International Journal of Innovative
Computing, Information and Control
Volume **15**, Number **4**, August **2019**

ICIC International ©2019 ISSN 1349-4198
pp. 1441–1453

IRIS FEATURES VIA FRACTAL FUNCTIONS FOR AUTHENTICATION PROTOCOLS

Nadia M. G. Al-Saidi[1,*], Arkan J. Mohammed[2], Razi J. Al-Azawi[3] and Aqeel H. Ali[1]

[1]Department of Applied Sciences
[3]Department of Laser Engineering
University of Technology
Baghdad 10066, Iraq
[*]Corresponding author: nadiamg08@gmail.com

[2]College of Science
Mustansiriyah University
Baghdad 10052, Iraq

Received October 2018; revised February 2019

Abstract. *Information technology is rapidly developing, thereby highlighting the need for new protection mechanisms to ensure the authenticity and integrity of communication information over an open network. Identification and authentication protocols have emerged as significant tools in this field. Biometric systems have played an important role in protocol authentication and identification because of their individualized properties used as appropriate measures. The iris has many advantages over other biometrics because of its features, including unique complex pattern, stability, and others. These properties make the iris an excellent choice for confidence authentication. The ability of fractal functions to model and describe complex natural patterns makes them highly interesting for use as a mathematical technique inefficient recognition and fast matching. In this study, the fractal encoding approach is used to transform a scanned iris into a compressed representative form. The authentication is satisfied by encrypting the representative parameters using one of the proven secure encryption methods to ensure secure transmission and storage. The resulting authentication system is analyzed to show the efficiency and accuracy of the proposed recognition method.*

Keywords: Fractal, Iterated function system, Iris identification, Authentication

1. **Introduction.** Authentication is considered as a significant tool for security performance in computer-based communication. Traditional authentication and identification techniques are based on physical token or knowledge, which have been proven to have numerous drawbacks. A good alternative to these traditional methods is the biometric technique using physiological or behavioral traits. Various methods and techniques to strengthen the capacity of the human identification system have emerged over the years.

The individual identification based on fingerprints is the most popular method because of the simple mechanism of the fingerprint. Galton and Henry [1, 2] were the first to work on fingerprint identification. Face recognition is one of the most commonly adopted biometric identification methods. Thorat et al. [3] introduced an initial idea of using facial characteristics in 1964. In 1992, Antonini et al. [4] proposed a new image-coding scheme using the fractal coding method for face recognition, considering features both in space and frequency domains. In 1998, Okada et al. [5] developed a system (ZB-Face)

DOI: 10.24507/ijicic.15.04.1441

considered as the most secure because of its ability to match perfect image. This technique is used by major international airports, banks, and government offices.

Different techniques have been used for feature extraction from the biometric. Fractals have the ability to represent complex and unstructured objects. Therefore, they have many properties that can be used in authentication and identification and in studying biometric features. The system security is perceived as biometric identification because the biometric characteristics of an individual are peerless and cannot be transformed. In 2005, Athale et al. [6] described a system to recognize face details depending on the fractal domain that leads to a large database of compact face images in fractal terms. The face images are identified using the compatibility of the pixels arising from fractal codes. The result of this system has been encouraging. In 2010, Potgantwar and Bhirud [7], used an iterated function system (IFS) to present a new approach for face recognition based on a partial IFS representation, which is more efficient than the image domain correlation. In 2014, Al-Saidi and Said [8], utilized fingerprint features to propose a new biometric identification method based on the self-similarity property used in fractals to represent a fingerprint image in a finite number of transformations.

The iris has many advantages over other biometrics because of its features, including unique complex pattern, stability, and others. It also has a good mathematical preference, such as, for different persons, there is enormous pattern variability. These advantages make iris a great choice for confidence authentication. The ability of fractal functions to model and describe complex natural patterns makes them highly interesting for use as a mathematical technique inefficient recognition and fast matching. For images have some degree of self-similarity, fractal encoding is useful. Similarity means that a given area in the image could be fitted to another area through some affine mapping. Iris patterns vary significantly among different persons. This advantage made the iris pattern highly interesting among biometric methods that include fingerprint or face recognition [9]. The first identification system based on the iris was introduced in 1936 by Burch [10]. In 1987, Flom and Safir presented the unique iris idea. Then, an automotive identification system based on the iris was developed by Daugman [11]. The same issue has been considered by many other researchers [12, 13, 14]. Iris identification is based on features that can be analyzed to recognize authorized people [6]. In 2012, Jampour et al. [15], developed a method to extract and classify iris images using fractal dimension and coding. Their technique was characterized by stability, redundant part exclusion, rotation sensitivity, and others. The method was also considered fast and can help reduce long recognition time. Many other researchers have used different types of fractal dimension for iris classification and recognition [16, 17, 18, 19, 20].

In this paper, a new approach is proposed based on the fractal encoding technique to be used for secure authentication protocol via iris biometric. Since fractal image coding technique suffers from time-consuming, which is the main drawback of this technique, Al-Saidi and Ali [21] proposed a fast fractal coding algorithm based on a fractal dimension. They have utilized the enhanced differential box-counting algorithm given in [22] to reduce the encoding time possessed in the searching for the best match between the domain and range pools. This improved approach is used to transform a scanned iris into a compressed mathematical representative form. Fractal dimension is used to speed the searching process for an approximate domain block for each range block; it was used as an index for the compared blocks. In comparing to the original technique, the experiment shows that by applying the proposed procedure, the encoding time is improved. The strength of the method lies in a high resolution of the recovered data and resulting in an efficient authentication protocol.

In addition to this section, five subsequent sections constitute the material of this paper. Section 2 presents the required theories for IFS and the fractal-encoding method. The iris biometric and its features are explained in Section 3. The proposed method and its structure with the proposed algorithm are introduced in Section 4. Several experiments with their implementation are discussed in Section 5. The study is concluded in Section 6.

2. **Theoretical Background.** The fundamental principles for fractal coding are presented in this section. Additional details are provided in [23, 24, 25, 26, 27].

2.1. **Fractal.** We can analyze geometric shapes around us in different visions using a fractal based on shape asymmetry. The fractal is viewed as a language that has proven its value because of its uses. It is used in the physical field in conjunction with the mathematical basis of physics, and various material and engineering areas. It is also employed in pure and applied mathematics [24]. Objects are called fractals if they have the following properties:

- Self-similarity
- Iterative process
- Non-integer dimension

2.2. **Iterated function system (IFS).** The foundation of the fractal coding scheme is called IFS. The basic idea of the IFS is to create a finite set of contraction mappings in affine transformation by choosing any seed image. The iterates of these mappings produce a unique attractor called fixed point of mapping. The IFS was first demonstrated in 1981 by Hutchinson [24], who defined it as a finite set of contraction mappings on a complete metric space, $\{f_i : X \longrightarrow X, i = 1, 2, 3, \ldots, N\}$. The IFS can be expressed mathematically as follows.

Let (X, d) be a metric space, and $w_n : X \longrightarrow X$, be a contractive transformation with contractivity factor s_n, for $1 \leqslant n \leqslant N$. For any $B \in H(x)$, the transformation $W : H(x) \longrightarrow H(x)$ is defined by $W(B) = \bigcup_{n=1}^{N} w_n(B)$ is a contraction mapping on the complete metric space $(H(x), h(d))$ where $s = \max_{1\leqslant n\leqslant N}(s_n)$ is the contractivity factor of W. By the contraction mapping theorem, W has a unique fixed point $A \in H(x)$, such that $A = W(A) = \bigcup_{n=1}^{N} w_n(B)$ for any $B \in H(x)$. A is the attractor of the IFS. Figure 1 shows an example of IFS transformation known as a Sierpinski triangle given in Equation (1) [24].

$$\begin{aligned} w_1(X) &= w_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ w_2(X) &= w_2 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 1 \\ 50 \end{pmatrix} \\ w_3(X) &= w_3 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 25 \\ 50 \end{pmatrix} \end{aligned} \tag{1}$$

2.3. **Fixed point theorem (Banach).** Let (X, d) be a complete metric space, and $w : X \longrightarrow X$ be a contraction mapping. A unique point $x' \in X$ exists such that, $w(x') = x'$. Furthermore, the sequence $\{w^{0n}(x) : n = 0, 1, 2, \ldots\}$ for any $x \in X$ converges to x', such that, $\lim_{n\to\infty} w^{0n}(x) = X'$.

The fixed-point theorem plays an important role in the fractal generation mechanism. The theorem provides the idea of forward convergence to the fixed point (the attractor),

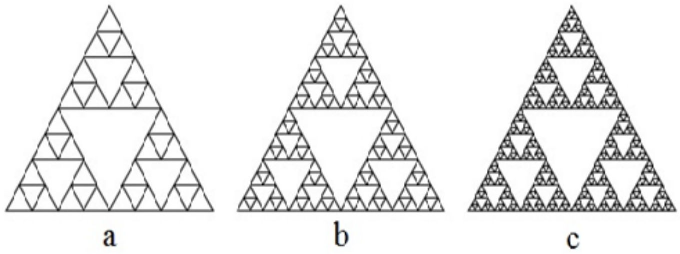


Figure 1. Iterated processes of Sierpinski triangle

especially when the function is contraction [24, 26]. Figure 1(c) represents the fixed point of the IFS given in Equation (1).

2.4. **Collage theorem.** Let $F : X \longrightarrow X$ be a contraction mapping defined on a complete metric space (X, d) with contractivity factor $0 \leqslant s < 1$. Let $x \in X$ be a fixed point of f, and then $d(x, x_f) \leqslant \frac{d(x,f(x))}{1-s}$ for all $x \in X$, $n \geq m \geq 1$, can be proven by the following steps [23,27].

$$
\begin{aligned}
d(x, x_f) = d\left(x, \lim_{n\longrightarrow\infty} f^{0n}(x)\right) &= \lim_{n\longrightarrow\infty} d\left(x, f^{0n}(x)\right) \\
&\leq \lim_{n\longrightarrow\infty} \sum_{m}^{n} d\left(f^{0(m-1)}(x), f^{0n}(x)\right) \\
&\leq \lim_{n\longrightarrow\infty} d(x, f(x)) \left(1 + c + \cdots + c^{(n-1)}\right) \\
&\leq \frac{d(x, f(x))}{1-c}.
\end{aligned}
$$

Using the collage theorem, we can understand that we must find a set of contractive transformations on the space containing M to find an IFS, of which the attractor is an approximation of a given set M, where the distance between the union of these transformations and this set M is as small as possible $(d(M, \bigcup_{n=1}^{\infty} w_n(M)) < \epsilon)$.

3. **Iris.** In the eye, the colorful complex textured part located between the pupil and the white sclera is called the iris. The iris is behind the transparent cornea and may be in different colors (e.g., black, blue, green, brown, and honeyed). Figure 2 shows the iris and other eye parts [27].

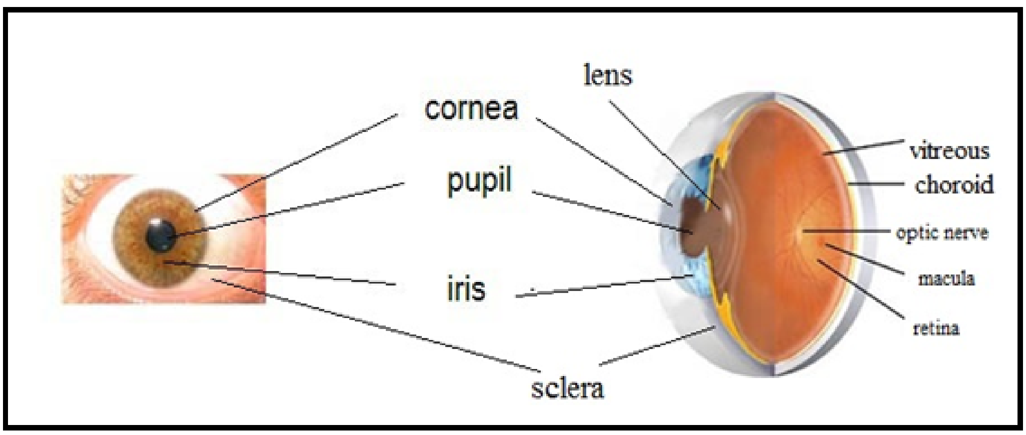


Figure 2. Eye structure

- **Cornea:** Its function is to focus and transmit light into the eye.
- **Lens:** It is responsible for focusing light rays into the retina.
- **Pupil:** It is located in the middle of the iris as a dark center responsible for determining the amount of light that should enter the eye. Its size changes according to the amount of light.
- **Optic nerve:** It is responsible for the connection between the eye and the brain. It carries retina impulses to the brain, and then the brain interprets them as images.
- **Retina:** It senses light and sends impulses to the brain through the optic nerves. It is constructed by the nerve layer that lines the back of the eye.
- **Macula:** It is the small part in the retina responsible for the special light-sensitive cells and helps people to clearly see fine details.
- **Vitreous:** It is a gel-like substance filling the middle of the eye; it helps the eye move in a round shape and allows light to pass through to focus on the retina.

4. **The Proposed Method.** Many methods and geometric representations for an object exist. However, fractal coding through an IFS provides us with the most accurate result in this field. The basic principle is that having any type of self-similarity in an image will help reconstruct it. In this paper, the availability of representing a digital image of the iris in a finite number of transformations is discussed by choosing samples from the iris image database and by studying the result of image encoding on this database based on the IFS.

4.1. **Extracting iris from eye image.** The eye image in Figure 2 shows that the iris has a fractal structure that can be described as follows:

- white area (sclera) with veins surrounds the cornea,
- the iris part with a complex fractal structure is the required part for extraction, and
- the central black part is called the pupil.

We must first isolate the iris from the other eye parts to eliminate the unwanted area from the image. The isolation can be achieved based on two relations: statistic processing and image histogram. These relations are used to remove the central part (black pupil) as shown in Figure 3 [28].

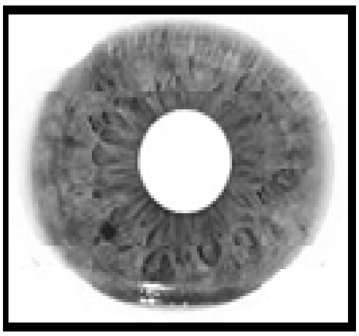


Figure 3. Eye structure

The idea of mean deviation is used to detect the pixel-level details (sclera area) such that

$$MD(i,j) = \frac{\mid \sum_{i,j}(PV(i,j) - AVG(PV)) \mid}{\sum_{i,j}(PV(i,j))} \tag{2}$$

where PV refers to the pixel value in the (i, j) position, and AVG is the average of pixels in the chosen block. Figure 4 shows the iris extraction process.

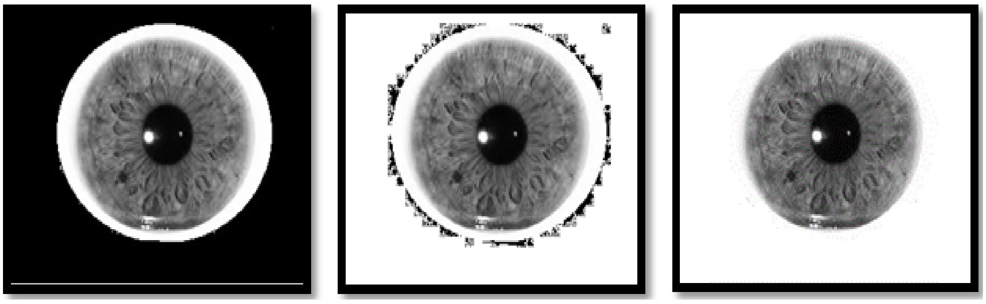


Figure 4. Image preprocessing and iris extraction

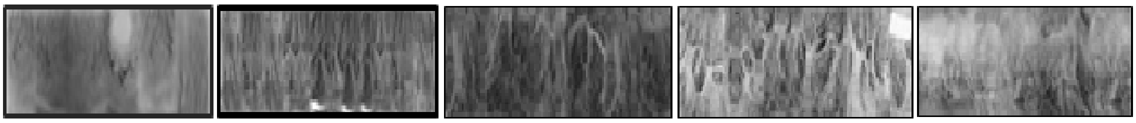


Figure 5. Iris's extraction results

Equation (2) considers the removal of uninteresting area parameters, including $MD(k, l)$ that takes a value of $[0, 1]$, which is zero in the white area and growing in the bloody area. The iris and pupil borders are recognized by the desired separation of the iris obtained from the common edge detection. The rotating geometrical change is used to recognize the iris. The ring shape of the pupil is then changed to a rectangle (Figure 5). This process is performed by applying Equation (3).

$$\begin{aligned} x_{new} &= x_1 \times \cos(\theta) + y_1 \times \sin(\phi) \\ y_{new} &= y_1 \times \cos(\theta) + x_1 \times \sin(\phi) \end{aligned} \tag{3}$$

4.2. **Iris features extracting by fractal.** Over the past few years, a trend toward classical coding method to improve coding efficiency has been observed. Fractal coding is a modern technique used to express images in a simple geometric manner by transforming them into compressed representative parameters. Coding helps to efficiently extract features and leads to an effective recognition process. This technique is used in the present study to secure authentication by the iris biometric and is applied through the following procedure.

1) An iris image M of size $n \times n$ is input.
2) The image M is partitioned into non-overlapping blocks of size $r \times r$. This size is responsible for the accuracy of the resulting parameters and is a predefined number. Hence, there are $(\frac{n}{r})^2$ blocks called the range pool.
3) The other pool is constructed by partitioning image M into overlapping blocks of size $2r$ called the domain pool according to $2r$. $(n - 2r + 1)^2$ domain block exists.
4) Each domain block flips in the horizontal and vertical directions and rotates clockwise at 45°, 60°, 80°, and 97°, with the original block mirrored. Thus, we have with the original block an additional seven new domain blocks. Therefore, the total number of domain blocks that need to be checked for each range block is equal to $8(n - 2r + 1)^2$.
5) Choosing the corresponding domain block for each range block requires searching through all blocks in the domain pool to determine which one of them looks most similar to the chosen range block. This matching task is achieved using the mean square error E.

6) This matching task produced five compressed parameters $[x, y, ios, o, s]$ considered to represent the representative parameters of the specific range block.

Figure 6 illustrates the partitions of M into blocks and the transformations between them. E is the error function that is used to determine the variation value of the image colors, which make the value of a_i less than that of b_i. The minimum value of E is obtained from its partial derivatives with respect to s and o. Parameters s and o introduce the light pixels and the offset of the image pixels, respectively. They are provided in Equation (5).

$$E = \sum_{i=1}^{n} (sa_i + o - b_i)^2 \tag{4}$$

where $(a_1, a_2, \ldots, a_n) \in D$, and $(b_1, b_2, \ldots, b_n) \in R$.

$$\begin{aligned} s &= \frac{n^2\big(\sum_{i=1}^n a_i b_i\big) - \big(\sum_{i=1}^n a_i\big)\big(\sum_{i=1}^n b_i\big)}{n^2 \sum_{i=1}^n a_i^2 - \big(\sum_{i=1}^n a_i\big)^2} \\ o &= \frac{\sum_{i=1}^n b_i - s\sum_{i=1}^n a_i}{n^2} \end{aligned} \tag{5}$$

By substituting in Equation (4), we get

$$E = \frac{\sum_{i=1}^n b_i^2 + s\big(s\sum_{i=1}^n a_i^2 - 2\sum_{i=1}^n a_i b_i + 2 * o\sum_{i=1}^n a_i\big) + o\big(on^2 - 2\sum_{i=1}^n b_i\big)}{n^2} \tag{6}$$

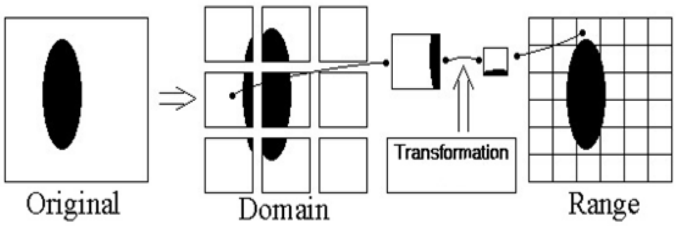


Figure 6. Domain and range blocks

4.3. **The authentication protocol.** Three main parts compose the architecture of the proposed authentication protocol. Some of these parts perform on the client side, while the others are on the server side. These are described as follows.

Initialization part

The transformation parameters that represent each captured iris are constructed by this part through the following steps.

1) M of size $n \times n$ is partitioned into non-overlapping range blocks RN with a size of $r \times r$, where r is a predefined parameter that determines the number of IFS transformations. $RN = (n/r)^2$ range blocks exist according to r.
2) M is partitioned into a set of overlapping domain blocks DN with a size of $2r \times 2r$. $DN = (n - 2r + 1)^2$ range blocks exist according to $2r$.
3) Each domain block goes through eight isometries in addition to the original, which are flip horizontal, flip vertical, rotating with clockwise 45°, 60°, 80° and 97°, and original block mirrored. Therefore, the number of domain blocks becomes $DN = 8 * DN$.
4) For each $RN(I)$, a corresponding similar domain block-based mean square error E is chosen and provided in Equation (6). Five parameters are constructed for each range block that represents the coefficient of one of the IFS transformations w_i, where $w_i = \{x_i, y_i, iso_i, o_i, s_i\}$, and $W = \{w_1, w_2, \ldots, w_n\}$, such that $E(RN(I); W(RN(I))) \approx 0$.

5) Matrix W is generated, which represents the compressed image in the form of a local IFS code, where $M' = W(M) = w_1(M) \bigcup w_2(M) \bigcup \cdots \bigcup w_n(M)$.

Registration part

Several captures are scanned in this part and transformed by the previous part to their representative parameters. The following steps are performed.

1) An iris reader is used to capture the iris of a specific person from different angles. This step helps overcome any limitation resulting from unstable movements and minor shifting.
2) FIC (the initialization part) is applied to obtaining the representative parameters. The matrix $W(n \times 5)$ is constructed for each capture, which represents the iris codes.
3) The matrix W, is then converted to vector $S_{(1\times 5)}$ by averaging each column in it.
4) The obtained parameters are encrypted using a secure encryption method called Diffie Hellman (DH) to establish a secure shared key for use on the server side.
5) The parameters are added to the server database after decryption.

   The parameters of this iris are encoded to authenticate any query on the iris image and sent to the server side for matching with the server database.

Login part

This part is implemented on the client side. Several tasks are performed as follows.

1) An iris reader captures the iris of the specific person.
2) The FIC (the initialization part) is applied to obtaining the iris parameters and constructing the matrix $W(n \times 5)$ that represents the iris codes for each capture, such that $W_i = (x_i, y_i, iso_i, o_i, s_i)$.
3) Matrix W is compressed to a vector $S = \left(\sum_{i=1}^{r} x_i, \sum_{i=1}^{r} y_i, \sum_{i=1}^{r} iso_i, \sum_{i=1}^{r} o_i, \sum_{i=1}^{r} s_i\right)$ by averaging each column in W.
4) The obtained parameters are encrypted using the DH encryption method to establish a secure shared key. Then, the encrypted code is sent to the server side.
5) The received data are decrypted on the server side to obtain the iris parameters.

The verification part

The following steps are accomplished on the server side to verify any iris query after receiving the registration or login request. All responses should pass through an encrypted channel during the registration or login between the server and the client to ensure information security. Again, the DH shared key is used for this purpose.

1) To verify any request from the registration part:
   (a) The received data from the registration phase are compared with the data on the server database;
   (b) Otherwise, the iris parameters are saved on the database and the step returns to "the user is registered".
2) To verify any request from the login part:
   (a) The data received from the registration phase are compared with the database data;
   (b) The step returns to "the iris" if the user exists. The requested account can then be accessed;
   (c) Otherwise, the step returns to "user does not exist".

Based on one threshold value, the decision for the verification phase is taken based on the error function. E given in Equation (4) between the input iris after converting to fractal codes in the client side, with the database fractal codes of the authorized persons, which is already saved in the server side. The block diagram that illustrates the proposed authentication system is presented in Figure 7.

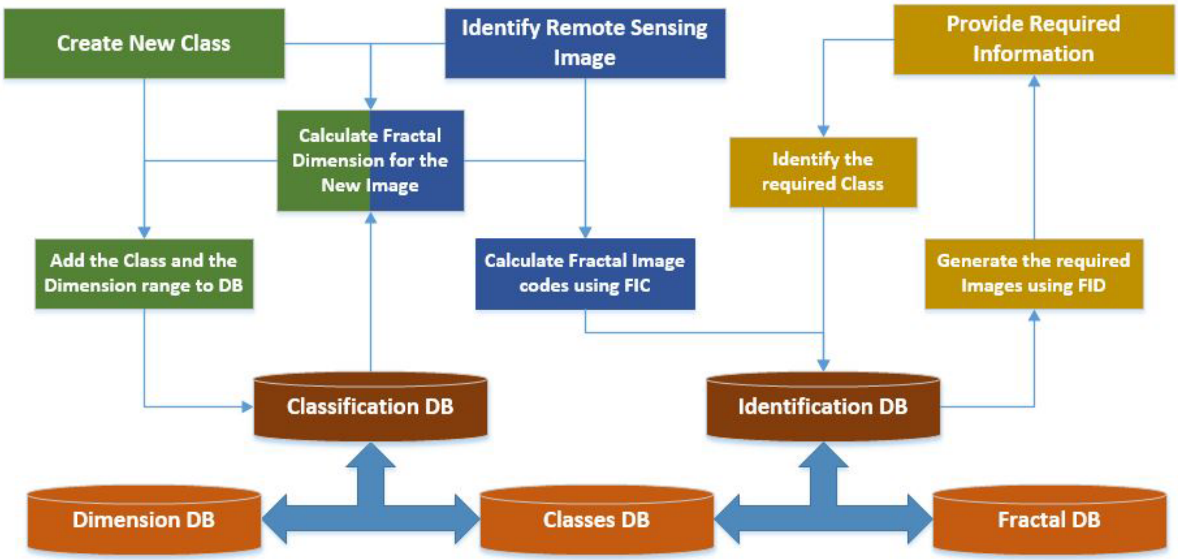


FIGURE 7. Block diagram for the proposed authentication system

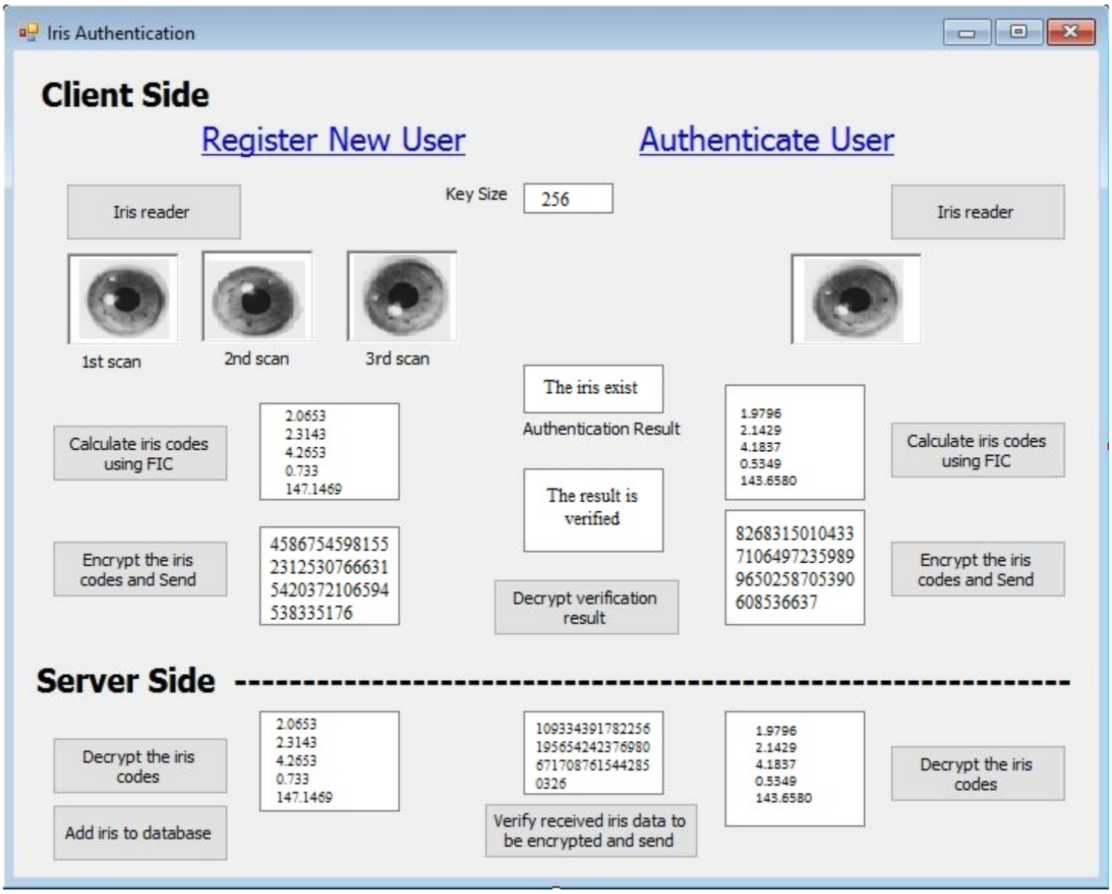
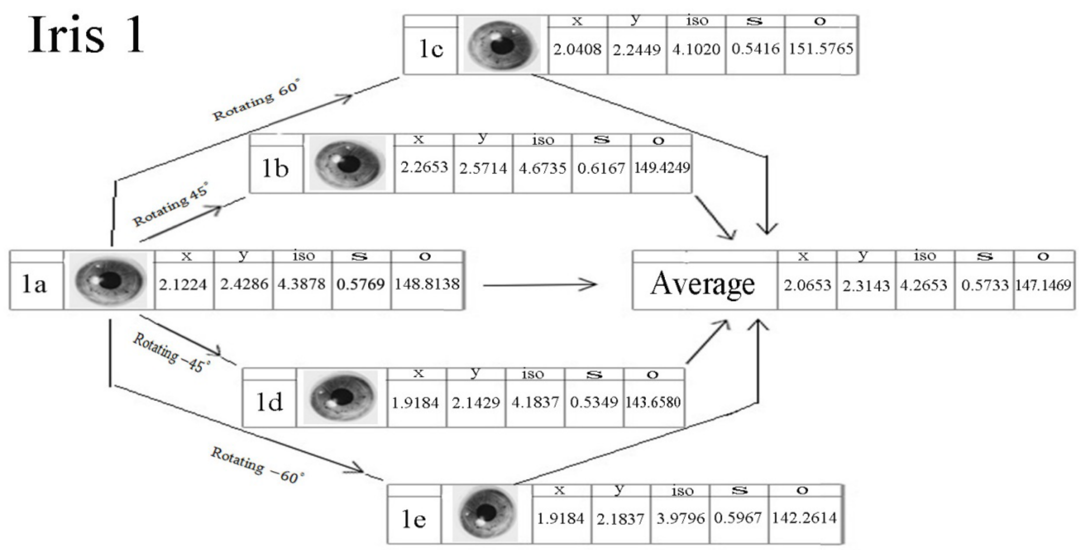
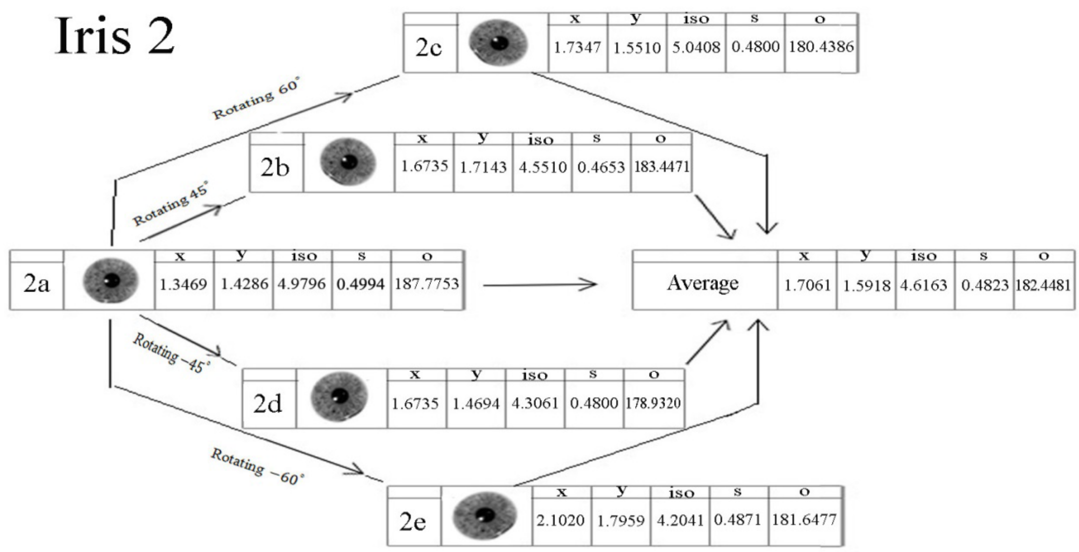


FIGURE 8. Authentication system user interface

5. **Implementation and Analysis.** Identifying an exact person that accesses an account requires highly sophisticated tools. Authentication plays an important role in controlling communication through computers. Many biometrics were used as tools to

achieve secure authentication for accurate identification. The iris is proven to be an effective tool for this purpose. The fractal is mostly used for image compression. However, several attempts have been reported on its use for authentication- and identification-based biometrics. In the present study, the fractal coding approach was used to transform an image into its compressed representative parameter, which can be used as a texture signature for image indexing by content and for recognizing the image. On the server side, these parameters built a database in low volume. They were then saved instead of the iris image itself and can be used in the identification process. Figure 9 (1-5) show five iris samples. Five captures in different angles were obtained for each one of them. The proposed technique was performed using Matlab on a computer running Windows 8 and with hardware consisting of CPU Intel Core i7 and 4 MB RAM. An experiment on 25 iris samples was conducted. Five rotation samples were also acquired for each one of the iris samples (Figure 8), a 96% success rate was recorded, which reflects the reliability of the proposed technique.





(continued)

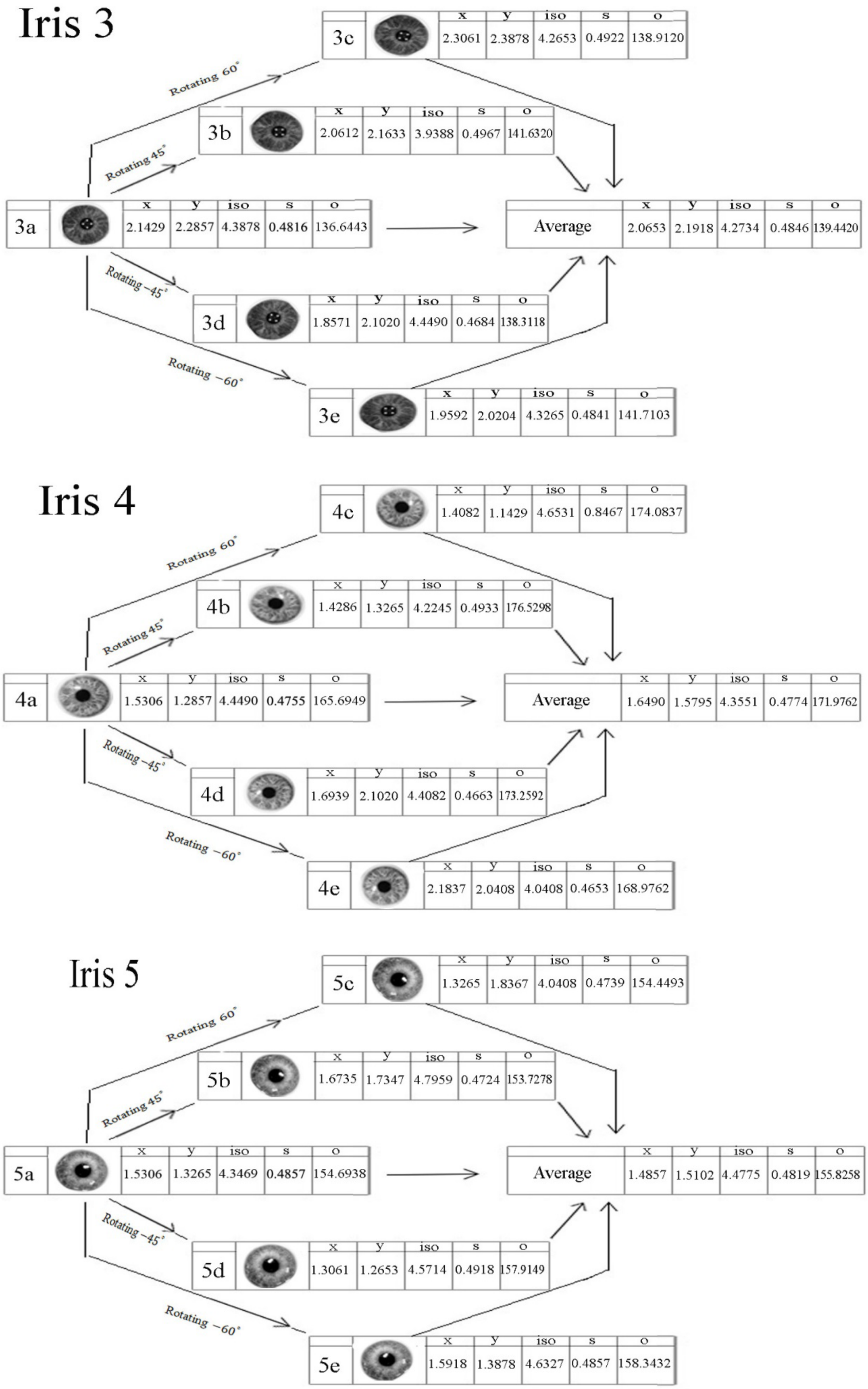


FIGURE 9. Irises with their fractal parameters

6. **Conclusions.** Using iris authentication for user identification is a technique that has attracted much attention from many researchers. This study has been accomplished based on the fact that an iris is a fractal object. A new authentication system is designed based on the modified fractal coding method. This system has many advantages, including reduction of processing time and storage area, an accurate analyzable feature, and fast verification. The iris structure is analyzed to increase the security of the authentication and identification protocols. Fractal encoding is used to create a secure database because the original irises are stored as fractal parameters. Only five parameters are required to be saved on the database for each iris capture, which results in the reduction of storage space compared with other methods. These codes are encrypted by one of the secure cryptography systems. The verification passes if the mean square error between the fractal codes of the iris query and one of the database codes is less than a certain threshold value. By applying this technique with the original one on a sample of 25 irises, we found that, the compression time of the proposed method is improved. This is due to converting the searching for an appropriate block for each range block to searching for the approximate dimension with less error.

REFERENCES

[1] F. Galton, *Finger Prints*, Macmillan and Company, 1892.

[2] E. R. Henry, *Classification and Uses of Finger Prints*, HM Stationery Office, 1905.

[3] S. B. Thorat, S. K. Nayak and J. P. Dandale, Facial recognition technology: An analysis with scope in India, *International Journal of Computer Science and Information Security*, vol.8, no.1, 2010.

[4] M. Antonini, M. Barlaud, P. Mathieu and I. Daubechies, Image coding using wavelet transform, *IEEE Trans. Image Processing*, vol.1, no.2, pp.205-220, 1992.

[5] K. Okada, J. Steffens, T. Maurer, H. Hong, E. Elagin, H. Neven and C. von der Malsburg, The bochum/USC face recognition system and how it fared in the FERET phase III test, in *Face Recognition*, Springer, Berlin, Heidelberg, 1998.

[6] S. S. Athale, S. K. Mitra and A. Banerjee, A fractal based approach for face recognition, *Proc. of 2005 International Conference on Intelligent Sensing and Information Processing*, pp.170-174, 2005.

[7] A. D. Potgantwar and S. G. Bhirud, Web enabled based face recognition using partitioned iterated function system, *International Journal of Computer Applications*, vol.1, no.2, pp.30-35, 2010.

[8] N. Al-Saidi and M. Said, Biometric identification using local iterated function, *The European Physical Journal Special Topics*, vol.223, pp.1647-1662, 2014.

[9] R. P. Wildes, Iris recognition: An emerging biometric technology, *Proc. of the IEEE*, vol.85, no.9, pp.1348-1363, 1997.

[10] L. Flom and A. Safir, *Iris Recognition System*, United States Patent, No. 4,641,349, 1987.

[11] J. Daugman, How iris recognition works, in *The Essential Guide to Image Processing*, Academic Press, 2009.

[12] A. E. Jacquin, Image coding based on a fractal theory of iterated contractive image transformations, *IEEE Trans. Image Processing*, vol.1, no.1, pp.18-30, 1992.

[13] S. Lian, Secure fractal image coding, *arXiv preprint arXiv:0711.3500*, 2007.

[14] B. Wohlberg and G. De Jager, A review of the fractal image coding literature, *IEEE Trans. Image Processing*, vol.8, no.12, pp.1716-1729, 1999.

[15] M. Jampour, R. Ebrahimzadeh, M. Yaghoobi and A. Soleimani-Nezhad, Towads a fast method for iris identification with fractal and chaos game theory, *International Journal of Pattern Recognition and Artificial Intelligence*, vol.26, no.4, 1256011, 2012.

[16] P. S. Lee and H. T. Ewe, Individual recognition based on human iris using fractal dimension approach, *International Conference on Biometric Authentication*, pp.467-474, 2004.

[17] M. Vatsa, R. Singh and A. Noore, Reducing the false rejection rate of iris recognition using textural and topological, *International Journal of Signal Processing*, vol.2, no.2, pp.66-72, 2005.

[18] C.-C. Tsai, J.-S. Tau and C.-W. Tao, Iris recognition using Gabor filters and the fractal dimension, *Journal of Information Science and Engineering*, vol.25, no.2, 2009.

[19] R. A. Boby, H. Madasu, S. Anjali and M. Bindal, Extraction of fractal dimension for iris texture, *The 5th IAPR International Conference on Biometrics (ICB)*, pp.330-335, 2012.

[20] W. K. Chen, J. C. Lee, W. Y. Han, C. K. Shih and K. C. Chang, Iris recognition based on bidimensional empirical mode decomposition and fractal dimension, *Information Sciences*, vol.221, pp.439-451, 2013.

[21] N. M. G. Al-Saidi and A. H. Ali, Towards enhancing of fractal image compression performance via block complexity, *NTICT 2017 Annual Conference on New Trends in Information & Communications Technology Applications*, pp.270-277, 2017.

[22] N. M. G. Al-Saidi, A. J. Mohammed and W. Abdulaal, Fingerprints authentication using grayscale fractal dimension, *Al-Mustansiriyah Journal of Science*, vol.29, no.3, pp.106-112, 2018.

[23] M. F. Barnsley, *Fractals Everywhere*, Academic Press, 2014.

[24] J. E. Hutchinson, Fractals and self similarity, *Indiana University Mathematical Journal*, vol.30, no.5, pp.713-747, 1981.

[25] P. Prusinkiewicz and M. Hammel, Language-restricted iterated function systems, Koch constructions and L-systems, *New Directions for Fractal Modeling in Computer Graphics*, 1994.

[26] H. E. Kunze, D. La Torre and E. R. Vrscay, Random fixed point equations and inverse problems using "collage method" for contraction mappings, *Journal of Mathematical Analysis and Applications*, vol.334, no.2, pp.1116-1129, 2007.

[27] Y. Fisher, *Fractal Image Compression Theory and Application*, Springer Science Business Media, 2012.

[28] *Basic Eye Anatomy*, www.eyesightresearch.org/background.htm.