of the iris image is then achieved by applying a hash function to the extracted features.

Section 2 describes some of the related work; Section 3 describes an iris recognition system with experiments and results. Conclusions are explained in Section 4.

2. RELATED WORK

Many efforts have been emulated to redesign and reconstruct the biometric authentication to improve its performance: in [8] intended to engage a broad audience to consider the merits of the Biometric Encryption approach to verifying identity, protecting privacy, and ensuring security. Our central message is that BE technology can help to overcome the prevailing “zero-sum” mentality, namely, that adding privacy to identification and information systems will necessarily weaken security and functionality. This paper explains how and why BE technology promises a “positive-sum,” win win scenario for all stakeholders involved. In [9] perform a quantitative security evaluation of the CASHMA multi-biometric authentication system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the ADVISE modeling formalism. The obtained results provide useful insight on the security offered by the different system configurations, and demonstrate the feasibility of the approach to model security threats and countermeasures in real scenarios. In [10], poor accessibility and usability in authentication methods can form a barrier to the use of important websites, such as tax and benefit services. Given current commercial trends, biometric authentication methods will be used more widely to ensure secure access to such services. There is currently a dearth of research into both accessibility and usability of authentication modalities, including biometric methods. Thus, we investigated the usability of biometric authentication schemes for users with and without disabilities (vision or hearing). We comparatively evaluated three biometric authentication schemes (fingerprint, eye, and palm recognition) and one non-biometric authentication scheme (PIN) on effectiveness, efficiency, and perceived usability. Traditional and biometric schemes showed some usability differences. And in [11], We examine three biometric authentication modalities – voice, face and gesture – as well as password entry, on a mobile device, to explore the relative demands on user time, effort, error and task disruption. Face and voice biometrics conditions were faster than password entry. Speaking a PIN was the fastest for biometric sample entry, but a short-term memory recall was better in the face verification condition. None of the authentication conditions were considered very usable. In conditions that combined two biometric entry methods, the time to acquire the biometric samples was shorter than if acquired separately, but they were very unpopular and had high memory task error rates. These quantitative results demonstrate cognitive and motor differences between biometric authentication modalities, and inform policy decisions in selecting authentication methods.

3. DESCRIPTION OF AUTHENTICATION SYSTEM

For interact with hash function the image iris must be converted into the features vector. This can be achieved by applying a series of processes as shown in figure 1.

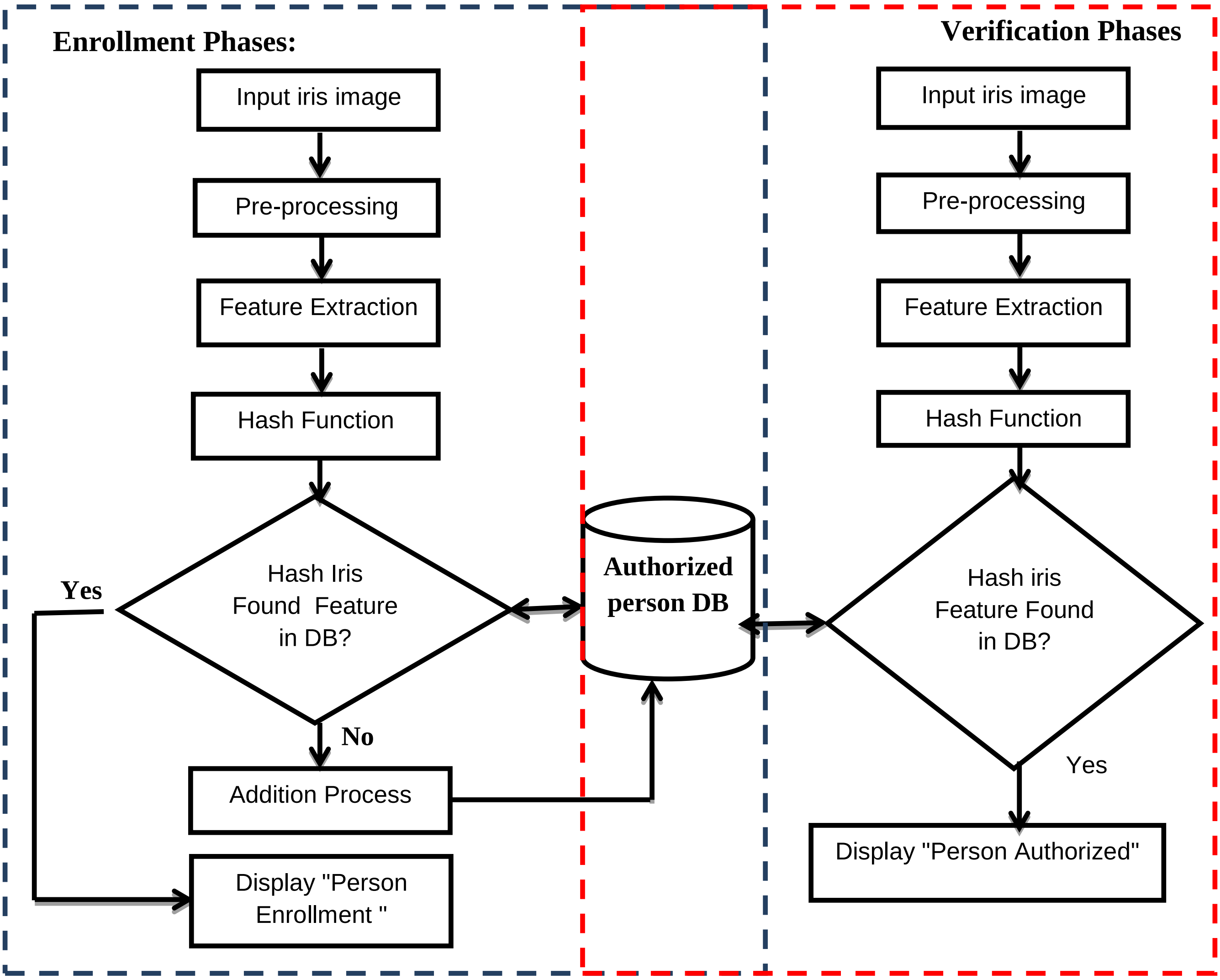


FIGURE 1: Authentication System.

The vector of the feature extracted from an iris image will be used with SHA-256 to generate unique values (hash value) to recognize authorized person or not authorized. Authentication system consists of two phases depending on the requested phase:

3.1 Iris Enrollment Phase

In this phase the SHA-256 hash function will be applied to the vector of feature extracted from iris image. The first stage in this system performs the preprocessing stage that explains in figure 2.

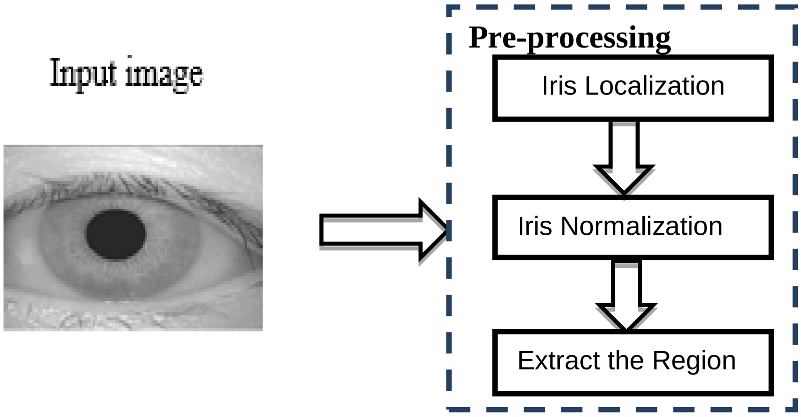


FIGURE 2: Pre-Processing Stage.

3.1.1 Image Binarization and Image Enhancement

To find the pupil, we first need to apply a linear threshold on the gray scale input image as shown in figure (3-A) is changed to binary image by using a suitable threshold as shown in figure (3-B).

0 if A(I,j)<=T

B (I,j)= if A(I, j)>T --------(1)

T is the threshold value used in the image segmentation (using an estimated global threshold). This value is found from separation of modes in the histogram.

Because the binary image B still has some black points outside the pupil region figure (3-C), an estimated point is performing chain code to find regions of 8-connected pixels that are assigned with value equal 1, figure (3-D).

In this edge detection step the boundary is found, this will simplify the feature extraction process. In this study, we have used the Laplace operator to find the edges; this is a linear operation, therefore very useful for digital implementation of the two-dimensional. Laplacian equation is obtained by summing two components, shown equation (2):

$$\vee 2f = [f(x+1,y)+f(x-1,y)+f(x,y+1)+f(x,y-1)]-4*f(x, y) \text{--------------}(2)$$

Where f is an image of size M x N (Laplace mask of size M x N).

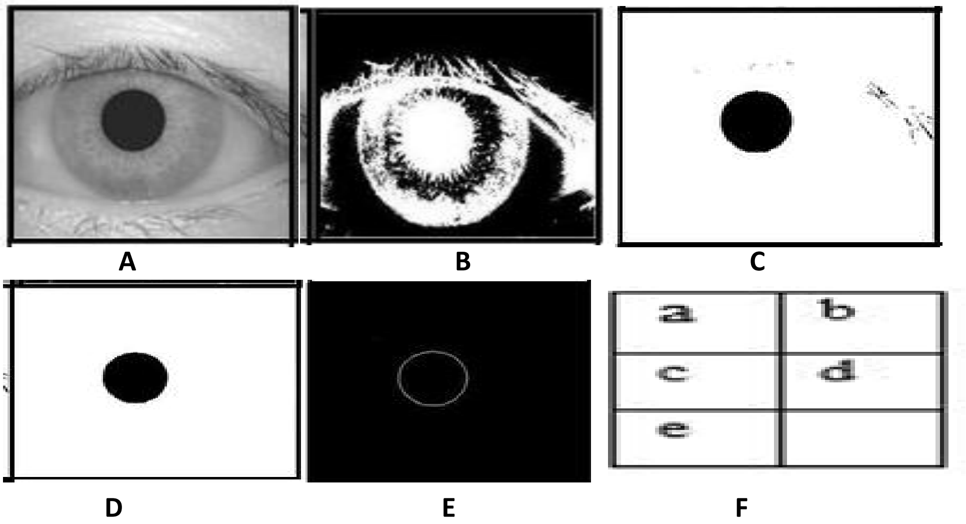
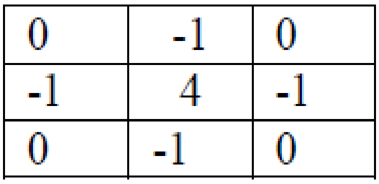


FIGURE 3: Image Binarization and Enhancement.

3.1.2 Edge Detection by Laplace Method

This equation can be implemented using the mask shown in figure 4, which gives an isotropic result for rotated in increments of 90 ◦ (isotropic filters, whose response is independent of the direction of the discontinuities in the image) [16]. They apply the mask and convolving it with the image. The sign of the result (positive or negative) from two adjacent pixel locations provides directional information, and tells us which side of the edge is brighter [12]. Figure 3-E shows the edges image obtained by applying a Laplace mask on the preprocessed image.



0	-1	0
-1	4	-1
0	-1	0

FIGURE 4: Laplace Mask.

Then the center and radius of the pupil can be computed easily because calculated from the edge image.

3.1.3 Extract the Region

The traditional methods extract a complete iris image, but the proposed method only extracts parts of the iris image for recognition. This will reduce the required computation and time and at the same time eliminate the confutation caused by eyelashes [6]. There are two types of eyelashes: separable eyelash can be distinguished from other eyelashes and multiple eyelashes are several overlapping in a small region [13]. Eyelashes appear randomly in the iris region. Figure 5 shows the removal of eyelashes, and extracted special regions from iris image.

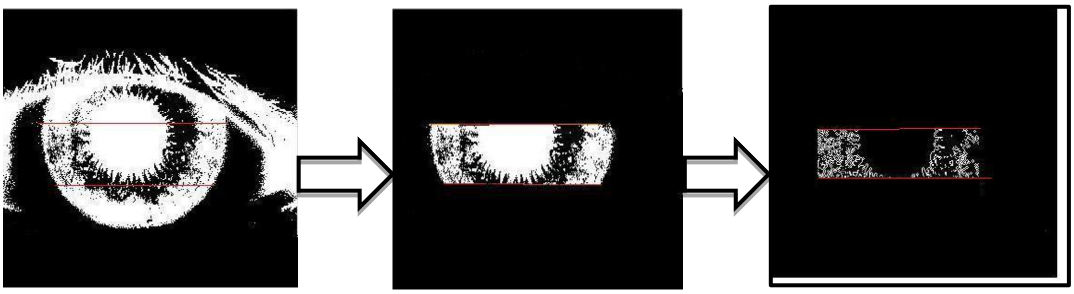


FIGURE 5: Extracting Part of Iris Image.

3.1.4 Feature Extraction

This process starts with forming a hundred sets of concentric arcs fifty from each side as shown in figure (6 a) are extracted from a size normalized image, the arcs are the rearranged in a two dimensional array as shown in figure (6 b), the two dimensional array is then organized in a set of 25 pixel blocks (each block is a 5X5 metric), the block is built from five successive layers taking five pixels from each layer, this will give a hundred blocks (fifty from each side).

The blocks data are used to construct a representative vector for the iris, which will be used for identification of the iris.

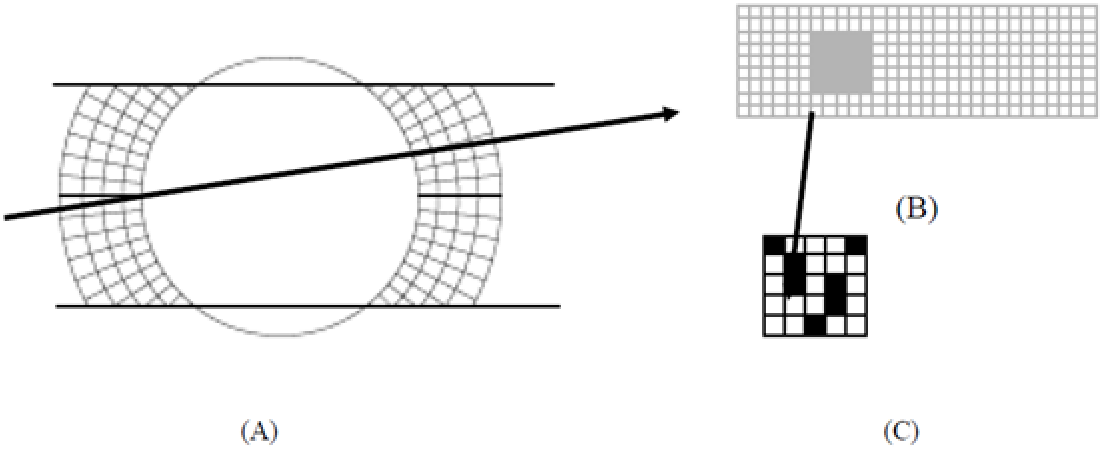


FIGURE 6: (A) Iris Arcs (B) Two Dimensional Array constructed from Iris arcs (C) A 5X5 Block.

3.1.4 Hash Iris Features

In this work used the different versions of SHA-2: SHA-224, SHA-256, SHA-384, and SHA-512. The perfect version of the authentication system is the SHA-256 after comparing and practice. Hash function provides a high security for protecting the features extracted from iris image and avoiding steal it. Hash value represented as "signature".

SHA-256 is one of the strongest hash functions available. SHA-256 is not much more complex to code than other hash functions. Figure 7 illustrated the hash iris feature by SHA-256.

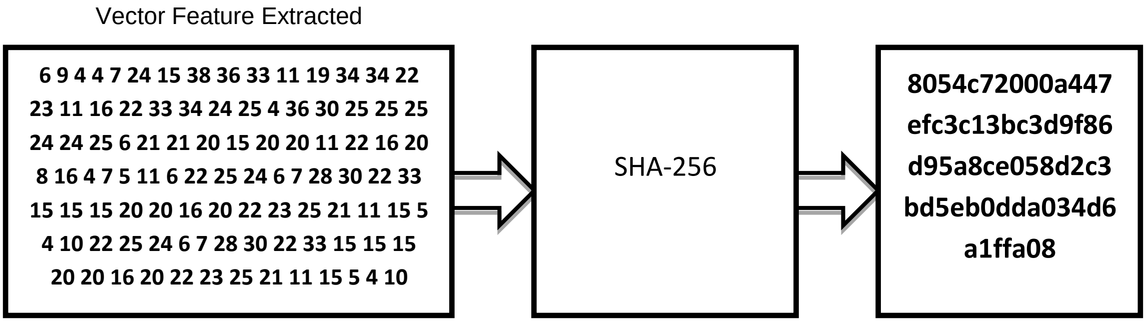


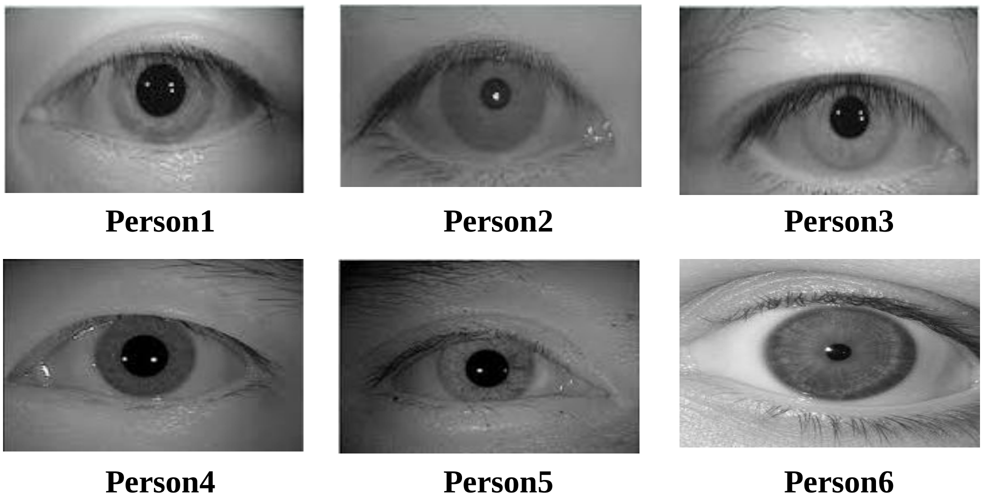
FIGURE 7: Hash Iris Feature.

3.2 Iris Verification Phase

In this phase perform the same steps of the enrollment phase; that explain in the previous sections, to determine if the person authorized or unauthorized.

4. DISCUSSION AND EXPERMINTAL RESULTS

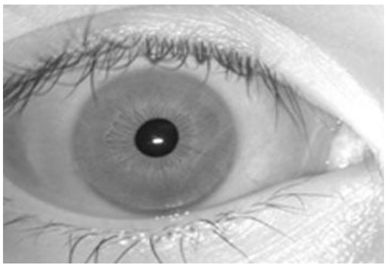
In testing the proposed system for a variant person that A total 100 different features will be extracted from the iris array, take as example 6 people and extracted iris feature, figure 8 illustrated the authorized persons and figure 9 illustrated unauthorized persons.



Person1 **Person2** **Person3**

Person4 **Person5** **Person6**

FIGURE 8: Iris Images of the Authorized Person.



Person7

FIGURE 9: Iris Image of Unauthorized Peron.

The first phase, enrollment phase generated feature extracted from the iris image for authenticating persons by preprocessing, table 1 explains feature extracted of authorized persons.

No_Image	Person Name	Feature Extracted
1	**Person1**	**6 9 4 4 7 24 15 38 36 33 11 19 34 34 22 23 11 16 22 33 34 24 25 4 36 30 25 25 25 24 24 25 6 21 21 20 15 20 20 11 22 16 20 8 16 4 7 5 11 6 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10**
2	**Person2**	**2 5 3 4 7 24 15 38 36 33 11 19 34 30 25 25 25 24 24 25 6 21 21 20 15 34 22 23 11 16 22 33 34 24 25 4 36 20 20 11 22 16 20 8 16 4 7 5 11 6 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10 15 20 20 16 20 22 23 25 21 11 15 5 4 10**
3	**Person3**	**3 6 4 2 3 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 22 16 20 8 16 4 7 5 11 6 38 36 33 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 15 5 4 10 15 20 20 16 20 22 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23**
4	**Person4**	**6 7 8 9 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 15 5 4 10 15 20 22 16 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23**
5	**Person5**	**1 5 2 7 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 15 5 4 10 15 20 22 16 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23**
6	**Person6**	**8 6 3 5 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 25 6 21 25 21 11 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 15 5 4 10 28 30 22 33 15 15 15 20 20 16 20 22 23 15 20 22 16 22 25 24 6 7**

TABLE 1: The Feature Extracted from Iris Image.

From the above result in table 1, extract 100 features from each iris image of authorized person after removing of eyelashes, and extracted special regions from the iris image by preprocessing process. Table 2 explains the hash iris image by performing different versions of SHA-2: SHA-224, SHA-256, SHA-384, and SHA-512.

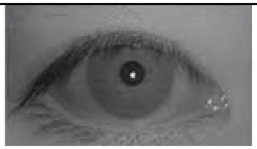
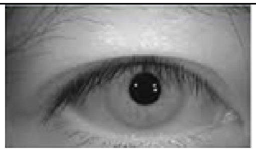
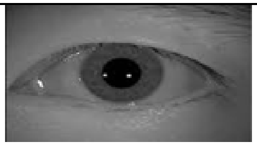
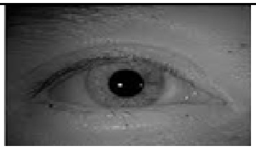
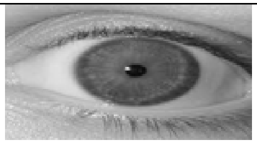
No	Person Name	Iris Image	Feature Extracted	SHA-2			
				SHA-224	SHA-256	SHA-384	SHA-512
1	Person1		6 9 4 4 7 24 15 38 36 33 11 19 34 34 22 23 11 16 22 33 34 24 25 4 36 30 25 25 25 24 24 25 6 21 21 20 15 20 20 11 22 16 20 8 16 4 7 5 11 6 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10	f0d24afefa204357dc051885d1ee01a709dd4cd1c8906e1e8b41a334	8054c72000a447efc3c13bc3d9f86d95a8ce058d2c3bd5eb0dda034d6a1ffa08	e23479c07743275239800bb2a571029d172c1672d56f3b2252382ba271594bf450f342aeddaceea63c2d579c4bac73b7	a78ebf025a57b6ae901c47da58e68a9537c87933c8822f9b81368652d3406c44c172f4c666888b11b7c01491ba626717b8445a463c0d8451d0e6745ddc924ec6
2	Person2		2 5 3 4 7 24 15 38 36 33 11 19 34 30 25 25 25 24 24 25 6 21 21 20 15 34 22 23 11 16 22 33 34 24 25 4 36 20 20 11 22 16 20 8 16 4 7 5 11 6 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10 15 20 20 16 20 22 23 25 21 11 15 5 4 10	116d63f2cd4c7a584fff24eb1713a17d94535849291198e70553b96f	5d3d8212912d3984bd68fed7869f8fc80841b16b0f5cd657b483c09fb809a38e	cf1297db42dcc95b4b259987ba986c4b085ac1225b5ec75065d1e1cbaaf57a53a3db262945ad0b7942acb5f87a023b9e	1cf49ba865362a2b98a5398dbeae5e1eb8b356c9d7dea525c283eb924627871e13cde28a22b8480b0edb0df40b48933231b218f0c08cb9e80bc6c42466b8362b
3	Person3		3 6 4 2 3 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 22 16 20 8 16 4 7 5 11 6 38 36 33 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 15 5 4 10 15 20 20 16 20 22 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23	fda6f28165c2fb977b430a2994f800c1078684f616aa8e122f3bb0f0	39e410835da5db1f77da5532aedde07852f55d9a2b56e5ee6aab8af0eb332f6e	ab61233e4d73a8f91ed629127db3690cb57af039fc00b6b9d9f06a47b450c036db1b781a58cc8114be4e4836c357621b	18890fa09f411660bfd008d8a923967eba45cfef89e7a7447c4edb894e96ae9686e7e851b3ebdbbeb53d1040bd14eab9e642c09421b15251263fd282d55352d9
4	Person4		6 7 8 9 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 15 5 4 10 15 20 22 16 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23	e80551eaca7adf0966b915014d7c98e225a3e22716f04f85e5832b50	f6b8d9a90e98f41ee1ee22e553f188e129e6490614bfe02f9035bd8edfe7217d	6eafc2a3b13b0587e2865259ba7488fa040151da81f1f716b1749419430410da333a7a27ec2f2830ce7d5bd584bb6eb5	266a5b646efc3152d0c6f1a46df1bbe2065e8fc7ecd5a9f4eff504b41ae0ba20dfde309745db4aaec3f18aef9a82f0ad80a7d1776c3d216e1ae709d2e8e42263
5	Person5		1 5 2 7 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 15 5 4 10 15 20 22 16 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23	87105bee8e729b9970c4d86f1880919044816a7b6b5c7a855ce7d9f7	9cd230de9fb7a33fa5e9f7da23e85621ac940482b8d6756e63f4220fe373dc35	fad3a992dd93e1a49966d6dd5c3c30253d0fc3c2104b1d9aa04872cb6479b45315e7e13725b2c847bbb99eb2af6cf477	4e8f34374baa9ed67f6326653978ca3cb0db096a24ce0383a36faea7fb6cade9b1db37fbea485d8e4e67a259dd305130f5f3e274ba04c474556a1bcb4ec45a3e
6	Person6		8 6 3 5 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 25 6 21 25 21 11 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 15 5 4 10 28 30 22 33 15 15 15 20 20 16 20 22 23 15 20 22 16 22 25 24 6 7	79fb454dec52fb0009b9746bc6c47b59e0f6307f8b0af37f218d721e	06c40cfc0480ec754952211f919633b3036e32255c72de06bf3b402dfc07d8c4	f8d04ef751b1076688f0cbc7de578d22dbf606b28a3f1e4dc84e015f8bd41c31e164c182478f788076875f5e244a3f79	de936271eed0304741f161f2aec6bc0ba2eebf6abf1dbe33a6fee438e2396705d70eaacaa69abaf27e481bfa9e018af504b71489cbdfc4a67d27ab6043783941

TABLE 2: Hash Functions of the Iris Image

From the above result in table 2, each SHA function generated hash value with different lengths, also comparing between them by calculating time consuming. Table 3 explains the time consuming for each version of SHA-2.

Size Input (In byte)	Time consuming of Hash Functions (nanosec)			
	SHA-224	SHA-256	SHA-385	SHA-512
100 B	1925801	2051039	2105269	2369319

TABLE 3: Time Consuming for Each Version of SHA-2.

The version SHA-224 in the shortest time and SHA-512 is the largest time when calculated time consuming (in nanosec). Figure 10 explains the time consuming of each version of SHA-2.

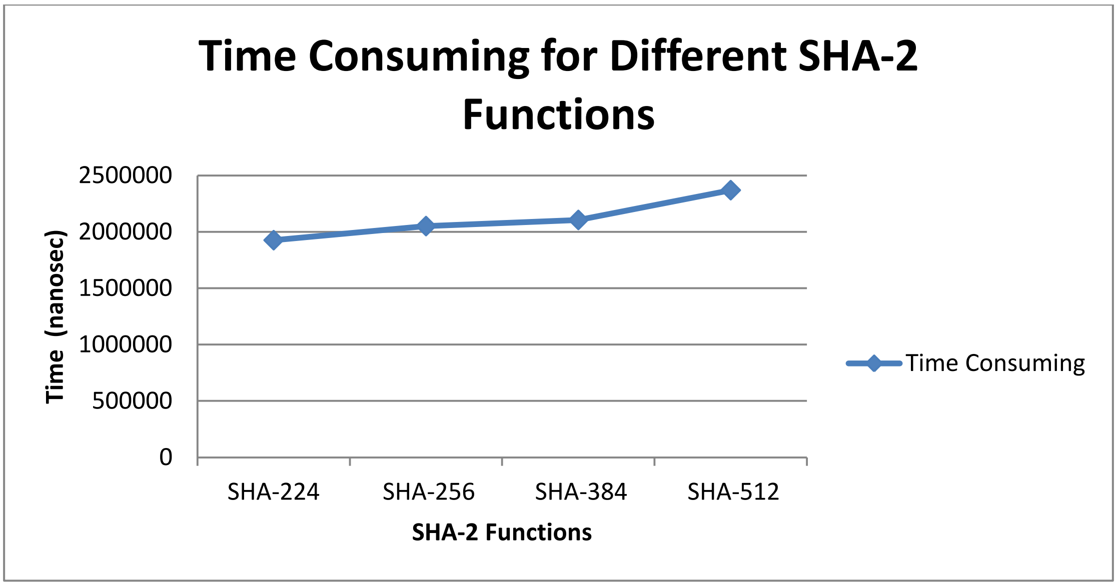


FIGURE 10: Time Consuming for different SHA-2 Functions.

The required time for calculating the hash value directly proportional to the length of the hash value. Also, the security level of the hash value directly proportional to the length of the hash value. Where, we chose the SHA-256 in the proposed work because its faster than the SHA-(384 and 512), its more safety than the SHA-224, and its appropriate in the proposed work for achieving two goals: the safe and the speed.

The second phase, verification phase tested by using authorized person and unauthorized person, the authentication system succeeds for verifying process, table 4 explains verification phase of the authentication system.

No	Person Name	Feature Extracted	Hash Value	Verify Phase
1	Person1	6 9 4 4 7 24 15 38 36 33 11 19 34 34 22 23 11 16 22 33 34 24 25 4 36 30 25 25 25 24 24 25 6 21 21 20 15 20 20 11 22 16 20 8 16 4 7 5 11 6 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10	8054c72000a447efc3c13bc3d9f86d95a8ce058d2c3bd5eb0dda034d6a1ffa08	Yes
2	Person2	2 5 3 4 7 24 15 38 36 33 11 19 34 30 25 25 25 24 24 25 6 21 21 20 15 34 22 23 11 16 22 33 34 24 25 4 36 20 20 11 22 16 20 8 16 4 7 5 11 6 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23 25 21 11 15 5 4 10 15 20 20 16 20 22 23 25 21 11 15 5 4 10	5d3d8212912d3984bd68fed7869f8fc80841b16b0f5cd657b483c09fb809a38e	Yes
3	Person3	3 6 4 2 3 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 22 16 20 8 16 4 7 5 11 6 38 36 33 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 15 5 4 10 15 20 20 16 20 22 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23	39e410835da5db1f77da5532aedde07852f55d9a2b56e5ee6aab8af0eb332f6e	Yes
4	Person4	6 7 8 9 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 25 25 24 24 25 6 21 25 21 11 15 5 4 10 15 20 22 16 20 8 16 4 7 5 11 6 38 36 33 20 16 20 22 23 25 21 11 15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 22 25 24 6 7 28 30 22 33 15 15 15 20 20 16 20 22 23	f6b8d9a90e98f41ee1ee22e553f188e129e6490614bfe02f9035bd8edfe7217d	Yes
5	Person7	15 5 4 10 21 20 15 34 22 22 25 24 6 7 28 30 22 33 15 15 15 5 4 10 15 20 22 16 20 8 16 4 7 5 111 5 2 7 11 24 15 23 11 16 22 33 34 24 25 4 36 20 20 11 11 19 34 30 25 15 15 15 20 20 16 20 22 25 25 24 24 25 6 21 25 21 11 23 25 21 11 6 38 36 33 20 16 20 22 22 25 24 6 7 28 30 22 33 23	2b8d6756ecd23a23e85621ac9404863f4220fe0de9fb7a33fa5e9f7d373dc35	No

TABLE 4: Verification Phase Of SHA-256.

From the above results, the proposed method can be recognized at a rate of 100% of the iris database. Also, it's accurate because it's used a secure method of authentication that iris-biometric and a hash function for avoiding stealing data from database or attacking by hackers for the traditional authentication method (such as passwords).

When comparing the current work with other works, the current work performs in a short time, while in [11] depend on three biometrics that have a long time for performing. The current work is performed in safety form, while in [8] used encryption for the extracted features, hash function more secure than encryption because it’s a one way function. Also, the current work and [10] explain the best method by using biometric authentication instead of the traditional authentication (such as a PIN) to avoid the stealing.

5. CONCLUSIONS

The study shows that the feature vector constructed by the proposed method provides an adequate data to distinguish the iris, although it is extracted from part (not all) of the iris image, and generated a secure signature for each authorized person in the enrollment phase by using hash function and recognized authorized and unauthorized person by verifying phase, the iris texture can give a very useful information to identify the iris. SHA-256 the best method for achieving high security to the authorized database and its faster than other types of hash function. In future can be applied a mobile biometric authentication depend on the iris and the hash function.

6. REFERENCES

[1] P. Robichaux. “Motivation Behind Iris Detection”. Connexions Project, 2004. cnx.org/content/m12488/latest/-12k.

[2] L. Masek.”Recognition of Human Iris Patterns for Biometric Identification”. Bachelor's Dissertation, School of Computer Science and Software Engineering, the University of Western Australia, 2003.

[3] C. Tisse, L. Martain, etal. ” Person Identification Technique Using Human Iris Recognition”. France University de Montpellier, Proceedings of the 15th International Conference on Vision Interface, PP. 294-299, 2000.

[4] C.M. Patil and S. Patilkulkarani. "Iris Feature Extraction for Personal Identification using Lifting Wavelet Transform". International Journal of computer Applications(0975-8887),Vol. 1,No. 14, 2010.

[5] H. Zuher.” Hand Geometry-based on Identity Authentication Method”. M.Sc. thesis, College of science, Al-Nahrain University, 2003

[6] C.T. CHU and C. CHEN. “High Performance Iris Recognition Based on 1-D Circular Feature Extraction”. I-Shou University (Taiwan), 2005.

[7] F. MSHTML. “Advantages and disadvantages of the Iris for Identification”. Technologies Journal, Vol. 7, No. 34, 2019.

[8] A. Stoianov. “Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy". Information and Privacy Commissioner of Ontario-Toronto, Ontario CANADA 2007.

[9] L. Montecchi1, P. Lollini, A. Bondavalli, E. L. Mattina." Quantitative Security Evaluation of a Multi-Biometric Authentication System ". Springer-Verlag Berlin Heidelberg 2011.

[10] R. N. Brink and R. I. Scollan. “Usability of Biometric Authentication Methods for Citizens with Disabilities”. The MITRE Corporation-MIT RE T E C HN I C A L R E P OR T, 2019.

[11] S. Trewin1, C. Swart1, L. Koved1, J. Martino1, K. Singh1, S. Ben-David. "Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption ". ACSAC ’12 Dec. 3-7, Orlando, Florida USA, 2012.

[12] S. E. Umbaugh. "Computer Vision and Image Processing". Printic-Hell,1998.

[13] R.Y.Fatt Ng, Y.H. Tay and K.M.Mok. "An Effective Segmentation Method for Iris Recognition System". Malaysia, 2007.

[14] R. C. Gonzalez and R. E.Woods. "Digital Image Processing". printice-Hell, 2002.

[15] "CASIA iris image Database". http://www.sinobiometrics.com/Databases.htm, (2007).