Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: July 2021 **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2022.19.1.0179

Retina Based Glowworm Swarm Optimization for Random Cryptographic Key Generation

Alaa Noori Mazher [1*] ***Jumana Waleed*** [2]

[1] Department of Computer Science, University of Technology, Baghdad, Iraq
[2] Department of Computer Science, College of Science, University of Diyala, Iraq
[*]Corresponding author: 110027@uotechnology.edu.iq[*] , jumanawaleed@sciences.uodiyala.edu.iq
[*]ORCID ID: https://orcid.org/0000-0001-7581-0866[*], https://orcid.org/0000-0003-3474-1029

Received 13/5/2020, Accepted 1/11/2020, Published Online First 20/7/2021

Abstract:

The biometric-based keys generation represents the utilization of the extracted features from the human anatomical (physiological) traits like a fingerprint, retina, etc. or behavioral traits like a signature. The retina biometric has inherent robustness, therefore, it is capable of generating random keys with a higher security level compared to the other biometric traits. In this paper, an effective system to generate secure, robust and unique random keys based on retina features has been proposed for cryptographic applications. The retina features are extracted by using the algorithm of glowworm swarm optimization (GSO) that provides promising results through the experiments using the standard retina databases. Additionally, in order to provide high-quality random, unpredictable, and non-regenerated keys, the chaotic map has been used in the proposed system. In the experiments, the NIST statistical analysis which includes ten statistical tests has been employed to check the randomness of the generated binary bits key. The obtained random cryptographic keys are successful in the tests of NIST, in addition to a considerable degree of aperiodicity.

Key words: Chaotic map, Glowworm Swarm Optimization (GSO), Random cryptographic key generation, Retina.

Introduction:

In order to design any cryptographic system, two significant parts are required; the cryptographic algorithm and cryptographic key [1]. Generally, the strengthening of the cryptographic systems is based on the secrecy of the cryptographic keys. The most cryptographic algorithms require secure, random, hard to memorize and long keys [2]. In the area of key generation, there are two classes: Pseudo-Random Number Generation (PRNG) and True-Random Number Generation (TRNG). In PRNG, the random keys are generated based on the randomness and security of the initial conditions. Generally, the security requirement cannot be satisfied in many PRNG, therefore, this disadvantage enables an attacker to attack the cryptographic system. While in TRNG, the random keys are generated based on the physical sources which are absolutely unpredictable [3].

In biometrics, there are many traits such as the face, fingerprints, and retina that are never the same in either person. Therefore, these traits can be utilized for generating random keys to be used for cryptographic applications. The main processes that should be included in biometric-based keys generation systems are extracting the features and then processing these features to obtain the preferable ones, after that, integrating them with the utilized cryptographic algorithm [4]. The cryptographic systems that are employed human retina possess specific priorities comparing with employing other available biometrics since the retina has the uniqueness in its vascular pattern, and it is embedded deeply in the organ of the human body and this property makes it unalterable, additionally, it does not have a tendency to change much with aging [5].

In recent years, nature-inspired optimization algorithms have acquired considerable popularity for tackling difficult real-world problems and solving complicated optimization functions in which the actual solutions are not available [6, 7]. Comparing with the other conventional algorithms of optimization, the swarm optimization algorithms has the merits of the simple theory, easy

implementation, and the effects of better search [8]. There are lots of new swarm optimization algorithms that are developed to provide rapid and optimal solutions almost in every aspect. In this paper, an algorithm of swarm intelligence inspired by the glowworm behavior has been applied to extract optimal features from the physical biometric retinal images. The proposed system has been utilized these optimal retina features as the entropy source known as biometric random number generation (BRNG) with the chaotic map to generate the random cryptographic keys. The arrangement of this paper is as follows; The essential details of the related systems are summarized in the second section; The algorithm of Glowworm Swarm Optimization (GSO) are explained in the third section; The proposed retina-based keys generation system is explained in the fourth section. In the fifth section, the experimental results are presented. Finally, the outcomes are shown in the last section.

Related Works

Physical biometric traits represent good entropy sources to generate random numbers that are close to TRNG. However, not all these biometric sources can be utilized for generating random numbers, hence, it depends on applying a comprehensive test to decide if the biometric source is appropriate or not [9]. Recently, there are several researchers who worked towards biometric-based keys generation systems, and some of these systems are integrated with chaotic maps to obtain unpredictable random keys for cryptographic applications, and the quality of the generated keys is verified by using the statistical test suites such as the National Institute of Standard and Technology (NIST) tests.

An iris-based key generation system was proposed by Zhu H et al. [10]. In this system, for generating the cryptographic key, the extracted features represent a binary image of the iris edges that are extracted directly by using the Canny edge detector, and then chaotic maps are utilized for overcoming the identical patterns in iris image obtained from the same person. While, Wei W, and Jun Z [11] proposed an iris-based key generation system in which the features represent coefficients obtained from the middle-frequency sub-bands (HL3, LH3, and HH3) by applying the three-level Haar wavelet transform (HWT) on the iris image. In order to generate the random cryptographic key, these extracted coefficients are encoded to binary codes based on their positive or negative values. In this system, the extracted keys are more robust compared with [10] since the frequency transform domain are utilized in the process of extracting the iris features.

Bajwa G, and Dantu R [2] proposed a brain waves-based key generation system in which the human's Electroencephalograms (EEG) signals can be utilized for generating a repeatable and unique cryptographic key. In this system, the features are extracted by utilizing the energy bands resulted from applying the Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). In this system, the random cryptographic key generation includes the selection of features depending on normalized thresholds and the protocol of the segmentation window. Another EEG-based key generation system is proposed by Nguyen D et al. [12]. This proposed system indicated that the EEG signal cannot be utilized directly as a source for generating random keys, rather it needs to be transformed before utilizing as random keys generator. In both systems [2] and [12], the utilization of such a trait of biometric for generating cryptographic keys represents a challenging task compared with other traits since it required devices of recording and mechanisms of feature fusion with better grades.

Panchal G, and Samanta D [13] presented a fingerprint-based key generation system. This system includes several steps to generate the random cryptographic key. Firstly, the image of the fingerprint is divided into blocks, and for each block, the minutiae points, delta and core points are extracted. Secondly, all the straight lines from one minutiae point in a reference block to all minutiae points that exist in all adjacent blocks are computed. Additionally, the straight lines among the minutiae points inside the reference block are also computed. Thirdly, the angle and length of each straight line are computed using delta and core points. Fourthly, the attribute of every straight line is converted to a binary form, then, an operation of XOR is performed between every binary bit of angle and length of a straight line. This system is capable of generating different cryptographic keys based on utilizing different parameters like the number of blocks, and the block size. The main limitation of this system is keeping these parameters secret.

Taha MA et al. [14] presented a retina-based key generation system in which the process of keys generation consists of several stages; firstly, the retina image preprocessing, secondly, the image segmentation using grayscale morphology algorithm. Thirdly, the feature extraction using the entropy algorithm, fourthly, determination of retina center using an adaptive canny edge detection algorithm, fifthly, the technique of linear interpolation is utilized between retina center point

and entropy points for generating other points. Finally, the coordinates of these new points are located the key values in chaotic matrix. In this system, the use of a chaotic map with retinal features for generating the cryptographic keys provides randomness, unpredictability, non-repeatability.

Although all the mentioned related systems are passed most of the NIST tests successfully, they have ignored the robustness of keys which can be achieved through extracting the strong and optimal features from the utilized biometric traits. Therefore, in order to provide this significant requirement; Firstly, the proposed retina-based key generation system uses the Low-frequency sub-band of HWT of the retina image since most of the energy of the image is concentrated in it, which makes it the best position for extracting the retina features; Secondly, the GSO has been applied to extract the optimal features from the LL sub-band of retina image.

Materials and Methods:

Glowworm Swarm Optimization (GSO)

Not many people have ever seen the glowworm, but this name is familiar to everyone. Nevertheless, this is not the cause of utilizing the glowworm in this paper. The fact is that the glowworms are one of the few families of insects in the entire animal kingdom that give the power of emitting natural light which named bioluminescence. The flashing of glowworms which is typically seen in the forests and meadows is a very prevalent sight. However, this remarkable phenomenon is somewhat rare, and the complex behavior of glowworm swarm is represented in assembling hundreds of glowworms on trees and emitting synchronous flashing.

The life cycle of glowworms is a few weeks, through this duration, they should find a mate, partner, and reproduce to increase their species. For achieving this objective, glowworms have developed efficient manners of communicating mating signals via utilizing their capability of controlling the light emission in a diversity of means; they are capable of generating a diverse and wide range of signatures via adjusting the glow parameters; color, brightness, continuous or discrete glow, flash duration, number of flashes per cycle, time period of flashes, and phase variation between female and male flashes [15].

Glowworm Swarm Optimization (GSO) is evolved depending on the glowworm's behavior by K. N. Krishnanand and D. Ghose in 2005 [16]. The ability of glowworms to change the bioluminescence intensity (glow at various intensities) is the behavior that is utilized in the algorithm of GSO. In GSO, every agent or glowworm is supposed to hold a pigment of luminous, named luciferin, and the luciferin's quantity encodes the fitness of glowworm position in the space of objective. This permits the glowworm to glow at an intensity nearly corresponding to the value of function being optimized. Generally, the glowworms are supposed to be attracted for moving towards other glowworms that hold a higher value of luciferin [15].

Algorithmically, the population of n agents is randomly scattered in the search space. At first, all agents should include an equal luciferin quantity l_0. Each iteration in the GSO algorithm includes the following steps [8];

Step 1: Luciferin Update: In this step, every agent is added to its former level of luciferin, and the quantity of luciferin proportional to the fitness of its current position in the space of objective function. Additionally, a fraction of the luciferin value is subtracted for simulating the decay in luciferin with the passage of time. The equation of this step is as follows:

$$l_i(m+1) = (1-d)l_i(m) + \varepsilon F\big(x_1(m+1)\big) \quad (1)$$

Where, $l_i(m)$ denotes the level of luciferin related with agent i at m time, d represents the decay constant of luciferin $(0 < d < 1)$, ε denotes the enhancement constant of luciferin, and $F\big(x_1(m)\big)$ is the objective function value at the agent i 's position at m time.

Step 2: The Movement: In this step, every agent decides to utilize a probabilistic mechanism for moving towards a neighbour which holds a value of luciferin higher than its value (agents are attracted to neighbours which hold brighter glow). To every agent i, the probability of moving towards a neighbour j is as follows:

$$d_{ij}(m) = \frac{l_i(m) - l_i(m)}{\sum_{j \in B_i(m)} l_j(m) - l_i(m)} \quad (2)$$

Where, $j \in B_i(m)$, $B_i(m) = \{j: e_{ij}(m) < r_e^i(m), l_j(m)\}$ represents the neighbours set of agent i at m time, $e_{ij}(m)$ denotes the Euclidean distance between i and j agents at m time, and $r_e^i(m)$ denotes the range of variable neighborhood related with agent i at m time. Let, agent i choose an agent $j \in B_i(m)$ with $d_{ij}(m)$. After that, the discrete time model of the agent movements is as follows:

$$x_i(m+1) = x_i(m) + Z\left(\frac{x_j(m) - x_i(m)}{\| x_j(m) - x_i(m) \|}\right) \quad (3)$$

Where, $x_i(m) \in R^n$ denotes the position of agent i at m time, in the n-dimentional real space R^n, the

step size z is greater than zero, and $\| \cdots \|$ is the operator of the Euclidean norm.

Step 3: Neighborhood Range Update; GSO utilizes an adjusted neighborhood range for detecting the multiple peaks presence in a multi-modal function landscape. Let, r_0 represented the initial neighborhood range of every agent ($r_e^i(0) = r_0 \; \forall i$). This step is accomplished as follows;

$$r_e^i(m+1) = min\left\{r_z, max\{0, r_e^i(m) + \delta(b_m - |B_i(m)|)\}\right\} \quad (4)$$

Where δ denotes a constant, and b_m denotes the controlling parameter for the number of neighbours.

Step 4: Stopping when the criterion is satisfied, else, $m = m + 1$ and go to Step 1.

The Proposed Retina-based Key Generation System

The proposed system includes four main stages; the acquisition and then preprocessing of retina image, then, the separation of the preprocessed retina image into four parts by using the Discrete Wavelet Haar Transform (DWHT), after that, the extraction of the optimal features using the algorithm of GSO, and finally the integration of the optimal features with the Chaotic map to generate the random cryptographic key. Figure 1 illustrates the block diagram of the proposed retina-based key generation system.

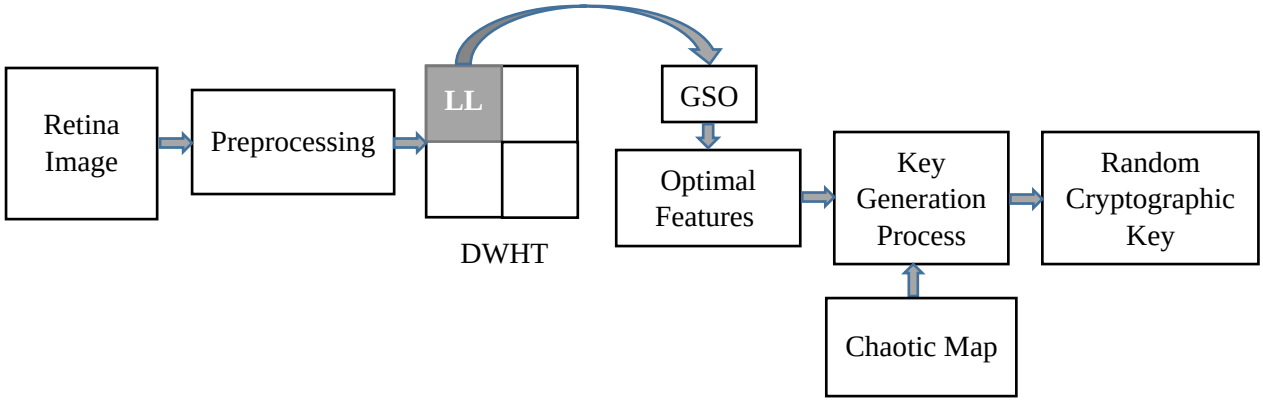


Figure 1. The block diagram of the proposed retina-based key generation system.

Retina Image Acquisition and Preprocessing

Retina image acquisition refers to capturing the retina image by using any retina camera existing in the markets. In this paper, the publicly available Database which is called DRIONS-DB (Digital Retinal Images for Optic Nerve Segmentation Database) has been used. After that, the input retia image needs to be preprocessed. The stage of preprocessing includes several processes:

1- In order to decrease the number of colors, the first pre-processing step is required for converting the RGB color images into Grayscales. The RGB components are segregated from the 24-bits color value for every (i, j) pixel and 8-bits grayscale value is computed. The process of converting is accomplished by calculating the average weight for the RGB value.

$$Grayscale(i,j) = \big((0.3 * R) + (0.59 * G) + (0.11 * B)\big) \quad (5)$$

2- The second pre-processing step is applying an adaptive algorithm of Histogram Equalization to adapt the spacing between every two adjacent gray levels in the histogram, therefore, it prevents the extreme gray pixel merger and the extremely bright local regions in the image. This step works as follows; firstly, record the original gray levels image as f_i, where i=1, …, m-1, and decide the location j of mapped gray level g_i using the ratio $\sum_{h=0}^{i-1} P_h$ and $\sum_{h=i+1}^{n-1} P_h$. Then, achieve the local uniform distribution by comparing i with j, and if j is greater than i, then map forward, else, map backward.

$$j = (n-1)\frac{\sum_{h=0}^{i-1} P_h}{\sum_{h=0}^{i-1} P_h + \sum_{h=i+1}^{n-1} P_h} \quad (6)$$

Where, n denotes the number of gray levels in the original image, $\sum_{h=0}^{n-1} P_h \; equal \; to \; 1$, $P_h = \frac{q_h}{Q}$, q_h is the number of pixels in an image of h^{th} gray level, and Q is the number of all pixels in an image. After that, in the process of mapping, the gray level with a little number of pixels can be phagocytosis via the gray level with a big number of neighborhood pixels. To prevent the phenomena of losing information, an adaptive parameter δ which is based on the information entropy is introduced in gray mapping. The relationship of mapping is as follows:

$$q_h = \log(q_h + 1) \quad (7)$$

$$j = (n-1)\frac{\sum_{h=0}^{i-1} P_h}{\sum_{h=0}^{i-1} P_h + \sum_{h=i+1}^{n-1} P_h}, \delta \in (0, +\infty) \quad (8)$$

3- The third pre-processing step is applying the median filter. This process is often used to remove noise. Such noise reduction is a typical pre-processing step to improve the results of later processing (for example, edge detection on an image).
4- The final pre-processing step is applying the canny edge detection filter to detect and recognize the vessel edges.

Discrete Wavelet Haar Transform (DWHT)

The 1-level DWHT is applied on the pre-processed image and decomposes that image into four sub-bands by performing row by row first and then column by column the result generating the four sub-bands called (LL, LH, HL, HH). LL represents the operational sub-band; it holds the whole operation that wants to be applied to the image.

Optimal Features Extraction Based on GSO

The main aim of GSO is to search for the optimal features in the selected sub-band "LL". The GSO is utilized according to the following steps;

1- Initialize the parameters of GSO: set the generation G =1, number of agents n=3, initial luciferin = l_0. The decay constant of luciferin $d = 0.4$. The enhancement constant of luciferin $\varepsilon = 0.6$. The distance moved by each glowworm when a decision is taken Step size =0.03. Initialize the luciferin levels = 5*ones(n,1). The desired no. of neighbors b_m = 5, and $\delta = 0.08$; No. of Iterations = 100.
2- The distribution of glowworms: glowworms are randomly uniformity distributed in search space. All glowworms carry an equal quantity of luciferin l_0 and on the same initial neighborhood domain radius r_0. The glow-worms search for the sixteen pixels of neighborhood with maximum light in retina image.
3- While G is less than themaximum generation, So, for all glowworms. Firstly, update luciferin according to Equation (1). Secondly, compute the probability of movement according to Equation (2). Thirdly, select a neighbor j using a probabilistic mechanism. Fourthly, the Glowworm i moves toward j according to Equation (3). Finally, update neighborhood range according to Equation (4).
4- Stopping once the number of iterations in GSO is satisfied, otherwise, go to the first step.

Key Generation Process

The length of the generated cryptographic keys is based on the number of optimal pixels extracted from the retina images, in this paper, the length of the generated keys is 128 bits, therefore the number of optimally extracted pixels is 16. In this stage, the retina optimal features (the sixteen extracted pixels) resulted from the previous stage are XORed with the random bits generated from a type of Chaotic map to obtain the final cryptographic key of 128-bits length. In this paper, the Tent map is used which is a one-dimensional Chaotic system, and its equation as follows

$$X_{n+1} = \begin{cases} \frac{X_n}{\mu} & 0 \le X_n \le \mu \\ \frac{1 - X_n}{\mu} & \mu \le X_n \le 1 \end{cases} . Where\ \mu \in (0,1). \mu \neq 0 \cdot 5, here, \mu = 0.62 \quad (9)$$

The Experimental Results:

The proposed system is tested and evaluated on the database DRIONS-DB that includes 110 bitmap retina images of 24 bit/pixel with size (565×584). The NIST Test Suite which includes ten statistical tests has been employed to check the randomness of the generated binary bits key. Fig. 2 demonstrates four samples of the retina images that are belonging to the utilized dataset. Before the process of extracting the optimal features, there are two important stages: the first one is the pre-processing stage which works on detecting the blood vessels with high clarity, and the second stage is extracting the LL sub-bund after applying the 1-level DWHT. Figures 3, 4, 5, and 6 show the obtained retina images after performing these stages.

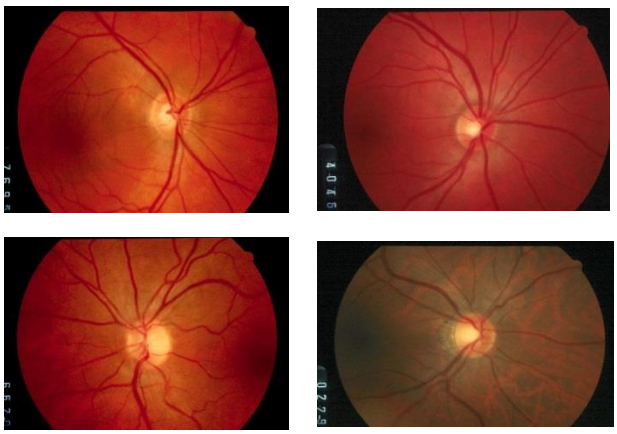
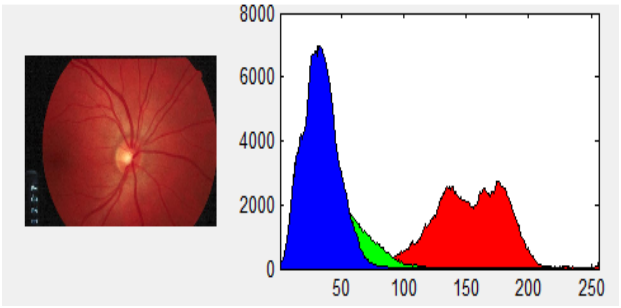
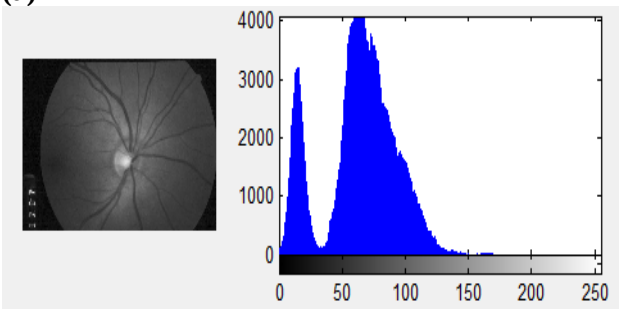


Figure 2. Four retina images samples from DIRONS-DB.

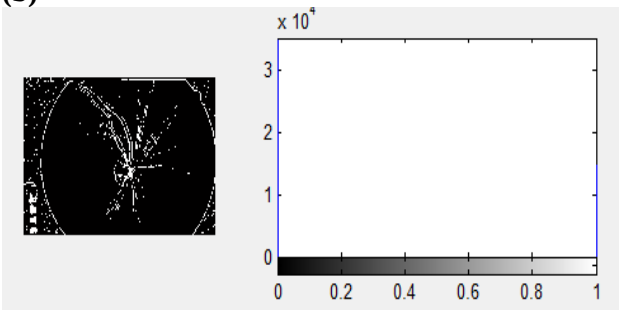
Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986



(a)

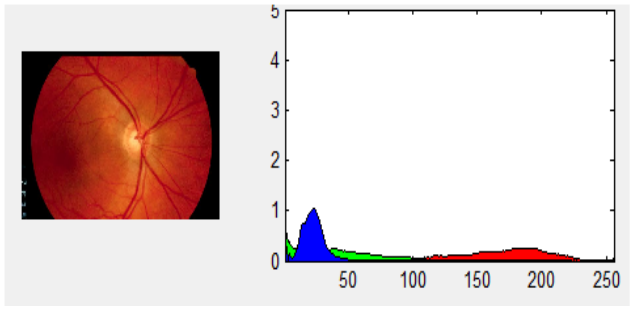


(b)

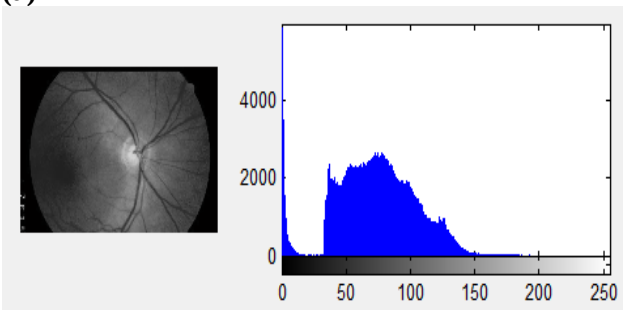


(c)

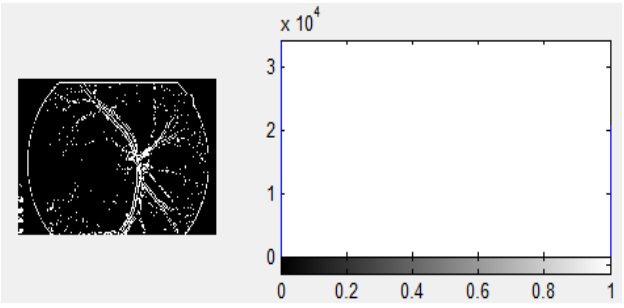
Figure 3. (a) The First sample of retina image, (b) The gray scale image, (c) The resulted image after performing the pre-processing and decomposition stages.



(a)

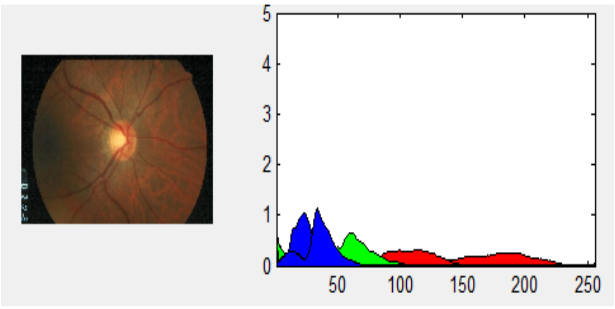


(b)

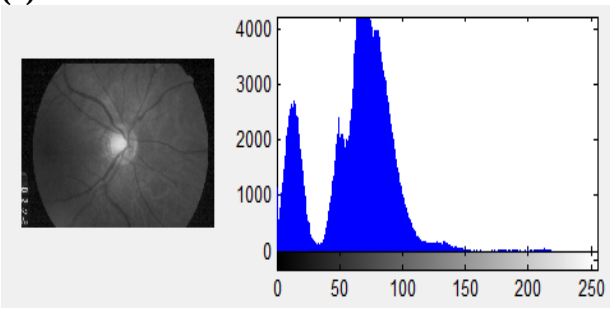


(c)

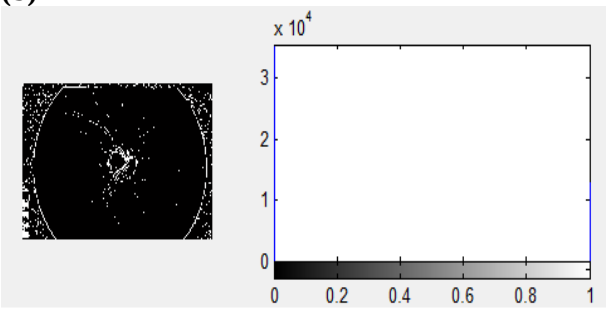
Figure 4. (a) The Second sample of retina image, (b) The gray scale image, (c) The resulted image after performing the pre-processing and decomposition stages.



(a)



(b)



(c)

Figure 5. (a) The Third sample of retina image, (b) The gray scale image, (c) The resulted image after performing the pre-processing and decomposition stages.

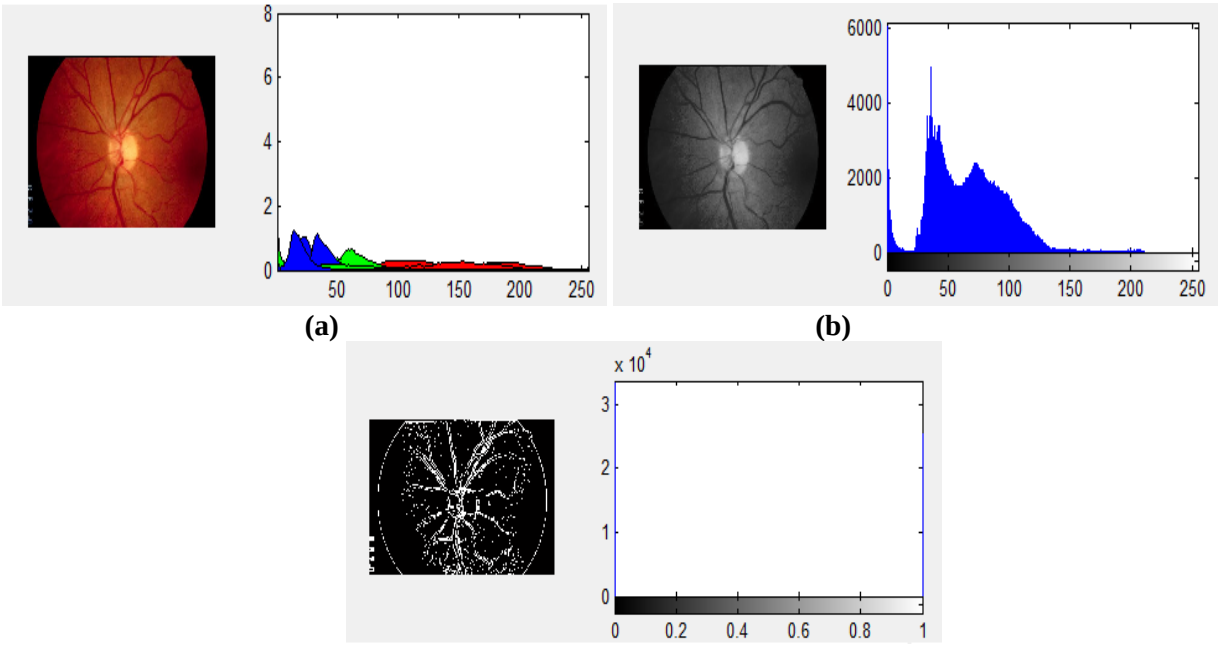
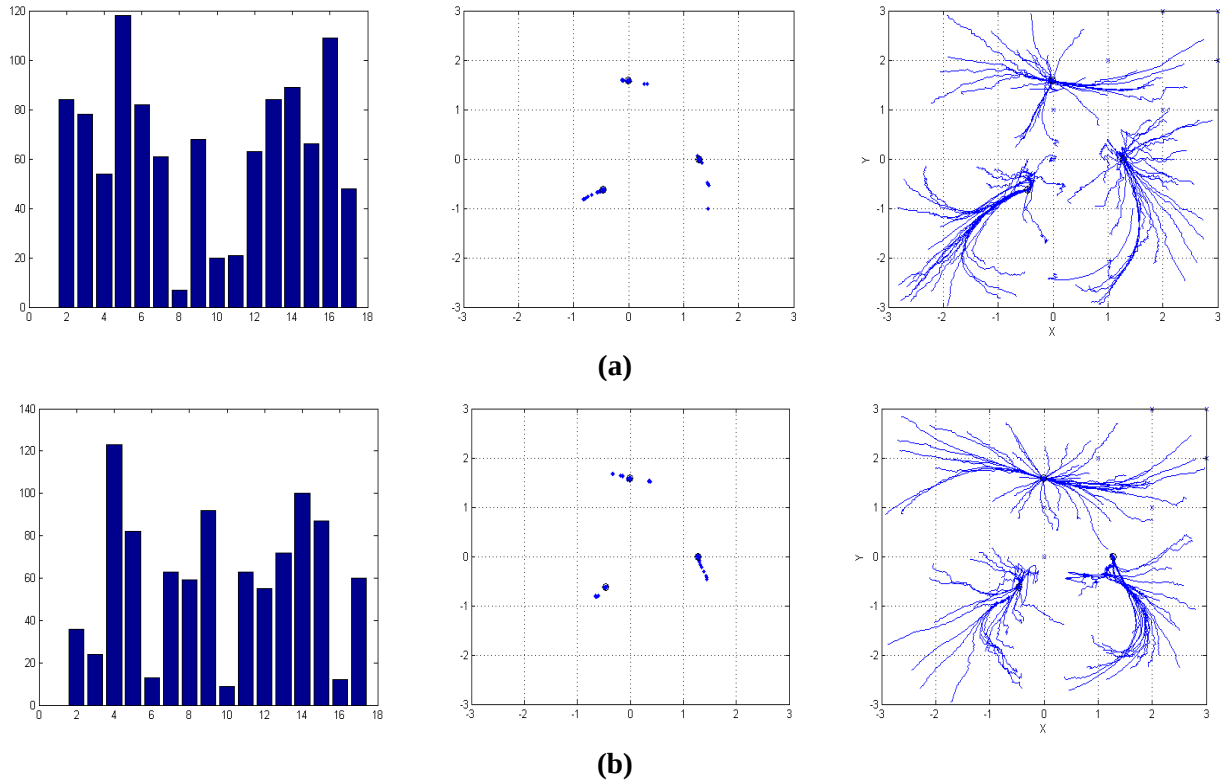
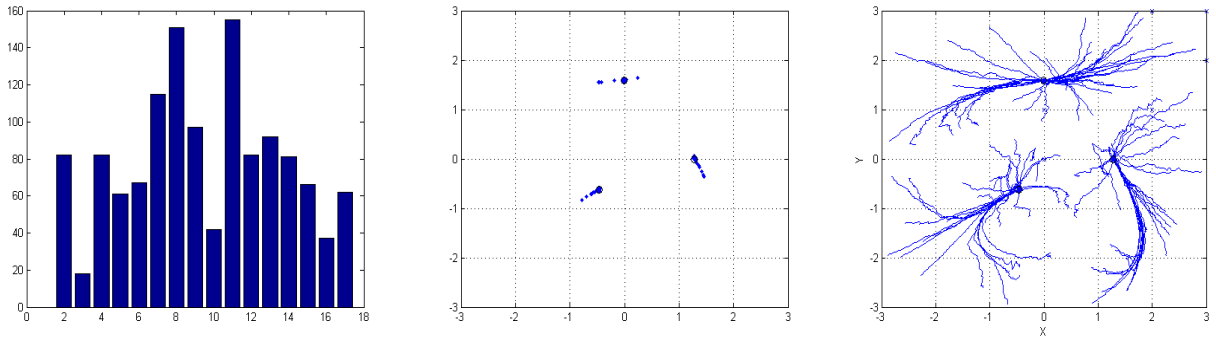


Figure 6. (a) The Fourth sample of retina image, (b) The gray scale image, (c) The resulted image after performing the pre-processing and decomposition stages.

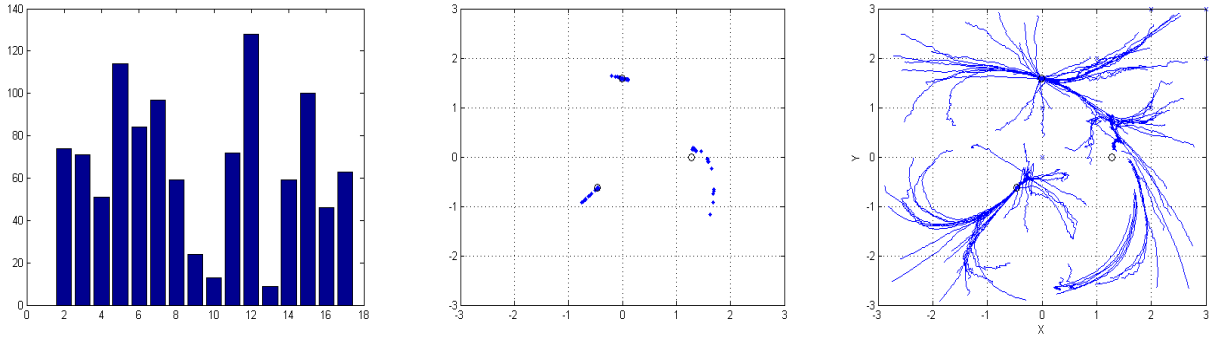
Figure 7 explains the trajectories of glowworms from their initial locations until reaching the final locations (optimal solutions) for the retina images samples.



Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986



(c)



(d)

Figure 7. From (a) to (d), the first figure represents the trajectories of glowworms from their initial locations until reaching the final locations, the second figure represents the optimal locations, and the third figure represents the values of optimal sixteen pixels, for the First, Second, Third, and Fourth samples of retina image respectively.

Table 1 explains the generated cryptographic key of 128-bits length for each retina image sample. Furthermore, Table 2 shows the results of NIST Test Suite for the generated cryptographic keys, and these obtained results passed all the NIST tests successfully.

Table 1. The generated cryptographic keys for the retina images samples.

	Optimal 16 pixels Using GSO	48 109 66 89 84 63 21 20 68 7 61 82 118 54 78 84
The 1st retina image	**Random bits generated from Tent map**	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 0 1 1 0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1
	XOR operation	1 1 0 1 1 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 0 1 1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 1 0 0 0 0 0 1 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 1 1 1 0 1 0 1 0 0 1 0 1 1 0 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0 1 0 0 0 1 0 0 0 0 0 1 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1
	Optimal 16 pixels Using GSO	36 24 123 82 13 63 59 92 9 63 55 72 100 87 12 60
The 2nd retina image	**Random bits generated from Tent map**	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 0 1 1 0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1
	XOR operation	1 1 1 1 0 1 1 0 1 1 0 1 1 0 0 0 0 0 0 0 1 0 1 0 0 0 0 1 1 0 1 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 0 0 0 1 1 1 0 0 1 1 1 0 1 0 1 0 1 1 0 1 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1 0 1 1 0 0 0 1 1 0 0 1 0 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1
	Optimal 16 pixels Using GSO	82 18 84 61 67 115 151 97 42 155 82 92 81 66 37 62
The 3rd retina image	**Random bits generated from Tent map**	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 0 1 1 0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1
	XOR operation	1 1 0 0 0 1 1 1 0 1 1 1 0 1 1 0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 0 0 1 0 0 1 1 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 1 0 0 1 1 1 1 1 0 0 0 0 0 0 0 1 0 1 1 0 1 1 0 1 1 0 1 0 1 0 1 1 0 0 1 0 0 1 0 1 0 1 0 0 1 1 0 1 0 0 1 1 0 0 0 1 1 0 1 1 1 0 0 1 1 0 1 1
	Optimal 16 pixels Using GSO	74 71 51 114 84 97 59 24 13 72 128 9 59 100 46 63
The 4th retina image	**Random bits generated from Tent map**	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 0 1 1 0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1
	XOR operation	1 0 1 1 1 1 1 0 1 0 1 0 0 1 0 1 1 1 1 0 0 1 1 1 1 0 0 1 1 1 1 0 1 0 0 1 0 0 1 0 0 1 1 0 1 1 1 1 1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 0 0 1 1 0 0 1 1 1 1 0 1 0 1 1 0 0 1 1 0 1 1 1 1 1 0 0 1 0 0 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 0 1 0 1 0 1 1 0 0 0 1 1 0 0 1 1 1 1 1 1 0 1 1

Table 2. The NIST Test Suite for the obtained cryptographic keys.

TEST	P Value of the 1st key	P Value of the 2nd key	P Value of the 3rd key	P Value of the 4th key	STATUS
Block Frequency Test	0.44049	0.74049	0.9229	0.6009	Success
Cumulative Sums Test	0.98119	0.88664	0.7921	0.5961	Success
Dft Test	0.4292	0.94129	0.9709	0.9709	Success
Run Test	0.32443	0.93425	0.9111	0.9562	Success
Frequency Test	0.837	0.8011	0.9066	0.9910	Success
Longest Run of One's Test	0.95435	0.96488	0.9188	0.9220	Success
Ndtr Test	0.9348	0.9300	0.9323	0.9778	Success
Non Overlapping Test	0.67568	0.97568	0.8911	0.7229	Success
Rank Test	0.61503	0.81203	0.7885	0.9221	Success
Evaluate Bit Stream	0.6915	0.7918	0.9915	0.9901	Success

The proposed system showed how the exploiting of optimal features in the retina biometric using GSO can lead to extract robust keys, and the utilization of a chaotic map provided high-quality of random, unpredictable, and non-regenerated keys. Also, the obtained results showed the efficiency of the proposed system.

The use of optimization techniques for extracting the robust features from the biometrics should be depended by several researchers for the applications of biometrics recognition and biometrics-based key generation.

Conclusion

An efficient system of retina-based key generation has been proposed in this paper. This proposed system generates a robust, unpredictability, and unique random key by concentrating on the utilization of GSO to extract the optimal features from the most important position of HWT of the retina image. These optimal extracted features are then integrated with chaotic maps to obtain unpredictable random keys for cryptographic applications. Experimental results on the utilized dataset demonstrate that the proposed system passes all the NIST tests, and provides a high randomness characteristic. In future works, the generated key will be used in one of the asymmetric cryptography algorithms for encryption.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Technology

Authors' contributions statement:

The conceptualization, design, data acquisition, analysis, implementation, drafting, proofreading, and modification of this manuscript were accomplished by Alaa Noori Mazher and Jumana Waleed.

References:

1. Mazhar AN, Naser EF. Hiding the Type of Skin Texture in Mice based on Fuzzy Clustering Technique. Baghdad Sci J. 2020 Sep;17(3):967–972.
2. Bajwa G, Dantu R. Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Comp and Sec. 2016 Sep;62:95–113.
3. Kaya T. Memristor and Trivium-based true random number generator. Physica A: Statistical Mechanics and its Applications. 2020 March;542:124071.
4. Pooja S, Arjun CV, Chethan S. Symmetric key generation with multimodal biometrics: A survey. In2016 International Conference on Circuits, Controls, Communi and Comp (I4C) 2016 Oct 4 (pp. 1-5). IEEE.
5. Fatima J, Syed AM, Akram MU. Feature point validation for improved retina recognition. In2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications 2013 Sep 9 (pp. 13-16). IEEE.
6. Waleed J, Jun HD, Abbas T, Hameed S, Hatem H. A Survey of Digital Image Watermarking Optimization based on Nature Inspired Algorithms NIAs. Int J of Sec and Its Applications. 2014;8(6):315–334.
7. Waleed J, Jun HD, Abbas T, Hameed S. An Optimized Digital Image Watermarking Technique Based on Cuckoo Search (CS). ICIC Express Letters Part B: Applications. 2015 Oct;6(10):2629–2634.
8. Hao YY, Zhang GL, Xiong B. An Improved Glowworm Swarm Optimization Algorithm. In2018 International Conference on Machine Learning and Cybernetics (ICMLC) 2018 Jul 15 (Vol. 1, pp. 155-160). IEEE.
9. Bansal M, Kardam H, Khairwal H, sharma J, Narang S. Review On Using Biometric Signals in Random Number Generators. Int J of Adv Res. 2019 April;7(4):1543–1550.

10. Zhu H, Zhao C, Zhang X, Yang L. A novel iris and chaos-based random number generator. Comp and Sec. 2013 July;36:40–48.
11. Wei W, Jun Z. Image encryption algorithm Based on the key extracted from iris characteristics. In2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI) 2013 Nov 19 (pp. 169-172). IEEE.
12. Nguyen D, Tran D, Ma W, Sharma D. Random Number Generators Based on EEG Non-linear and Chaotic Characteristics. J of Cyber Sec and Mobil. 2017 July;6(3):305–338.
13. Panchal G, Samanta D. A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security. Comp & Elec Eng. 2018 July;69:461–478.
14. Taha MA, Hasan TM, Sahib NM. Retina Random Number Generator for Security Applications. 2019 2nd Int Conference on Engineering Technology and its Applications (IICETA). 2019 Aug 27-28; Al-Najef, Iraq. 2019;99-104.
15. Krishnanand KN, Ghose D. Glowworm Swarm Optimization: Theory, Algorithms, and Applications. Studies in Comp Intelligence. 1st ed. Springer Int Publishing; 2017. 698.
16. Krishnanand KN, Ghose D. Detection of multiple source locations using a glowworm metaphor with applications to collective robotics. Proceedings 2005 IEEE Swarm Intelligence Symposium. 2005 June 8-10; Pasadena, CA, USA. 2005; 84-91.

توليد مفتاح التشفير العشوائي بالاعتماد على شبكية العين و تحسين سرب الدودة المتوهجة

علاء نوري مزهر [1] **جمانة وليد [2]**

[1] قسم علوم الحاسبات، الجامعة التكنولوجية، بغداد، العراق
[2] قسم علوم الحاسوب، كلية العلوم ، جامعة ديالى، ديالى، العراق

الخلاصة:

ان توليد المفاتيح المستندة إلى المقاييس الحيوية يمثل استخدام الميزات المستخرجة من السمات التشريحية (الفسيولوجية) البشرية مثل بصمات الأصابع أو شبكية العين أو السمات السلوكية مثل التوقيع. تتميز القياسات الحيوية لشبكية العين بمتانة متأصلة، وبالتالي، فهي قادرة على توليد مفاتيح عشوائية بمستوى أمان أعلى مقارنة مع السمات الحيوية الأخرى. في السنوات الأخيرة ، اكتسبت خوارزميات التحسين المستوحاة من الطبيعة شعبية كبيرة في معالجة المشكلات الواقعية الصعبة وحل وظائف التحسين المعقدة التي لا تتوفر فيها الحلول الفعلية. في هذه الورقة ، تم اقتراح نظام فعال لتوليد مفاتيح عشوائية آمنة وقوية وفريدة من نوعها تستند إلى ميزات شبكية العين لتطبيقات التشفير. يتم استخراج ميزات شبكية العين باستخدام خوارزمية تحسين سرب الدودة المتوهجة (GSO) والتي توفر نتائج واعدة من خلال التجارب باستخدام قواعد بيانات شبكية العين القياسية. بالإضافة إلى ذلك، من أجل توفير مفاتيح عشوائية عالية الجودة وغير متوقعة وغير مجددة، تم استخدام الخريطة الفوضوية في النظام المقترح. حيث يتضمن النظام المقترح أربع مراحل رئيسية: التقاط صورة شبكية العين باستخدام أي كاميرا شبكية موجودة في الأسواق، أو باستخدام قاعدة البيانات المتاحة والتي تسمى DRIONS-DB، ثم معالجتها معالجة اولية، ثم فصل صورة شبكية العين المعالجة مسبقًا إلى أربعة أجزاء باستخدام تحويل مويجات الهار المنفصلة ذات المستوى الواحد (DWHT)، بعد ذلك ، يتم استخدام النطاق الفرعي ذو التردد المنخفض (LL) للمرحلة التالية حيث يمثل النطاق الفرعي التشغيلي، بعد ذلك ، يتم استخراج الميزات المثلى باستخدام خوارزمية تحسين سرب الدودة المتوهجة (GSO)، وأخيرًا يتم دمج الميزات المثلى مع الخريطة الفوضوية لإنشاء مفتاح التشفير العشوائي. في النتائج التجريبية، تم استخدام التحليل الإحصائي NIST الذي يتضمن عشرة اختبارات إحصائية للتحقق من عشوائية مفتاح البت الثنائي المولد. مفاتيح التشفير العشوائية التي تم الحصول عليها كانت ناجحة في اختبارات التحليل الإحصائي NIST ، بالإضافة إلى درجة كبيرة من اللامركزية.

الكلمات المفتاحية : خريطة الفوضى، تحسين سرب الدودة المتوهجة (GSO)، توليد المفتاح العشوائي، شبكية العين.