Webology (ISSN: 1735-188X)
Volume 19, Number 2, 2022

Iris Image Cryptography Using AES And Black Widow Optimization Algorithm

Anfal thaer hussein alrahlawee[1] , Oguz bayat[2]

Abstract

Cryptography methods are becoming increasingly important for ensuring secure data transfer in a variety of applications. As the usage of images in industrial processes grows, it's more important than ever to keep proprietary image data safe from unwanted access. The Advanced Encryption Standard (AES) is a great block cipher with several advantages in data encryption. So, in numerous image processing applications, multilevel thresholding image segmentation has gotten a lot of interest. Thresholding is a common image segmentation method that separates an object from its background based on the distribution of gray levels. Metaheuristic algorithms like the Black Widow Optimization (BWO) Algorithm are one technique to determine the Otsu threshold. This paper aims to show how to use the iris template to build a unique and more secure cryptographic key. The iris photos are processed to create an iris template or code, which is then used for encryption and decryption. The preprocessing step takes advantage of images thres holding using a Black Widow Optimization (BWO) algorithm. The iris portion of the eye image is segmented and then encrypted and decrypted using the AES method, which may be employed in various applications requiring information security. The experimental findings show that the encryption and decryption algorithms used on a data set of iris images were fast and more secret.

Keywords: Image Segmentation, Thresholding, Black Widow Optimization (BWO), Iris, Cryptography, Advanced Encryption Standard (AES).

1. Introduction

Digital data such as images, audio, and video became more readily available with the introduction of the Internet. Content authentication, security, copyright protection, and ownership identification are all difficulties that arise due to easy access to multimedia [1]. Currently, as an authentication technique, people choose a shorter password. which is vulnerable to attack. Biometric technologies such as fingerprint scanning, voice authentication, face recognition, signature, hand geometry, and iris identification are now widely used, particularly in security applications [2]. Cryptography is one of the most essential technologies nowadays and a widely used technique for protecting data from intruders through the use of two key processes:

encryption and decryption [3]. The AES algorithm is one of the symmetric cryptographic encryption algorithms [4]. One of the most challenging and critical tasks in digital image processing is image segmentation [5]. Because of its simplicity and computational efficiency, picture thresholding is a common technique for image segmentation [6]. The main principle behind image thresholding is to use gray-level distribution to automatically determine an optimal gray-level threshold value, then compare each pixel in the image to the threshold value to distinguish items of interest from the background. Many automatic thresholding techniques have been presented in the literature due to their vast applicability to different fields of image processing and applications [7]. Using metaheuristic algorithms like the BWO as an option to find thresholds depending onthe Otsu threshold approach. At the appropriate time, these algorithms can determine the image's important thresholds [8].In this study, we proposed an approach to use the iris biometric to generate a key in the AES algorithm instead of the text key.

2. Related Work

The preceding studies are examined in this section.
In 2017, authors presented yet another security demonstration that displays a plan for successful correspondence security using AES encryption and unscrambling. It depends on AES Key Expansion, which is a selective encryption method, or on the operation of an image pixel arrangement with a 128-piece key that changes for each pixel arrangement.The transmitter and receiver both know the secret key when using AES encryption. Even if an eavesdropper knows the plaintext and the ciphertext, the AES technique remains safe; the key cannot be obtained by any known means [9]. In 2018, authors developeda new image encryption technique that combines the sequence of chaos with animproved AES algorithm. Using the chaotic sequence, the encryption key is constructed in this way.The input image is then encrypted using an improved AES method and the chaotic system's round keys. Asuggested solution not only eliminates the algorithm's temporal complexity but also adds diffusion capability, making the process' encrypted images resistant to differential attacks.The proposed method's key space is large enough to withstand brute-force attacks [10]. In 2021, authors present Round Key Permutation (RKP) as a new secret diffusion scheme for encrypting images by block-based on nonlinear, dynamic, and pseudorandom permutation, because images are due to their size and information, they are considered exceptional data, which is two-dimensional and characterized by high redundancy and strong correlation. The master and sub-keys are used to create the permutation table.Second, the permutation table will be used to scramble pixels for each block that needs to be encrypted. Following that, the AES encryption method is applied [11].

3. Image Processing

A function called a Two-Dimensional Image defines the Image. It has plane coordinates for spatial coordinates and amplitude for pair coordination, which can be written as f. (x, y). The x and y of gray-level images were used to represent the intensity of such coordinates [12]. Digital image processing is employed when spatial coordinates and intensity values are finite with

discrete quantities. With the help of basic mathematical calculations, it is possible to evaluate and edit digital images to increase their quality [13].The technique of processing digital photographs using various algorithms is known as Digital Image Processing (DIP). Image segmentation is one of these algorithms or approaches [14].

3.1.Image Segmentation

The technique of segmenting an image into discrete portions with similar pixel attributes is known as picture segmentation. The ideal segmentation strategy for pixels is whenall adjacent pixels must have different values based on continuity and similarity features, and they should all relate to almost the same class of multivariate values and form connected regions[15].

3.2. Thresholding

The thresholding approach is a quick and easy way to separate important things from the backdrop [16]. When compared to a gray level image, which typically contains 256 levels, the segmented image created through thresholding offers the advantages of limited storage space, faster processing time, and manipulation simplicity. As a result, thresholding strategies have gotten a great deal of publicity in the last two decades [17]. Thresholding is a non-linear procedure that turns a gray-scale image into a binary image by assigning two levels to pixels that are below or above a threshold value [18]. Nobuyuki first proposed the Otsu multilevel thresholding method in 1979, and it is a global thresholding type. The Otsu approach is popular because it comprises a basic yet effective method for image segmentation that relies just on different classes' maximum variance values. The image intensity value can be computed using the L intensity level of each RGB color component's gray image using equation (1) [19]:

$$\mathrm{ph}_i^c = \frac{\mathrm{h}_i^c}{\mathrm{N}} . \sum_{i=1}^{N} \mathrm{ph}_i^c = 1 \qquad (1)$$

$$\mathrm{C} = \begin{Bmatrix} 1.2.3 & \text{if RGB} \\ 1 & \text{if grayscale} \end{Bmatrix}$$

Where,
ph_i^c= Distribution probability
h_i^c= From i to c, the pixel value corresponds to the intensity level.
N= the number of image's pixels.
I= intensity level ($0 \leq i \leq L\text{-}1$)
C= content of an image (RGB or Grayscale)

4. Swarm Intelligence

Swarm intelligence has piqued the curiosity of many researchers in a variety of fields (SI). SI defines collective intelligence as "the emergent collective intelligence of groupings of simple agents". SI is the collective intelligence behavior of self-organized and decentralized systems, such as artificial groupings of simple agents.SI includes foraging in groups, cooperative transportation, social insect nest-building, and community sorting and clustering [20].One of the newest and most important of these algorithms is:

4.1.Black Widow Optimization Algorithm (BWO)

The technique begins with a population of spiders, each representing one possible answer. The spiders then get together to reproduce, resulting in a new generation. Males have been reported to be consumed by female black widows during mating or shortly following [21]. The female holds the sperm in her web before permitting them to enter the egg sac, as seen in Fig. 1. (a). The juvenile spiders appear after 11 days and can stay on the mother spider's web for up to a week, often eating one other, as shown in Fig. 1. (b). They eventually leave the web when they are swept away by the wind [22].

(a)

(b)

Figure 1. (a) The Egg Sac of a Female Black Widow Spider, (b) Baby Spiders Dispose of Their Egg Sacs [22].

Algorithm (1) below describe the BWO in detail:

Algorithm (1). Black Widow Optimization(BWO)
Input:highestnumber of iterations possible, the procreation ratio, Cannibalism Rates, Mutational rate
Output: The goal function has a near-optimal solution.
//Initialization **1:**Black widow spiders in their original population for a D-dimensional issue, each pop is a D-dimensional chromosomal array. **//Loop until the terminal condition** **2:**Determine the reproductions' number "nr" based on the procreating rate. **3:**In pop, select the finest number solutions and store them in the pop1 folder. **// Procreating and Cannibalism** **4:** For i=1 to nr do **5:**Choose two solutions at random as parents from pop1. **6:**Produce "D" children. **7:**Father should be destroyed. **8:**Destroy some of the youngsters based on the rate of cannibalism (brand-new solutions) **9:**Store the rest of the solutions in pop2.

10: End For
// **Mutation**
11: Compute the number of mutation children "nm" based on the mutation rate.
12: For i=1 to nm do
13: Choose one of the pop1 solutions.
14: Create a new solution by randomly changing one of the solution's chromosomes.
15: Store the new one as a pop3 file.
16: End For
// **Updating**
17: Updating pop = pop2 + pop3
18: Restore the most effective solution.
19: Restore the most appropriate solution from pop.

5. Cryptography Concept

Cryptography is a combination of mathematics and security engineering that allows specific information to be transmitted via communication channels in the face of adversarial or impostors. It provides us with the instruments that are at the heart of the majority of today's security solutions.Converting the original plain text to ciphertext (encryption operation) and restoring the primary text from ciphertext is the most appropriate key enabling approach for protecting various systems (decryption operation) [23]. As a result, unless the key used in the encryption technique is known, it will be tough to restore files to their original state [24].The main components of cryptography are an algorithm (a cryptographic approach) and the algorithm's key. A method is a quantitative sequence, and the key is a variable that affects data. The major goal of cryptography is to ensure security principles including Non-repudiation, confidentiality, data integrity, authentication, and authorization [25]. The two types of encryption algorithms used in cryptography are asymmetric (public) key algorithms and symmetric (secret) key algorithms. Only one key is used for both encryption and decryption in symmetric algorithms like DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC2, and RC6.As illustrated in Fig. (2) [26], In asymmetric algorithms (public-key algorithms), two keys were employed: SSH, DH, DSA, RSA, and SSLsince both the encryption and decryption processes have their keys (public and private key).

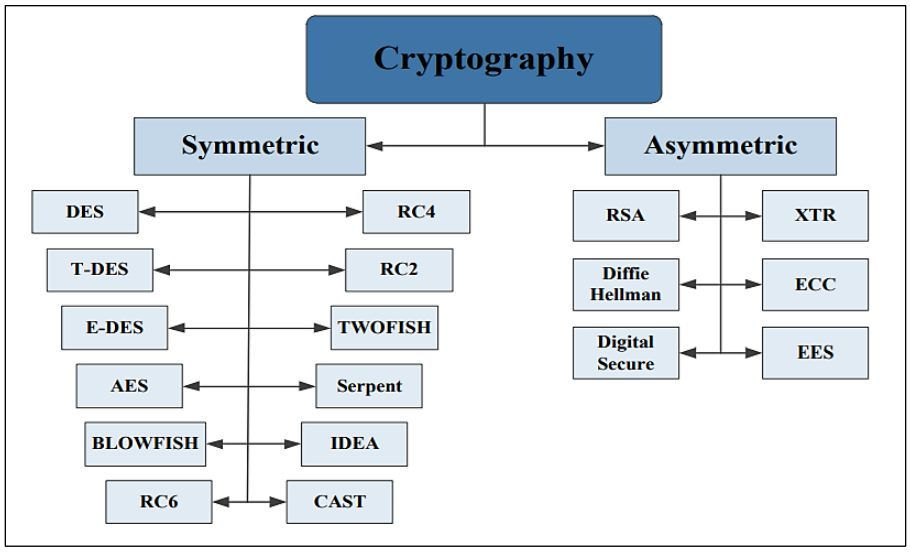


Fig. 2. The Classification of Encryption Algorithms [26].

5.1. Advanced Encryption Standard (AES)

In 2001, NIST proposed this algorithm as a modern ciphering approach to replace DES. Any set of databases could be provided by AES. The AES algorithm encodes 10 rounds for 128-bit keys during encryption and decryption. To deliver the final encoded message, for 192-bit keys, go through 12 rounds, and for 256-bit keys, go through 14 rounds. AES allows for a 128-bit data length that can be broken into four main active blocks.Those elements are handled as a single line of bytes, which are integrated into the state matrix, a 4*4 matrix[27].The cipher begins with an "Add round key stage" for encoding and decoding. However, shortly before the final round, the output is subjected to nine fundamental rounds, each of which includes four transformations: 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, and 4) Add round Key. Mix columns transformation is not accessible in the ninth round. The full procedure is depicted in Figure (3). Decryption is the inverse process, with the following phases [28]:

- **Substitute Byte Transformation:** AES is made up of 128-bit data blocks, which means that each database item comprises 16 bytes. In sub-byte transformation, each bite of a data item is turned into another piece by utilizing an 8-bit substitution box called the Rijndael s-box.
- **Shift Rows Transformation:**This is a straightforward transposition; this means that the bytes in the last three lines of the state which are dependent on row position are cycled.The second line does a one-byte circular left shift. While circular shifts of two bytes and three bytes took place in the third and fourth rows, respectively.
- **Mix Columns Transformation:** it is the inverse of a multiplication set of each state's column. Every is multiplied by a stable matrix. Bytes are treated as multiple names in this operation.
- **Round Key Transformation:**A bit-like XOR between the round key's 128 bits and the current state's 128 bits.Transformation is the polar opposite of this.

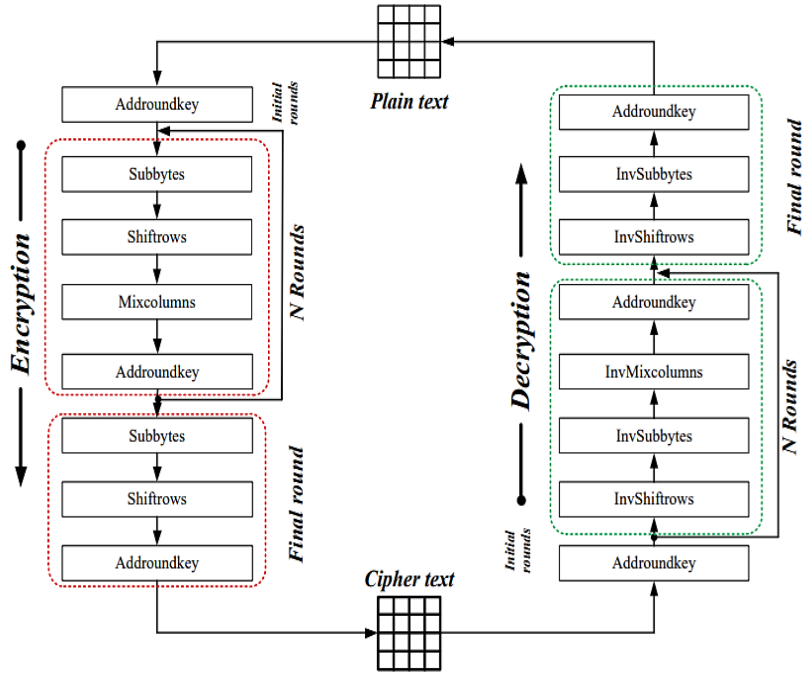


Fig. 3. Advanced Encryption Standard Process [28].

6. Proposed System

Because biometric templates are maintained in a centralized database, they may be updated by an attacker as a result of security threats. Authorized users will not be able to access the resource if the biometric template is changed. AES approaches can be used to secure the iris template to deal with this problem. The proposed system will be made up of several sub-systems.These are the stages:

6.1. Dataset Description

The dataset which used in this study was downloaded from the Kaggle website. The Multimedia University (MMU1) database contains Eye Images for training models of IRIS-based Biometric Attendance Systems. IRIS patterns for each eye are unique to each individual, which aids in identifying a person. This dataset contains 5 photos of each person's left and right IRIS, for a total of 460 images, as well as a few empty files. Individual identification/classification of an IRIS image according to a preserved dataset can be done using IRIS segmentation. Figure (4) illustrate some of the images used in this work:

Fig. 4. Examples of dataset images

6.2. Preprocessing Phase

The first step of this system is image segmentation, this phase consists of three processes as follows:

a) Segment iris image using Otsu thresholding

Segmentation is used to extract the iris from an eye image. The boundary of the iris is searched using multilevel thresholding. Eyelids are recognized and eyelashes are separated using the threshold approach by fitting two lines using the improved Otsu thresholding.

b) Optimize segmentation using BWO Algorithm

To get the optimum threshold, this method compares all of the image's thresholds inbetween 0 and 255, if the value of thresholds is greater than 1 and equals n, the value corresponds to 255n. The number of states required to discover thresholds grows in lockstep with the number of thresholds, adding to the problem's already high complexity. The proposed method, on the other hand, can calculate this number of thresholds with a little error made in an acceptable amount of time.A well-formulated problem, each solution to be counted as a participant in the Black Widow Optimization (BWO) process, and a correctly stated objective function are all prerequisites for the proposed strategy. Each solution to the problem in the proposed method is a group of image histogram thresholds, which is given by Eq. (2). Each solution is comprised of a group of thresholds or a black spider in the sharpness of the lighting range between 0 and 255, and a population of these solutions, such as Eq. (3), As part of the BWO algorithm's population, this is generated at random.

$$BWO = \ll \mathrm{BWO}_{\mathrm{i}}^{1}, \mathrm{BWO}_{\mathrm{i}}^{2}, \mathrm{BWO}_{\mathrm{i}}^{3}, \ldots, \mathrm{BWO}_{\mathrm{i}}^{\mathrm{D}} \gg \quad (2)$$

$$\mathrm{BWO}=\begin{bmatrix} \mathrm{BWO}_{1}^{1} & \mathrm{BWO}_{1}^{2} & \ldots & \mathrm{BWO}_{1}^{\mathrm{D}} \\ \mathrm{BWO}_{2}^{1} & \mathrm{BWO}_{2}^{2} & \ldots & \mathrm{BWO}_{2}^{\mathrm{D}} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{BWO}_{\mathrm{n}}^{1} & \mathrm{BWO}_{\mathrm{n}}^{2} & \ldots & \mathrm{BWO}_{\mathrm{n}}^{\mathrm{D}} \end{bmatrix} \quad (3)$$

In this situation, the$\mathrm{BWO}_{\mathrm{i}}$is a member of the current algorithm and in the image histogram representation, a threshold vector. In the proposed algorithm's i^{th} component, $\mathrm{BWO}_{\mathrm{j}}$ is also the image's j^{th} threshold, and D is the image's total number of thresholds. In these equations, BWO is the population of n thresholds with n elements of the suggested technique.The Otsu goal function needs to look at each of these thresholds. Eq. (4) can be used to analyze a spider or a threshold set:

$$f_{Otsu} = w_0(\mu_0 - \mu_T)^2 + w_1(\mu_1 - \mu_T)^2 + \ldots + w_m(\mu_m - \mu_T)^2 \quad (4)$$

The various thresholds are the optimal solution of m such as vector $\{t1, t2, \ldots, tm\}$ for image threshold. The histogram of the image is divided into m + 1 portions. using this set of thresholds, such as threshold classes $\{C0, C1, \ldots, Cm\}$ of light intensity. This function may

be given each threshold set to evaluate the population of the proposed technique through using the defined objective function, and also the value of each spider can be calculated using Eq. (5):

$$f_{Otsu}(\mathrm{BWO}) = \begin{bmatrix} \mathrm{f\,Otsu}\,(\mathrm{BWO}_1^1 & \mathrm{BWO}_1^2 & \dots & \mathrm{BWO}_1^{\mathrm{D}}) \\ \mathrm{f\,Otsu}\,(\mathrm{BWO}_2^1 & \mathrm{BWO}_2^2 & \dots & \mathrm{BWO}_2^{\mathrm{D}}) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{f\,Otsu}\,(\mathrm{BWO}_{\mathrm{n}}^1 & \mathrm{BWO}_{\mathrm{n}}^2 & \dots & \mathrm{BWO}_{\mathrm{n}}^{\mathrm{D}}) \end{bmatrix} \quad (5)$$

Many random thresholds, each of which is a spider, were first produced in this method, and their domain can be thought of as the minimum and highest sharpness of lighting in the photographs, with this sharpness of lighting being Eq. (6):

$$\mathrm{BWO_i} = L + (U - L).rand\,(0,1) \quad (6)$$

The image's both the lowest and highest sharpness of lightingsare represented by L and U, respectively, so although rand (0,1) is an integer that's also chosen at random from 0 to 1. The proposed algorithm's relations are used on these threshold vectors and their values are altered at each iteration. The following are the phases of the suggested technique for establishing optimal Otsu thresholds utilizing the BWOalgorithm:

- The parameters of a proposed approach are set, including population volume and the maximum number of BWO rounds.
- The suggested method necessitates the use of an image as its input.
- After it has been pre-processed, the input image's quality improves.
- The image's histogram diagram is determined, as well as the frequency of sharpness of lighting employed in it.
- A threshold group is regarded as a component of the suggested method and the suggested algorithm generates several such arrays as members of a random population.
- The Otsu thresholding objective function was used to evaluate each of the suggested algorithm's threshold vectors or population members.
- As the most ideal answer to the provided procedure, the most ideal threshold vector is produced, which contains the best thresholds.
- The blending and combining phase is based on two deserving parents picked from the image's thresholds.
- In the Otsu thresholding, the cannibalism process is employed to get rid of the population with a low density or a group of thresholds that do not optimize the target function.
- A mutation phase occurs in good populations or at appropriate thresholds.
- The threshold vectors in the suggested technique are adjusted after each iteration, and their optimal value is evaluated afresh.
- The algorithm iteration counter is increased by one unit, and the preceding steps are repeated if the counter is lower than the maximum number of iterations, the next step is taken; otherwise, the previous step is repeated.

- The image is thresholded using the best threshold vector available.
- In this categorization, the input image is segmented using thresholds.

Images after this phase are present in Figure (5).

Fig. (5). Images after thresholding and segmentation

6.3. Encryption Phase

Figure (6) depicts the operationof encrypting data. The steps in the encryptionoperation are as follows:

Step 1: To construct the iris binary code, the iris image was retrieved using a thresholding procedure.
Step 2: By using AES cryptography, the user's identifying data is encoded in the binary coding for the iris image.
Step 3: After the encryption procedure, a ciphertext is formed and stored in the datab

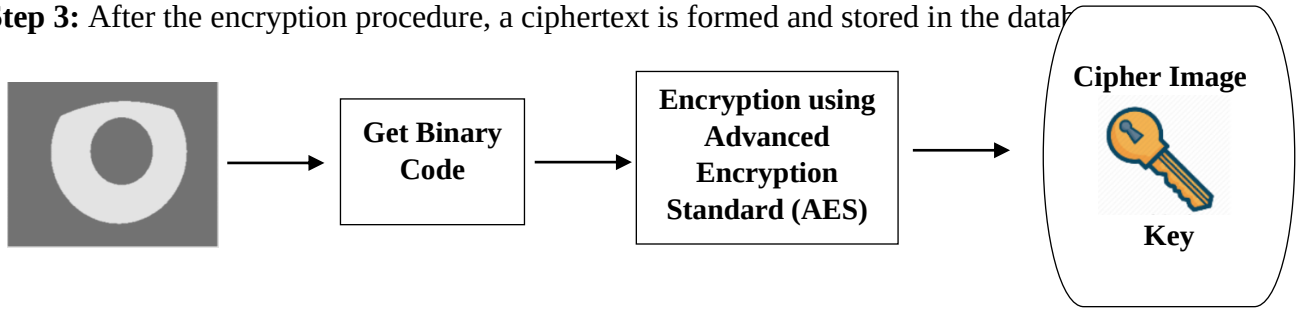


Fig. 6. AES encryption process of the proposed system.

6.4. Decryption Phase

The decryption operation of proposed method is depicted in Figure 7, with the steps of decryption underlined. To acquire the user identifying data, the iris image that was made public will be decrypted using the AES cryptographic technology with the ciphertext.

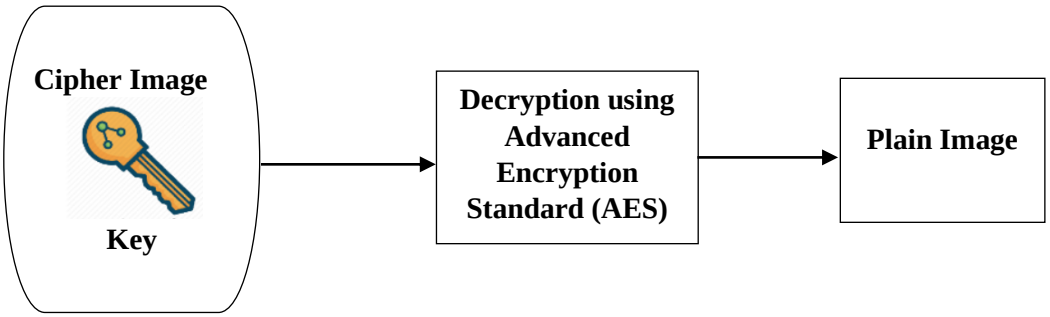


Fig. 7. AES decryption process of the proposed system.

7. Evaluation Metrics

There are two types of metrics in this system, the first one was used to evaluate the performance of the BWO algorithm of enhancing threshold. While the other one was used to measure the encryption algorithm's strength which uses the features of the iris image to encrypt data.

7.1.Preprocessing Evaluation

Image quality approaches can be listed as follows [29]:

- **Mean Square Error (MSE):** It is the most widely employed image quality metric estimator. The lower the value, the better, because it's a broad reference metric. Eq. (7) defines how to obtain the value of this metric between two images, such as $g(x.y)$ and $\hat{g}(x.y)$ is formulated as in an Eq. (7):

$$\text{MSE} = \frac{1}{MN}\sum_{n=0}^{M} \quad \sum_{m=1}^{N}[\hat{g}(n.m) - g(n.m)]^2 \quad (7)$$

- **Peak Signal to Noise Ratio (PSNR):**It is the most widely used metric for evaluating the quality of lossy image compression codec reconstruction.This metric value fluctuates between 30 and 50 dB for 8-bit data representation and between 60 and 80 dB for 16-bit data in image and video compression quality degradation. PSNR is calculated as follows:
  $\text{PSNR} = 10 \log_{10} (\text{peakval}^2)/\text{MSE}$ (8)
- **Structure Similarity Index Method (SSIM):**It determines how comparable two photos are: the original and the recovered. SSIM is expressed as:

$$\text{SSIM}(x.y) = [l(x.y)]^{\alpha} \cdot [c(x.y)]^{\beta} \cdot [s(x.y)]^{\gamma} \quad (9)$$

7.2.Encryption Evaluation

Two measures were used to evaluate the encryption of images [30] as follows:

- **Unified Average Changing Intensity (UACI):**It calculates the average difference in intensity between the plain and ciphered images.
  $$\text{UACI} = \frac{1}{W*H}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|f(i.j)-\hat{f}(i.j)|}{256}\right] * 100\% \quad (10)$$
- **Image Encryption Quality:** The following factors can be used to assess image encryption quality:
  $$\text{Encryption Quality} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|f(i.j)-\hat{f}(i.j)|}{256} \quad (11)$$

Let $f(i.j)$and $\hat{f}(i.j)$denotes the original (plain-image) and encrypted (cipher-image) images, both of which are M×N pixels in size and have L grey levels.

8. Results and discussion

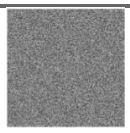
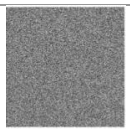
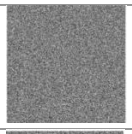
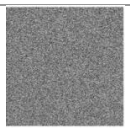
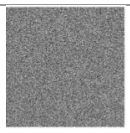
The results of preprocessing phase are shown in Table (1) as follow:

Table. 1. Preprocessing performance metrics

Data	Threshold	PSNR	SSIM
	3346.1452	20.3593	0.9673
	2129.3618	24.5236	0.9729
	758.1093	26.0854	0.9862
	1298.4520	27.9854	0.9919
	1624.3823	29.4539	0.9658

In a thresholding strategy, the highest PSNR and SSIM values reflect theaccuracy of the algorithm. Depending on the outcome of the trials in the tables in the query, the suggested approach has produced values for the objective function, PSNR, and SSIM in the majority of cases. In reality, the suggested method's maximum of these three indications suggests that it gives a much better threshold of images.Table (2), show the value of these metrics on encryption and decryption processes.

Table. 2. Encryption quality measurements

Data	UACI	Encryption Quality
	33.02%	100
	32.82%	99
	31.43%	98
	32.68%	99
	30.98%	98

Through the results obtained, it is clear that the high values of UACI indicate the great difference of the pixel values between the original image and the encrypted image, and this indicates the strength of the encryption and thus the difficulty of obtaining information by the attackers.

9. Conclusion

By rising the number of thresholds, the suggested strategy yields a higher target function value, whilst the preprocessing provided method yields greater PSNR and SSIM index values are more accurate than other meta-heuristic techniques, and they take less time to run.In this paper, the proposed method is used to segment iris images as a practical application. Experiments using medical sample photos show that the suggested method can extract iris areas in the eye with a high degree of accuracy.In the proposed system AES encryption techniques are applied to protect the iris template in the database.The security of the images kept in the database is ensured in this way, as the images are encrypted for usage in sensitive security applications, giving the images increased security and reliability. Unauthorized users cannot access the image data in the database unless they have a private key to decrypt the image and retrieve the original image.

Reference

[1] S. Wadhera et al., "A Comprehensive Review on Digital Image Watermarking". Workshop on Computer Networks & Communications, May 01, 2021, Chennai, India.

[2]H. Adamu Biu, R. Husain, and A. Magaji, "An Enhanced Iris Recognition and Authentication System Using Energy Measure". Science World Journal, Vol. 13, No. 1, pp. 11-17, 2018.

[3]A. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data". Journal of Cryptography and Network Security, 2017.

[4]P. Prabhu et al., "Data Integrity of Radiology Images Over an Insecure Network Using AES Technique". Asian Pacific Journal of Cancer Prevention, Vol. 22, No.1, pp.185-193, 2021.

[5]N. Zuodong and L. Handong, "Research and analysis of threshold segmentation algorithms in image processing". Journal of Physics: Conference Series, Vol. 1237, 2019.

[6] A. Mahmoud et al., "Medical Image Segmentation Techniques, aLiterature Review, and Some Novel Trends". Menoufia J. of Electronic Engineering Research (MJEER), Vol. 27, No. 2, July 2018.

[7] M. Abd Elaziz et al., "Multilevel thresholding image segmentation based on improved volleyball premier league algorithm using whale optimization algorithm". Multimedia Tools and Applications, Vol. 80, No. 18, pp.12435–12468, 2021.

[8]N. Munirah et al., "The Development of Parameter Estimation Method for Chinese Hamster Ovary Model using Black Widow Optimization Algorithm". International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 11, No. 11, 2020.

[9] B. Verma and S. Malhotra, "Secure Image Processing Using AES Algorithm". Indian Journal of Computer Science and Engineering (IJCSE), Vol. 8 No. 3 Jun-Jul 2017.

[10]A. Arab, M. Javad, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm". The Journal of Supercomputing, Vol. 75, pp. 6663–6682, 2019.

[11] R. RIMANI et al., "An Efficient Image Encryption Using a Dynamic, Nonlinear and Secret Diffusion Scheme". Baghdad Science Journal, Vol. 18, No. 3, pp.628-639, 2021.

[12]R. Ravikumar and V. Arulmozh, "Digital Image Processing-A Quick Review". International Journal of Intelligent Computing and Technology, Vol.2, No. 2, pp.16- 24, 2019.

[13] Z. Zijiang, "Age estimation algorithm of facial images based on multi-label sorting". EURASIP Journal on Image and Video Processing, No. 114, 2018.

[14]H. Ramadan, C. Lachqar, and H. Tairi, "A survey of recent interactive image segmentation methods". Computational Visual Media Journal, Vol. 6, No. 4, pp. 355–384, December 2020.

[15]R. Chakraborty, G. Verma, and S. Namasudra, "IFODPSO-based multi-level image segmentation scheme aided with Masi entropy". Journal of Ambient Intelligence and Humanized Computing, No. 12, pp.7793–7811, 2021.

[16] A. Hemeida, R. Mansour, and M. E. Hussein, "Multilevel Thresholding for Image Segmentation Using an Improved Electromagnetism Optimization Algorithm". International Journal of Interactive Multimedia and Artificial Intelligence, Vol. 5, No. 4, 2018.

[17]H. Makkar, A. Pundir, "Image Analysis Using Improved Otsu's Thresholding Method". International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 2, No.8, pp. 2122 – 2126, 2017.

[18]A. Khairuzzaman and S. Chaudhury, "Brain MR Image Multilevel Thresholding by Using Particle Swarm Optimization, Otsu Method and Anisotropic Diffusion". International Journal of Applied Metaheuristic Computing, Vol. 10, No. 3, pp. 91-106, July-September 2019.

[19]D. Oliva et al., "Cross entropy-based thresholding for magnetic resonance brain images using Crow Search Algorithm". Expert Systems with Applications, Vol. 79, pp. 164–180, 2017.

[20]H. Kanoosh, E. Houssein, and M. Selim, "Salp Swarm Algorithm for Node Localization in Wireless Sensor Networks". Journal of Computer Networks and Communication, 2019.

[21]E. Houssein et al., "A novel Black Widow Optimization algorithm for multilevel thresholding image segmentation". International Pre-Proof Journal of Expert Systems with Applications, 2020.

[22]S. Sukpancharoen, S. Chantarachit, And U. Jantontapo, "Manufacturing and Schedule Planning Via Black Widow Optimization Algorithm". International Journal of Mechanical and

Production Engineering Research and Development (IJMPERD), Vol. 10, No. 2, pp.1409–1418, Apr 2020.

[23]I. Latif, "Time Evaluation of Different CryptographyAlgorithms Using LabVIEW". IOP Conf. Series: Materials Science and Engineering, 2020.

[24]O. Abood, M. Elsadd, and K. Guirguis, "Investigation of cryptography algorithms used for security and privacy protection in smart grid". Nineteenth International Middle East Power Systems Conference (MEPCON) - Cairo, Egypt, (2017.12.19-2017.12.21), 2017.

[25] R. Adhie et al., "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)". Journal of Physics: Conference Series, 2018.

[26]M. Abdul Wahid et al., "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA, and Blowfish for Guessing Attacks Prevention". Journal of Computer Science Applications and Information Technology, Vol. 3, No. 2, pp. 1-7, 2018.

[27]F. D'souza and D. Panchal, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach". International Conference on Computing, Communication, and Automation (ICCCA),Greater Noida, India, 5-6 May 2017.

[28] O. Abood and S. Guirguis, "A Survey on Cryptography Algorithms". International Journal of Scientific and Research Publications, Vol. 8, No. 7, July 2018.

[29]S.Umme, M. Akter, and M. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE, and PSNR—A Comparative Study". Journal of Computer and Communications, Vol. 7, pp. 8-18, 2019.

[30]O. Fatih, "Role of NPCR and UACI tests in security problems of chaos-based image encryption algorithms and possible solution proposals". International Conference on Computer Science and Engineering (UBMK) - Antalya, Turkey (2017.10.5-2017.10.8), 2017.