Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Opposition Based Joint Grey Wolf-whale Optimization Algorithm Based Attribute Based Encryption in Secure Wireless Communication

Raja M (kingraaja@gmail.com)

Department of Computer Science and Engineering, Kalaslingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India

Dhanasekaran s

Kalasalingam Academy of Research and Education

Vasudevan v

Kalasalingam Academy of Research and Education

SI: Natural and Bio-inspired Algorithms for Secure Wireless Communication

Keywords: Medical images, Cybersecurity, Image Encryption, Key generation, Attribute based Encryption

Posted Date: February 4th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-175337/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Version of Record: A version of this preprint was published at Wireless Personal Communications on March 11th, 2021. See the published version at https://doi.org/10.1007/s11277-021-08357-8.

Opposition based joint Grey Wolf-Whale Optimization Algorithm based Attribute based Encryption in Secure Wireless Communication

M.Raja[1,*], S. Dhanasekaran[2], V. Vasudevan[3]

[1]Department of Computer Science and Engineering, Kalaslingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India.

M.R: kingraaja@gmail.com

S. D: srividhans@gmail.com

V.V: vasudevan_klu@yahoo.co.on

*Corrresponding author: M.Raja, Email: kingraaja@gmail.com

Abstract

At present times, medical image security becomes a hot research topic in the healthcare sector. This paper presents an efficient lightweight image encryption model based on the Dynamic key generating Attribute based encryption (ABE) method with Opposition based joint Grey Wolf-Whale Optimization Algorithm (OjGW-WOA). The proposed encryption method undergoes certain pre-encryption steps like rotation and random column addition steps. Once the pre-encryption steps are done, ABE with OjGW-WOA is incorporated, where the optimal key is generated based on entropy value. In addition, the oppositional based learning (OBL) concept is introduced to enhance the convergence rate and searching process of GWO and WOA algorithms. Next, the proposed encryption method is designed with a dynamic key generating model that generates updated keys during every time period. Therefore, during decryption, two-level key verification is done. At the first decryption stage, the key corresponding to that particular time period is required, then the original key is generated from that key and then employed for decrypting the original data. The proposed method is simulated using MATLAB tool and a detailed comparative results analysis is carried out. The performance of the proposed work is validated with the aid of performance metrics like Peak Signal to Noise Ratio (PSNR), number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI). The experimental results stated that the presented model has resulted to a higher PSNR of 62.29dB, NPCR of 99.23%, and UACI of 23.67%.

Keywords: Medical images, Cybersecurity, Image Encryption, Key generation, Attribute based Encryption.

1. Introduction

In recent times, data transmission plays an important role in a massive number of healthcare applications. Using the telecommunication model, data is forwarded through the unprotected medium. Therefore, the data is secured using recently developed security models. According to the data transmission, data hiding is divided into 3 major classes like steganography, watermarking, and transform the timing stations [1]. Moreover, the hidden data is recorded in a cloud. The privacy-preserving model has been employed for protecting the cloud data under the application of a fuzzy duplication concept. A coverless data hiding method has been used for protecting important details. It conceals the hidden details with no change in the molecular structure image [2]. Malicious prediction, integrity, and authorization are some of the critical models in various applications. For telemedicine, clinical details are screened and Electronic Patient Records (EPR) is some of the protected transmission mechanism. In the case of transmission, there is an opportunity for attacking the clinical details by an intruder for data extension. Finally, the diagnosis mechanism is provided with a negative solution. Due to the sensitivity of clinical data, then it has to be recorded before transmitting the information. The clinical details are secured using the watermarking mechanism. Digital watermarking secures the clinical details by using data integrity, confidentiality, and authorization. In clinical image watermarking, EPR data has been incorporated inside a cover clinical image. In the case of diagnosing the disease, the forwarded medical data has to be received with no loss.

Image encryption [3] is applied extensively in armed reconnaissance and common security examination. Clinical image transmission is prone to eavesdropping intrusion as it is essential for medical image encryption prior to sending the data. Therefore, the scrambling task is carried out for security purposes, and quality is maintained for the decrypted image. Stream cipher [4] is defined as symmetric key encryption in which an encryption key has been applied for encrypting binary image and cipher image generated mathematically which is highly impossible. The major benefit of applying stream cipher is implementation is higher than block ciphers with minimum complexity of the hardware. Some of the general encryption models are accentuation on text or paired data. Hence, the customary ciphers are IDEA, AES, DES, and RSA and many other models

are improper for practical image encryption as the ciphers need the costlier processing time and maximum registering energy. Using the advantages of encryption is that, better security is provided for exclusive details and project an efficient technology for encryption and decryption on clinical images. The main aim of the Optimization Algorithm is to scramble and decrypt the image for exchanging the details among the transmitter and receiver. In this module, a self-governing mechanism has been developed for the protective inter-changing of clinical images. Finally, simulation outcome and security investigation provides the efficiency and effective encryption process.

Kanso and Ghebleh [5] suggested that a specific confusion related image encryption intends to make clinical image encryption models. Hence, the developed approach is composed of some iteration, in which iteration is composed of 2 phases namely, shuffling stage and covering stage. These phases are block related and apply chaotic cat maps for rearrangement and hide the data content. The results produced are highly supreme than traditional models which exhibit the efficiency over cryptanalytic intrusions, hence affirming the protective image communication. A clinical image encryption system is developed in [6]. It is relied on cosine value which is a mathematical tool where submission is essential for a specific operation. This principle is trained for terminating basic cryptographic intrusions.

An Image encryption mechanism using Blowfish Algorithm is introduced in [7] due to the effective and proficient implementation of data hiding mechanism and Least Significant Bit (LSB) is applied because of the efficiency and Bit management. In order to show the maximum security, a hybrid scheme is presented for blinding image encryption and hiding. PSNR and MSE have been applied for determining the image nature. An effective signcryption concept is developed in [8] interms of negativity of RSA presumption and discrete logarithm problem on conic bends across a ring Zn. The traditional method ensures a forward mystery where a sender's mystery keys are not covered and under ciphertext verification by an external component without computing decryption. It is ensured by applying mechanized cryptographic approval using ProVerif.

An extended version of Flower Pollination Algorithm (FPA) is developed in [9]. It has hybridized the remarkable FPA with Clonal Selection Algorithm (CSA) and managed to determine novel estimation using benchmark problems. The outcomes have depicted that newly projected calculation has identified accurate organizations when compared to FPA and alternate 4 principles.

A security condition of projected organization of production network management is presented in [10], where a network embeds the neutrosophic Decision Making Trial and Evaluation Laboratory (N-DEMATEL) model with a programmatic chain of importance process (AHP). The N-DEMATEL model has been employed for deducing the circumstances and ends in interrelationships between savvy security necessities. Therefore, the N-AHP has been applied for computing the weight of criteria as well as sub-criteria. At this point, the embedded structure forces developers for developing protective organization of supply chains.

The Whale Optimization Algorithm (WOA) along with a neighborhood scan system to manage the stage stream shop booking problem in [11] The Largest Rank Value (LRV) has to be determined for managing discrete pursuit space of a problem. Therefore, an assorted difference of competitor plans is maximized using a swap transformation. Moreover, half breed whale calculation (HWA) is combined with Nawaz – Enscore - Ham (NEH) for enhancing the implemented calculation. It can be pointed out that HWA offers aggressive results with recent calculations.

Attribute-based Encryption (ABE) is recommended as a tremendous candidate as it is capable to offer data confidentiality and fine-grained access control to cloud space. In recent times, the industrial enterprises are enhanced under the application of ABE. For industrial alliance, enterprises share encrypted data related to parameters. The organization with attributes meets an access policy for decrypting the encrypted data. Even though studies are performed in ABE, various problems are still unresolved. Recently developed ABE systems do not regard as secured protection in the key generation phase. Followed by, the key generation center (KGC) learns the attributes and matching keys of a user. It fails the user's privacy and data confidentiality.

This paper develops a new medical image security model using ABE with Opposition based joint Grey Wolf-Whale Optimization Algorithm (OjGW-WOA), called ABE-OjGW-WOA. The proposed method involves two major stages namely encryption and optimal key generation. Initially, the ABE encryption process takes place to encrypt the plain image. Next, the optimal key generation process gets executed where the optimal keys are chosen using OjGW-WOA. The hybridization of GWO and WOA to develop the OjGW-WOA algorithm takes place in two ways namely global and local search processes. During the global process step, the GWO algorithm is utilized together for discovering the solution communicated whereas, in the local search process,

the WOA algorithm has been utilized to intensify the local neighbors. Furthermore, oppositional based learning (OBL) concept is included to improvise the convergence rate and searching process of GWO and WOA algorithms. At the time of decryption, two-level verification process takes place to reconstruct the original images. To assure the effective performance of the proposed model, a detailed set of simulations were carried out.

The rest of the paper are organized as given here. Section 2 offers the presented model, section 3 validates the performance of the proposed method. Finally, section 4 concludes the study.

2. The Proposed Methodology

This work involves the generation of random values, which acts as a significant process in the quality of the cryptographic primitives, and it is indicated by the encryption key. Some of the security challenges relevant to the medical image processing and transmission exist, and it is needed to maintain image security. The verification of medicinal images ensures protection, safety, and security of the details saved in the information system. In the proposed image security system, the input image is partitioned into an arbitrary count of blocks which are sorted within the range. The modified image is encrypted using the ABE technique to achieve the encryption process and also considers the OjGW-WOA encryption algorithm. Once the image is encrypted and transmitted to the destination, then the resultant image is decrypted and retrieves the original image. Fig. 1 depicts the overall block diagram.

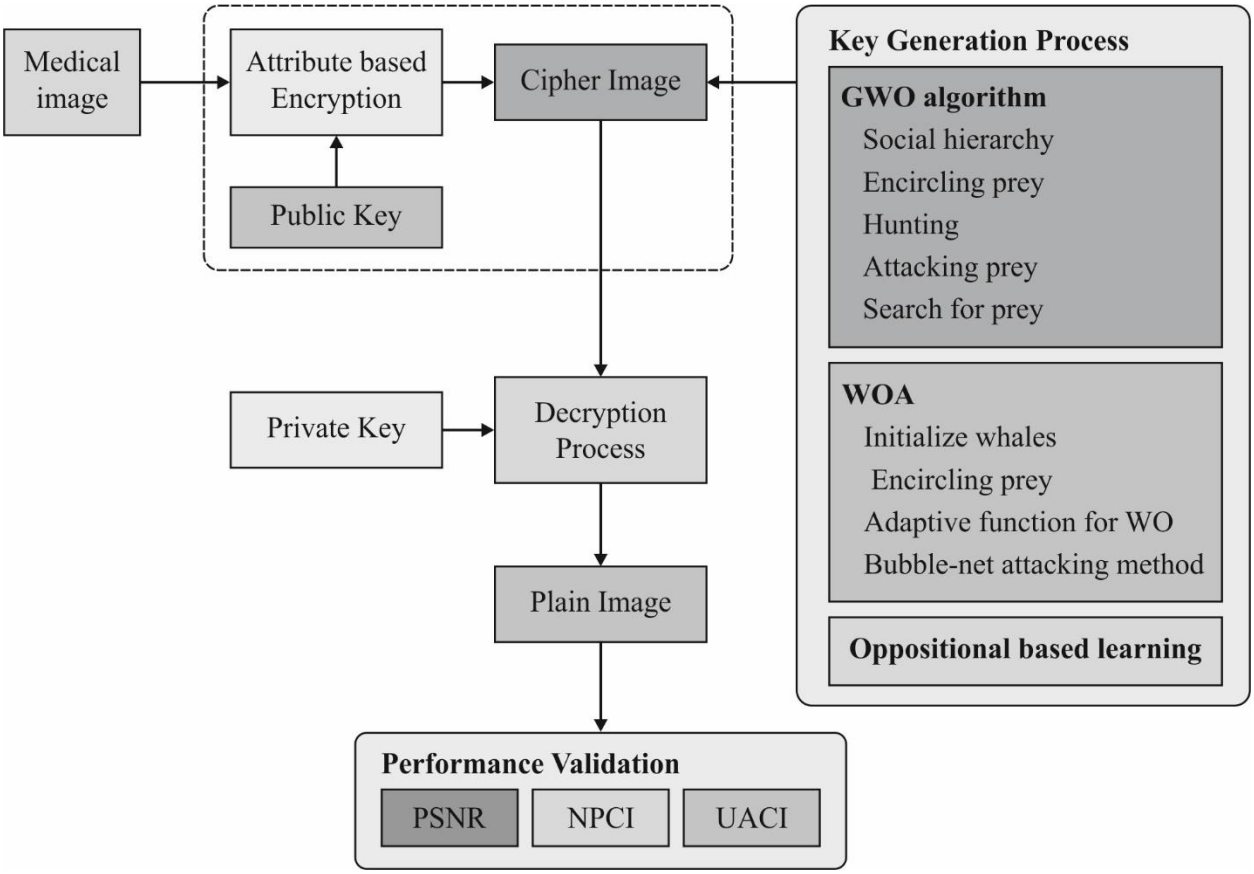


Fig. 1. Block diagram of ABE-OjGW-WOA model

2.1. Attribute based Encryption

Initially, [12] introduced a common description regarding ABE which is classified as key-policy ABE (KP-ABE) as well as cipher-text-policy ABE (CP-ABE). For the key generation phase of classical ABE, KGC learns the details of the parameters of all users. It highly affects the user's integrity. For resolving these issues, 2 functions are Attribute auditing and Key extraction. Moreover, Attribute Audit Center (AAC) in the ABE model has been established for authorizing the user's parameter for making a blind token. KGC is defined as simple technical support which plays a role for key generation; however, it does not know the associated parameters of these keys.

In the key generation phase (as depicted in Fig. 2), 3 kinds of entities have been applied namely, AAC, KGC, and data user. Here, the user provides the attributes and related evidence for the AAC. The key objective of AAC is to audit the user’s parameters and offers a blind token with AAC authentication of a user. In real-time domains, AAC has been performed to certify the user’s

attributes like government forces. Besides, a blind token is defined as evidence for users to own some parameters. These tokens do not reveal user data and ensure authentication. When a user demands obtaining the attributes key where the blind token is submitted to KGC. Once the blind key is obtained, the secret key is attained in a local fashion.

- The user displays corresponding attributes and related evidence for AAC.
- The AAC audits a user attribute and finally submits a blind token with the signature.
- While there is a requirement for accomplishing attribute keys then, it submits a blind token for KGC. A KGC is not applied for deriving user's details. It is applicable to ensure user based parameters.
- The KGC verifies the legitimacy of a token, and when a signature is illegal; else, it executes the key generation model and results in a blind key.
- A user obtains a blind key from KGC and filters a private key.

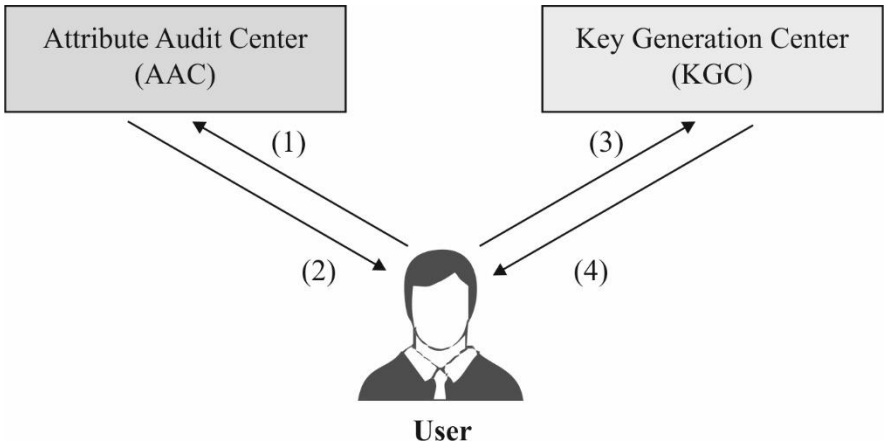


Fig. 2. Structure of ABE

2.2. Key Generation Process

During the key generation stage, the important domain parameters namely private/public keys are generated and a certificate for the public key for each client is created, in addition, consider a prime number P_N. The elements of the system are divided into a pair of fields namely prime and binary fields [13]. The proper field is considered for the cryptographic processes with maximum attention. Here, P_N defines the prime number, P_F is the prime factor, i is an integer with P_f modulo P_N in the range of $[1,..,P_{N-1}, H_f$ is the one-way hash function with the outcome of 128 bits and KH_F is the

keyed hash function, which is selected in a random way. The sender and receiver key pairs are $(AK_1, BK_1)\ and\ (AK_2, BK_2)$ where $AK_1\ and\ BK_1$ are private and public keys of the transmitter side and vice versa. For improving the secrecy of the images, the presented model makes use of OjGW-WOA to generate the optimal keys in the image security process.

2.2.1. GWO algorithm

In general, GWO is evolved from Swarm Intelligence (SI) method presented by [14]. It is an efficient model as it provides better accuracy, low computational impact, and a basic convergence model. Based on the physical as well as the social nature of the grey wolf, the numerical modeling of the GWO approach is composed of 5 parts like social hierarchy, encircling, hunting, attack, and exploring.

The GWO approach applies a hierarchical model and it is deployed according to the communal nature of grey wolves. The fitness of individuals is evaluated while 3 wolves with best fitness values which are represented as $\alpha, \beta,$ and δ. The inferior group of the grey wolf is implied as ω. The optimization of GWO is used by 3 optimal solutions. In the case of hunting, grey wolves surround the prey slowly. Hence, the numerical representation of this mechanism is illustrated as,

$$D = C \cdot I_p(l) - I(l), \tag{1}$$

$$I(l+1) = I_p(l) - A \cdot D, \tag{2}$$

$$A = 2a \cdot r_1 - a, \tag{3}$$

$$C = 2r_2, \tag{4}$$

where l implies count of iterations, A and C refers the coefficient vectors, $\cdot I_p$ denotes a position vector of a victim, $I(l)$ refers a location vector of a wolf, and $\cdot r_1$ and r_2 denotes a random vector from [0,1].

In order to stimulate the exploration nature of grey wolves, it is considered that wolves are effective in finding d supreme prey. For all iterations, robust wolves (α, β, δ) are retained while changing the position of exploring agents and it is maximized based on the position. Therefore, numerical mechanism is demonstrated as provided in the following:

$$D_\alpha = Coe_1 \cdot I_\alpha - I, D_\beta = Coe_1 \cdot I_\beta - I,$$

$$D_\delta = Coe_1 \cdot I_\delta - I, \tag{5}$$

$$I_1 = I_\alpha - Acc_1 \cdot D_\alpha, I_2 = I_\beta - Acc_2 \cdot D_\beta,$$

$$I_3 = I_\delta - Acc_3 \cdot D_\delta, \tag{6}$$

$$I(l+1) = \frac{I_1 + I_2 + I_3}{3} \tag{7}$$

where $I_\alpha, I_\beta, I_\delta$ termed as locations of α, β and δ, while I depict a place of wolves, $D_\alpha, D_\beta, D_\delta$ illustrates the distance between a present candidate and optimal 3 wolves, when $|A| > 1$, the grey wolves are scattered for searching a victim, and when $|A| < 1$, the wolves focus on victim hunting. According to the function of victim encircles, a major reduction of Acc is performed. A refers to a random vector from $[-2a, 2a]$, where a linear reduction is performed for all iterations. When Acc exists from [1, 1], afterward a location of the searching agent may be between present wolves and prey. Also, variable a is expanded linearly within $(2,0)$ as showcased below:

$$a = 2 - L \times \frac{2}{\mathrm{Max}_{Iter}} \tag{8}$$

where L refers a round and Max_{Iter} represents the measures of iterations which performs the optimization process.

Generally, the grey wolf relies upon α, β, and δ for prey identification. Firstly, it explores a victim's location and initializes for encircling a victim. In this approach, if $A > 1$, after that searching agents move away from a victim and apply GVVO to perform the global searching process. Coe is defined as an alternate search coefficient of GWO method. In surrounding victim for Coe is a random vector among $[0,2]$ which provides random weights to a victim (Coe > 1) or diminish (Coe < 1). The GWO guides in executing unsystematic searching behavior whereas the optimization task eliminates the failure of local optima.

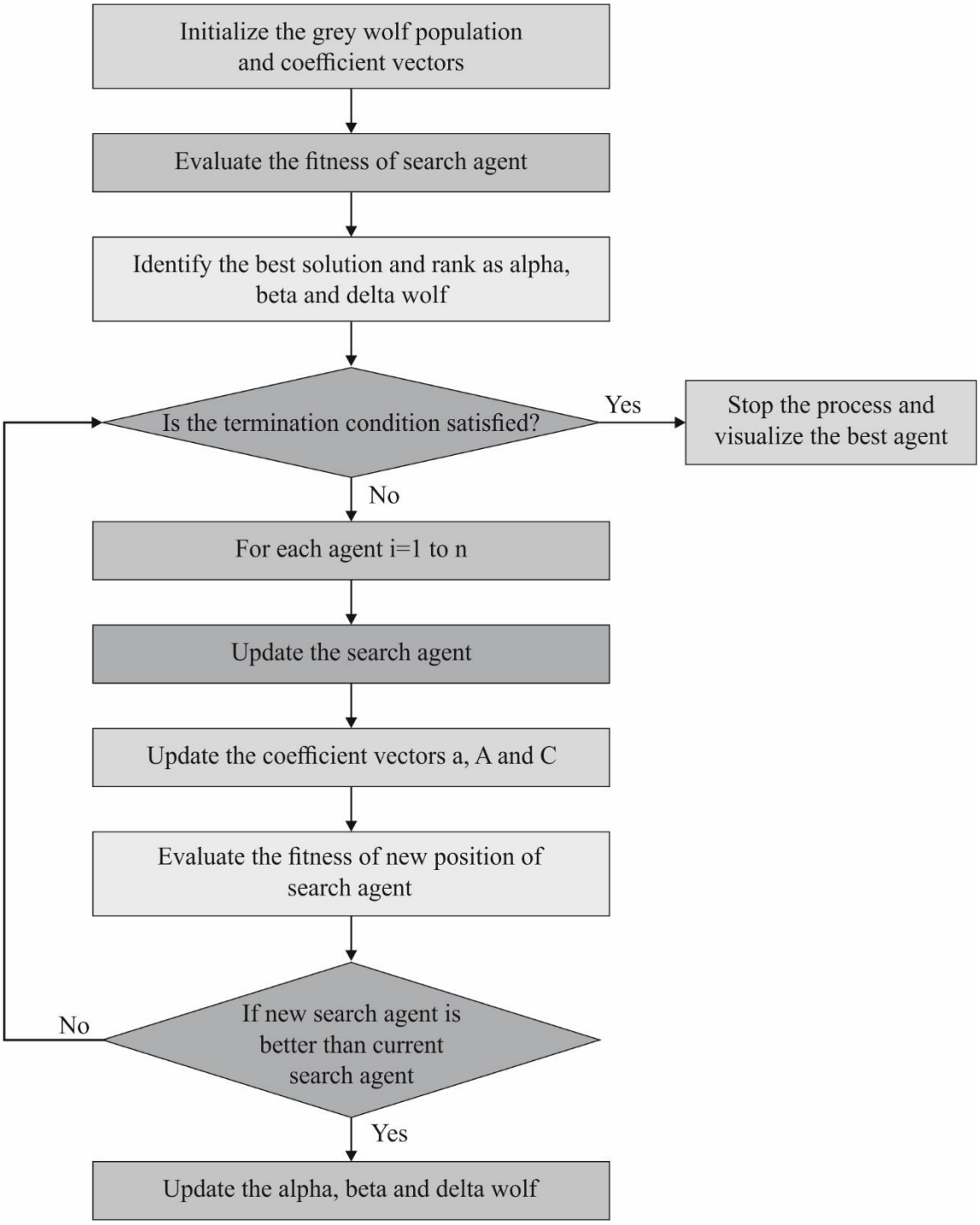


Fig. 3. Flowchart of GWO algorithm

2.2.2. Processes involved in WOA

The WO model was evolved from the whales' hierarchy. In fact, the important objective of WO is regarding the humpback whales and the individual hunting principle. The foraging nature is named

a bubble-net nourishing model. The recent and optimal candidate solution is fixed for accomplishing objective preys or optimal solutions [15]. Basically, bubble-net encouraging or chasing behavior is viewed with positive objective where humpback whale goes down in unpleasant water in the depth of 10-15 meter whereas latter some other models have a spiral shape prey encirclement and the air pockets move over the surface.

Objective Function

The key optimization model is referred to as the fitness function (FF) of PSNR with higher image supremacy. In this model is related to amplifying massive linear as well as non-linear problems. A dimension of accurate image matrix and dimensions of the decomposed image matrix should be in-differentiable. Therefore, novel key optimization mechanism refers the PSNR as defined in the following:

$$F_i = Max\ (PSNR\ ). \tag{9}$$

(i) Initialize whales (multiple keys) for MHE

In this approach, key value is considered as a random value $K_i(i = 1,2,3 \ldots n)$ where 'n' implies the overall key values. Initially, the consolidation of manual allocation is applied by various parameters for presented technologies and the coefficient vectors of the whale, for instance, Y, and S

$$K = \{K_1, K_2, \ldots . K_n\}. \tag{10}$$

Followed by, whale key solutions identify PSNR for all solutions in image blocks while getting highly significant fitness measures and the procedure is terminated; which is not applicable to accomplish better results in novel private and public key solutions with the help of underneath updating mechanism.

(ii) Encircling preys

Humpback whales perceive prey's position and surround them. In order to accomplish an ideal place in a search space, recent and optimal competitor solution is objective prey in a WO model. After gaining the optimal search agent, alternate search agents endeavor to reform the situations to effective search agent,

$$\vec{U} = |\, S.\vec{K}^*(t) - \vec{K}(t)|$$

$$\vec{K}(t+1) =. \vec{K}^*(t_{best}) - Y^*\vec{U}.$$

From the above function, $S = 2.r$ *and* $Y = 2.I.r - I$, where "I" has reduced from 2 to 0 for all iterations, a novel place of search agent is simplified in the center of the actual position of an agent and the location of the recent best agent.

(iii) Adaptive function for WO

A novel solution is identified for predicting fitness values and optimal highlights with low parameter dependence. It has not been needed for defining the primary parameter and step size for the ideal solution. Based on the functional fitness values, find a coefficient vector "y", where the versatile possibility function is received,

$$y \Rightarrow Probobility \; = \begin{cases} C_1(f_{\max} - f_x)/(f_{\max} - F_{avg}), f_x \geq F_{ovg} \\ c_3, f_x \leq f_{avg}. \end{cases}$$

Here, $f_{\min}$ *and* f_{max} refers a maximum and minimum FFs, while C_1 *and* C_3 grades among (0,1). Position towards an ideal solution modifies and is represented by functional fitness values. Thus, meta-heuristic approaches are effective when applied with an adaptive system, which results in low processing duration for accomplishing ideal results such as minimal evasion, and effective convergence.

(iv) Bubble-net attacking method

The mathematical representation denotes a bubble net behavior of humpback whales, with 2 improved models. Initially, shrinking and circling which is reduced for detecting the dimension for coefficient vectors.

Exploitation Phase

A spiral function has been applied among the location of whale and victim for referring the helix-shaped humpback whales that are exhibited as,

$$\vec{K}(t+1) = e^{bt}.\cos(2\pi.y).\vec{U}' + \vec{K}^*(t)\,. \qquad (11)$$

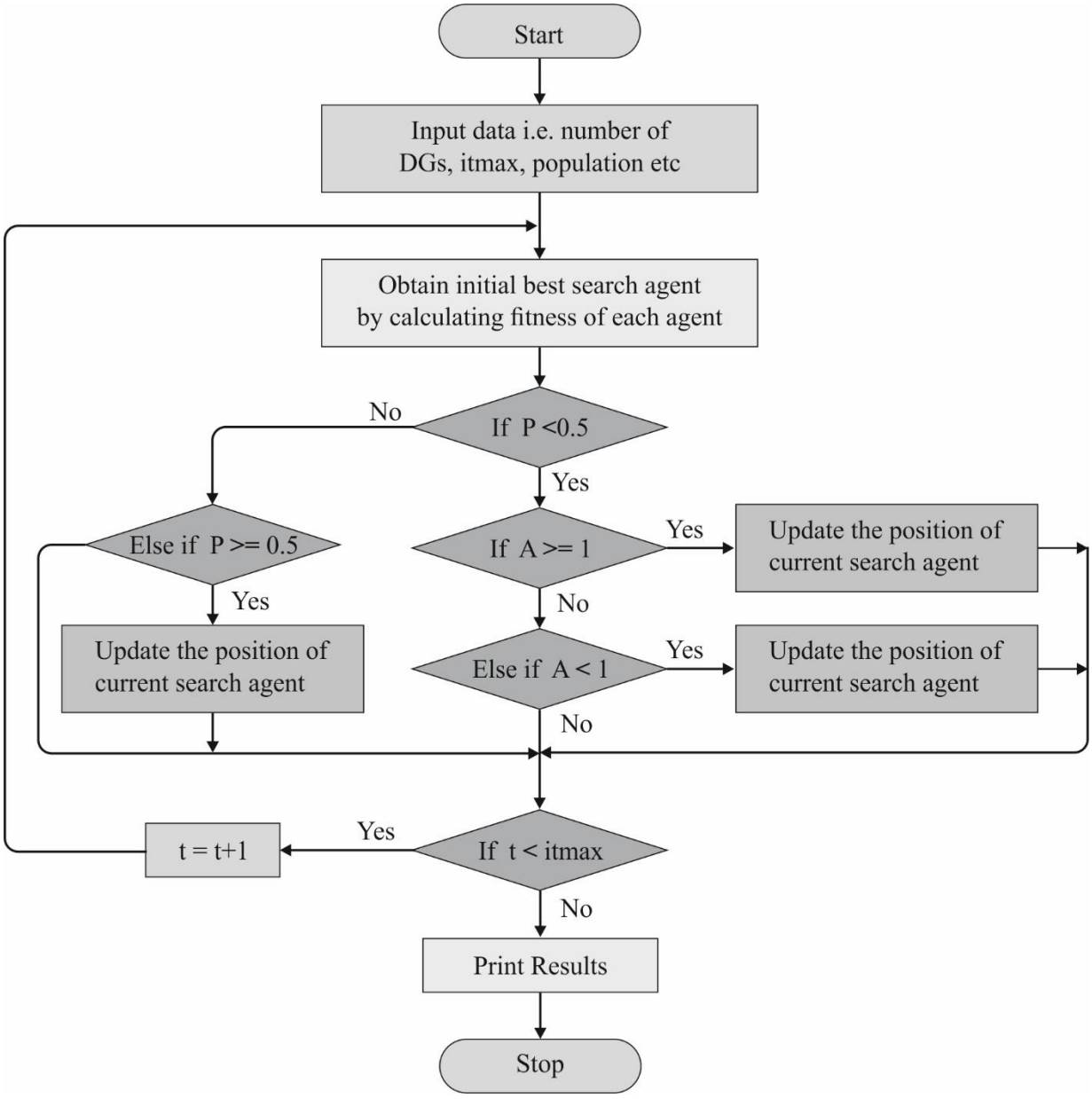


Fig. 4. Flowchart of WOA

It can be pointed out that humpback whales swim across prey within an expanding circle and winding produced for the entire process. In order to demonstrate the synchronous nature, the maximum possibility is among contracting and enclosing mechanism that refreshes the optimization process. A numerical method is depicted as given below:

$$\vec{K}(t+1) = \begin{cases} \widehat{K}(t) - y..\vec{U} & if\ p < 0.5 \\ \vec{U}'.e^{bs}.\cos(2\pi s) + \vec{K}(t) & if p \geq 0.5, \end{cases} \quad (12)$$

where y implies a random score among -1 to 1, which represents the synchronous nature that acknowledges a possibility among contracting surrounding system and twisting model for the midst of optimization.

Exploration phase

A competing model with respect to the arrangement of a vector is applied for searching for prey. Followed by, complete analyzer request for the administrator is invigorated using a randomly selected search specialist than using an optimal searching operator

$$\vec{U} = \left|\vec{s}.\overline{K}_{rond} - \vec{K}\right| \tag{13}$$

$$K(t+1) = \vec{K} - \vec{Y}.\vec{U}. \tag{14}$$

Therefore, random values are applied frequently among 1 and -1 for computing the search operation. Instead of using an exploitation phase, a search specialist is reformed in the exploration stage as represented as an aimlessly-selected search operator when compared to the best search operator as identified until now. Hence, system $|\vec{Y}| > 1$ emphasizes searching operation and enables the WO model for preceding a global optimum and $|\vec{Y}| > 1$ for examining a scenario of search agents.

(v) Termination criteria

This principle is followed until reaching a higher number of iterations. A novel set of solutions is accomplished and trailed on the basis of updating principles until the termination criteria are satisfied.

2.2.3. Oppositional based Learning (OBL) Concept

For increasing the convergence level of GWO and WOA models, oppositional based learning (OBL) mechanism is applied. The concept of OBL is applied to increase the convergence and determine the optimal global solution. Here, the present and the opposite population are concurrently created in the search space. The idea of OBL is based on the production of opposite numbers that are nearer to the global solution over the arbitrarily generated number. Also, the

opposite number and points are defined here. The opposite number is determined as a mirror point in the solution space from the intermediate point, as defined below.

$$x^0 = a + b - x \tag{15}$$

where a and b are 2 extreme points in the search region. Assume $P(x_1, x_2, \dots, x_d)$ is the point in d-dimension area, afterward, the opposite point $OP(x_1^O, x_2^O, \dots, x_d^O)$ is determined as.

$$x_i^{OP} = a_i + b_i - x_i \tag{16}$$

where $x_i \in [a_i, b_i]; i = 1,2, \dots, d$.

2.2.4. Process involved in Key Optimization of ABE using OjGW-WOA model

The different processes involved in the key optimization process of ABE using the OjGW-WOA model is discussed in the following.

Key Representation

The OjGW-WOA algorithm begins with the subjective creation of solutions in the search area. Assume D as grey wolves (random keys) structure and it comprises present position, therefore, the initial solution is defined by $S = M_1, M_2, \dots, M_D$ and all wolves speak to $M_D = C_1, C_2, \dots, C_L$. In the same way, the set of opposite solutions are created.

Opposite solution for FP

Primarily, anyone of the opposition candidate is steadily closer to the solution and then assuming the opposition is beneficial compared to the generation of extra arbitrary solutions and consider the optimal one from the available solutions. The current and the corresponding opposite solutions are simultaneous to display signs of optimal estimation of the current solution. It can be given that an opposite wolf solution offers an optimal possibility to be nearer to the overall ideal strutter of the random solution, which can be generated using the following criteria.

$$OS = O_1, O_2, \dots, O_{M_j} \tag{16}$$

where $O_{M_j} = L_j + H_j - K_j$, and the position of the jth opposite solutions O_{M_j}, depending upon the initial process of identifying the FF.

Fitness Evaluation

The process of selecting the fitness value is important in the OkGW-WOA method. In the process of encrypting medical images, the PSNR is considered as the FF for every image with optimum solutions. It can be represented as

$$F_j = \max(PSNR) \tag{17}$$

Update New Key solution for OjGW-WOA

Once the fitness value is determined, the solution gets updated by the GWO algorithm. During the hybridization of the OjGW-WOA algorithm, there are two important improvements take place containing global and local search processes. At the global process step, the GWO algorithm is applied for exploring the communicated solution. In addition, few solutions are chosen in a random way to carry out the global searching process.

$$M_i^{t+1} = \frac{M_\alpha + M_\beta + M_\delta}{3} \tag{18}$$

where $M_\alpha + M_\beta + M_\delta$ denotes the alpha (best), beta (second best), and delta (third best) wolves or solution. At the same time, the local searching process in the WOA has been utilized to intensify the local neighbors. It has been mathematically formulated as follows:

$$M_i^{t+1} = D.e^{bl}.\cos(2\pi l) + M(t) \tag{19}$$

Termination condition

The above-mentioned process will be continued until the highest PSNR of the image security procedure takes place. The algorithm gets termination when the highest counts of iterations are attained and the solution with optimal fitness value Peak Signal to Noise Ratio (PSNR) is chosen.

3. Performance Validation

The performance of the ABE-OjGW-WOA technique is simulated using MATLAB tool and the results are examined using different benchmark medical images. The evaluation parameters utilized for determining the performance are PSNR, number of changing pixel rate (NPCR) and

the unified averaged changed intensity (UACI). PSNR is a commonly employed measure to assess the image quality and it is needed to be high for better performance.

$$PSNR = 10 \log\left(\frac{255^2}{MSE}\right) \tag{20}$$

$$Mean\ Square\ Error: MSE = \sum\left(\frac{1}{Dim}(O_i - D_i)^2\right) \tag{21}$$

For testing the impact of pixel changes in the whole cipher text image, UACI and NPCR measures are employed. For any two images I_1 and I_2, the respective grayscale images $I_1(i, j)$ and $I_2(i, j)$, bipolar array B, I_1, and I_2 are found to be identical image sizes. When $I_1(i, j) = I_2(i, j)$, then $B(i, j) = 1$, else $B(i, j) = 0$. Therefore,

$$NPCR = \frac{\sum_{i,j} B(i,j)}{W \times H} \times 100\%. \tag{22}$$

where W and H define the width and height of the encrypted image, and NPCR defines he ratio of the pixel count with distinct pixel values among the two images to the total pixel value. Then, the UACI computes the mean strength of the two images and validates the medical image by altering a single pixel, as given below.

$$UACI = \frac{1}{W \times H}\left[\sum_{ij} \frac{I_1(i,j) - I_2(i,j)}{255}\right] \times 100\%. \tag{23}$$

Fig. 5 shows the different sample medical images used for the validation of the ABE-OjGW-WOA model. Fig. 6 illustrates the analysis of the qualitative results of the ABE-OjGW-WOA model under different images along with the histogram of the input image, encrypted, decrypted versions and histogram of the decrypted image. The images depicted that the ABE-OjGW-WOA model has effectively encrypted and decrypted the images with maximum security with no loss of quality.

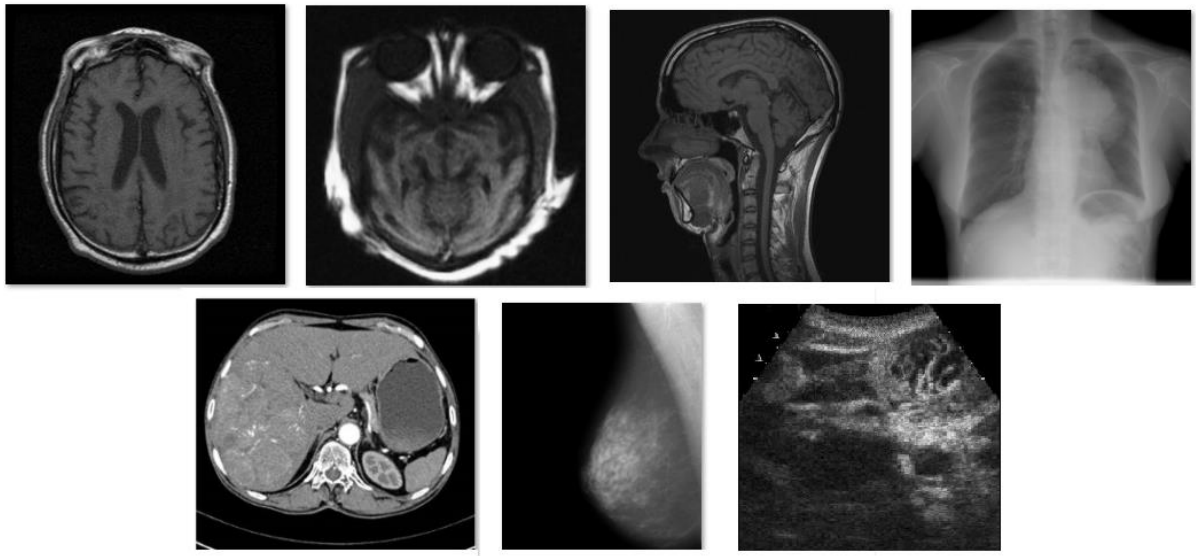


Fig. 5. Sample Images (1) Brain 1 (2) Brain 2 (3) Brain 3 (4) Lung (5) Liver (6) Mammogram (7) Mitral Valve

The PSNR analysis of the ABE-OjGW-WOA model with the existing models takes place in Table 1 and Fig. 7 under distinct medical images. On the applied image 1, the ABE-OjGW-WOA model has shown effective performance with the maximum PSNR of 57.57dB whereas the GWO, WOA, FFA, and PSO algorithms have shown ineffective outcome with the minimum PSNR of 53.42dB, 54.87dB, 54.23dB, and 48.65dB. In line with this, on the applied image 2, the ABE-OjGW-WOA method has displayed efficient function with a high PSNR of 60.48dB while the GWO, WOA, FFA, and PSO methodologies have showcased worse result with low PSNR of 56.37dB, 57.99dB, 56.9dB, and 50.34dB. Along with that, on the applied image 3, the ABE-OjGW-WOA framework has depicted remarkable performance with the higher PSNR of 59.6dB while the GWO, WOA, FFA, and PSO approaches have illustrated poor results with least PSNR of 54.89dB, 55.08dB, 54.97dB, and 48.85dB.

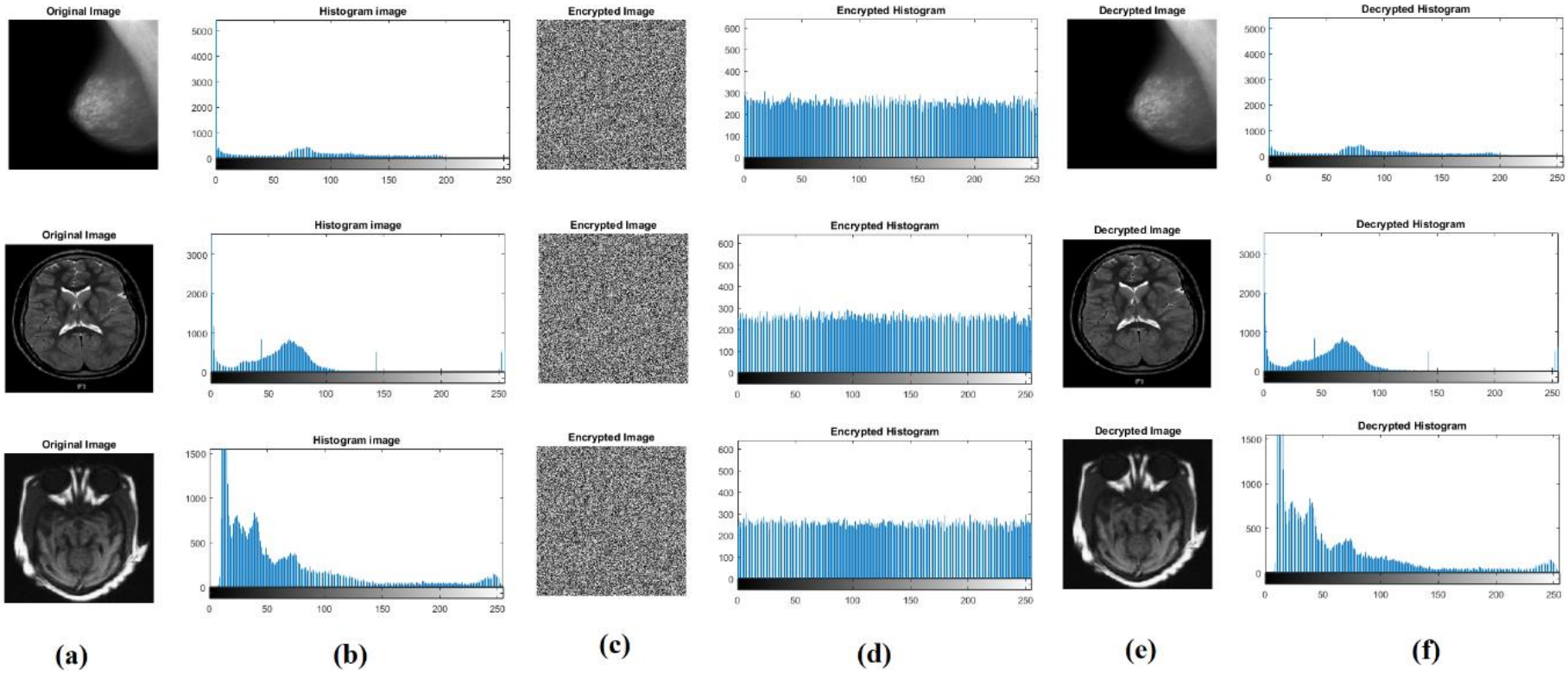
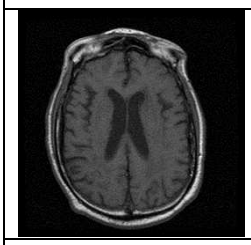
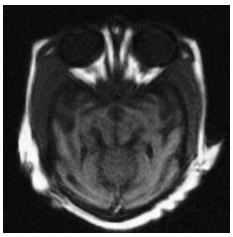
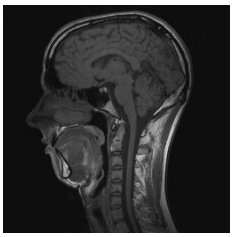
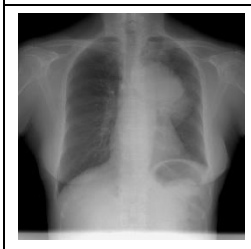
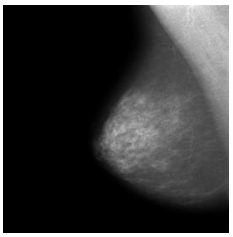


Fig. 6. Visualization of Proposed Method a) Original Image b) Histogram of Original Image c) Encrypted Image d) Decrypted Image e) Histogram of Decrypted Image

Table 1 Performance of Proposed Method with Existing Methods in terms of PSNR

No. of Images	ABE-OjGW-WOA	GWO	WOA	FFA	PSO
	57.57	53.42	54.87	54.23	48.65
	60.48	56.37	57.99	56.90	50.34
	59.60	54.89	55.08	54.97	48.85
	75.32	67.21	69.62	68.12	51.47
	64.30	58.31	61.56	60.44	52.84
	55.00	49.67	52.31	50.25	43.85

	63.77	55.98	56.87	56.16	49.71

On the other hand, on the applied image 4, the ABE-OjGW-WOA technology has defined maximum performance with the high PSNR of 75.32dB and GWO, WOA, FFA, and PSO frameworks have demonstrated insignificant outcome with minimal PSNR of 67.21dB, 69.62dB, 68.12dB and 51.47dB. Additionally, on the applied image 5, the ABE-OjGW-WOA scheme has showcased productive function with a higher PSNR of 64.3dB while the GWO, WOA, FFA, and PSO technologies have signified poor results with the lesser PSNR of 58.31dB, 61.56dB, 60.44dB, and 52.84dB.

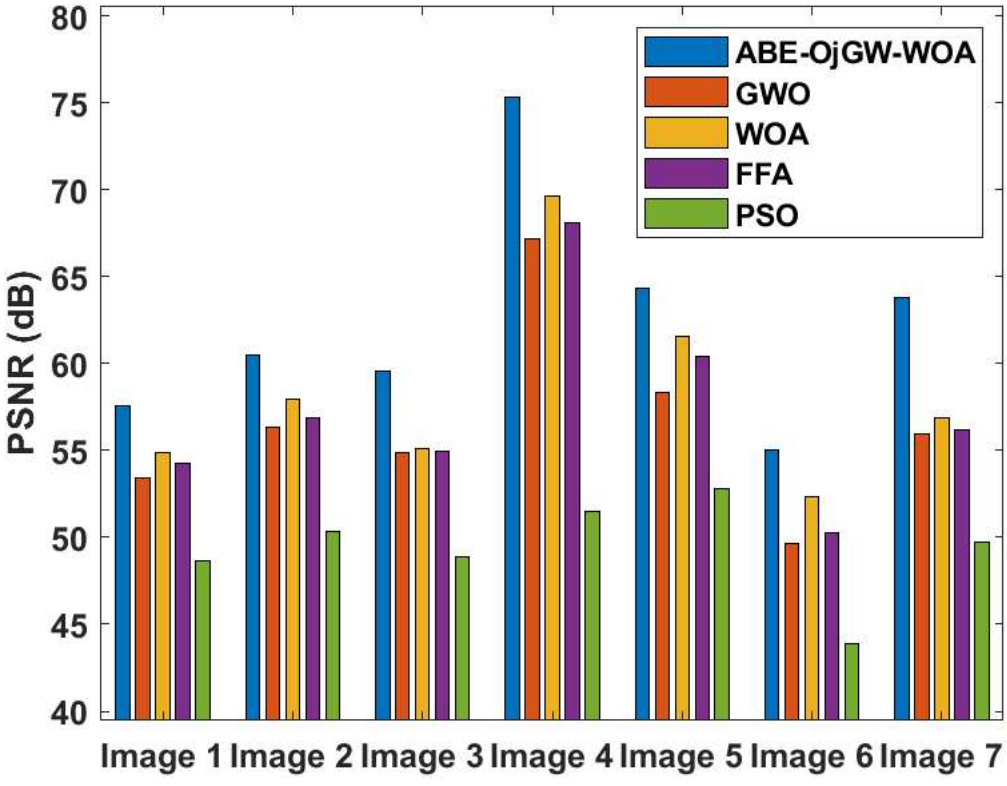


Fig. 7. PSNR analysis of ABE-OjGW-WOA model

In addition, on the applied image 6, the ABE-OjGW-WOA method has depicted maximum performance with a supreme PSNR of 55dB while the GWO, WOA, FFA, and PSO models have exhibited inefficient outcome with the lower PSNR of 49.67dB, 52.31dB, 50.25dB and 43.85dB. Moreover, on the applied image 7, the ABE-OjGW-WOA approach has represented proficient function with a high PSNR of 63.77dB while the GWO, WOA, FFA, and PSO techniques have referred worse outcome with least PSNR of 55.98dB, 56.87dB, 56.16dB, and 49.71dB.

Table 2 Performance of Proposed Method with Existing Methods in terms of NPCR (%)

No. of Images	ABE-OjGW-WOA	GWO	WOA	FFA	PSO
Image 1	99.30	96.73	96.91	96.82	94.72
Image 2	99.26	96.35	97.83	97.78	94.71
Image 3	99.19	97.32	98.13	98.08	93.89
Image 4	99.21	97.84	98.11	98.05	92.41
Image 5	99.23	96.72	97.54	97.41	92.84
Image 6	99.19	95.87	96.89	96.67	92.54
Image 7	99.26	96.22	97.32	97.17	93.56

The NPCR analysis of the ABE-OjGW-WOA method with previous approaches is depicted in Table 2 and Fig. 8 under diverse clinical images. On the applied image 1, the ABE-OjGW-WOA technology has represented maximum performance with the standard NPCR of 99.3% while the GWO, WOA, FFA, and PSO frameworks have worse results with low NPCR of 96.73%, 96.91%, 96.82%, and 94.72%. Similarly, on the applied image 2, the ABE-OjGW-WOA technology has exhibited remarkable performance with better NPCR of 99.26% while the GWO, WOA, FFA, and PSO technologies have represented poor outcome with the least NPCR of 96.35%, 97.83%, 97.78%, and 94.71%. Likewise, on the applied image 3, the ABE-OjGW-WOA scheme has showcased proficient function with the higher NPCR of 99.19% while the GWO, WOA, FFA, and PSO methodologies have depicted poor outcome with the low NPCR of 97.32%, 98.13%, 98.08%, and 93.89%. On the other hand, on the applied image 4, the ABE-OjGW-WOA scheme has illustrated standard function with supreme NPCR of 99.21% and the GWO, WOA, FFA, and PSO

technologies have depicted insignificant result with the less NPCR of 97.84%, 98.11%, 98.05%, and 92.41%.

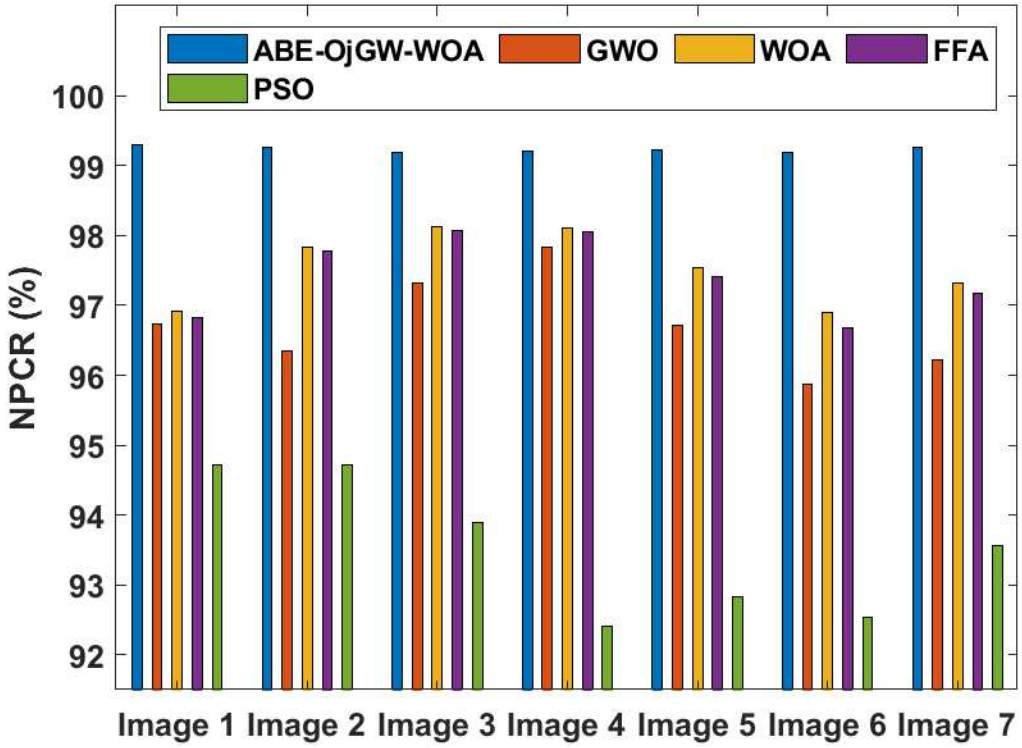


Fig. 8. NPCR analysis of ABE-OjGW-WOA model

Moreover, on the applied image 5, the ABE-OjGW-WOA scheme has represented productive function with the better NPCR of 99.23% while the GWO, WOA, FFA, and PSO frameworks have illustrated inferior results with lower NPCR of 96.72%, 97.54%, 97.41%, and 92.84%. Furthermore, on the applied image 6, the ABE-OjGW-WOA approach has exhibited productive function with remarkable NPCR of 99.19% while the GWO, WOA, FFA, and PSO technologies have exhibited poor outcome with negative NPCR of 95.87%, 96.89%, 96.67%, and 92.54%. Moreover, on applied image 7, the ABE-OjGW-WOA scheme has been referred to as proficient function with the supreme NPCR of 99.26% whereas the GWO, WOA, FFA, and PSO algorithms have implied worse outcome with the minimum NPCR of 96.22%, 97.32%, 97.17%, and 93.56%.

Table 3 Performance of Proposed Method with Existing Methods in terms of UACI (%)

No. of Images	ABE-OjGW-WOA	GWO	WOA	FFA	PSO
Image 1	25.19	23.76	23.98	23.81	22.63
Image 2	24.15	22.33	23.18	23.09	20.93
Image 3	24.44	22.74	23.10	22.98	19.53
Image 4	19.86	18.53	19.16	19.07	15.72
Image 5	22.89	21.82	22.43	22.16	18.53
Image 6	26.17	24.09	25.12	24.85	19.42
Image 7	23.04	22.08	22.95	22.78	20.45

The UACI analysis of the ABE-OjGW-WOA framework with traditional methods is illustrated in Table 3 and Fig. 9 under different clinical images. On the applied image 1, the ABE-OjGW-WOA method has showcased efficient function with higher UACI of 25.19% while the GWO, WOA, FFA, and PSO methodologies have exhibited poor results with lower UACI of 23.76%, 23.98%, 23.81%, and 22.63%. In line with this, on the applied image 2, the ABE-OjGW-WOA technique has illustrated productive function with supreme UACI of 24.15%% while the GWO, WOA, FFA, and PSO technologies have exhibited poor outcome with the lower UACI of 22.33%, 23.18%, 23.09%, and 20.93%. Similarly, on the applied image 3, the ABE-OjGW-WOA scheme has represented proficient function with better UACI of 24.44% while the GWO, WOA, FFA, and PSO methods have represented negative results with least UACI of 22.74%, 23.10%, 22.98%, and 19.53%. Followed by, on the applied image 4, the ABE-OjGW-WOA approach has represented maximum performance with the high UACI of 19.86% and the GWO, WOA, FFA, and PSO methods have referred worse results with low UACI of 18.53%, 19.16%, 19.07%, and 15.72%.

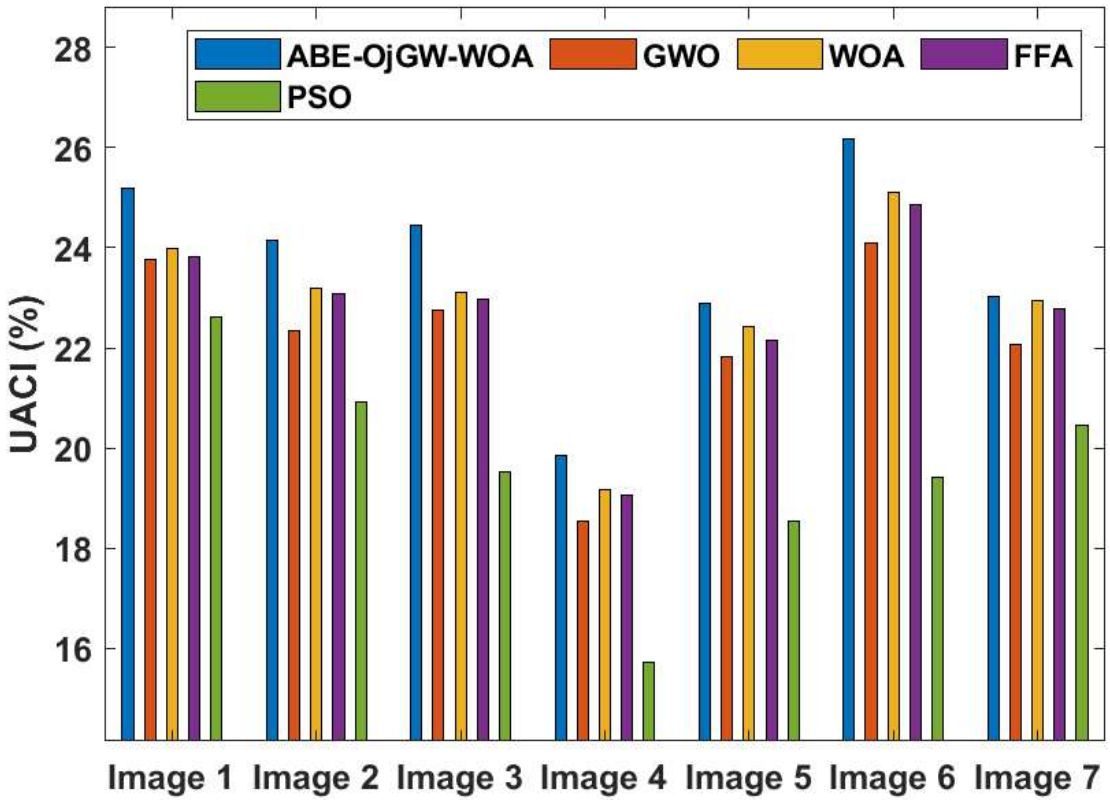


Fig. 9. UACI analysis of ABE-OjGW-WOA model

Moreover, on applied image 5, the ABE-OjGW-WOA scheme has represented a remarkable function with higher UACI of 22.89% while the GWO, WOA, FFA, and PSO approaches have depicted worse outcome with the less UACI of 21.82%, 22.43%, 22.16%, and 18.53%. Additionally, on the applied image 6, the ABE-OjGW-WOA technology has represented supreme performance with the greater UACI of 26.17% while the GWO, WOA, FFA, and PSO schemes have resulted in insignificant result with lower UACI of 24.09%, 25.12%, 24.85%, and 19.42%. Also, on the applied image 7, the ABE-OjGW-WOA technique has exhibited productive performance with the superior UACI of 23.04% while the GWO, WOA, FFA, and PSO technologies have represented imbalanced result with the least UACI of 22.08%, 22.95%, 22.78%, and 20.45%.

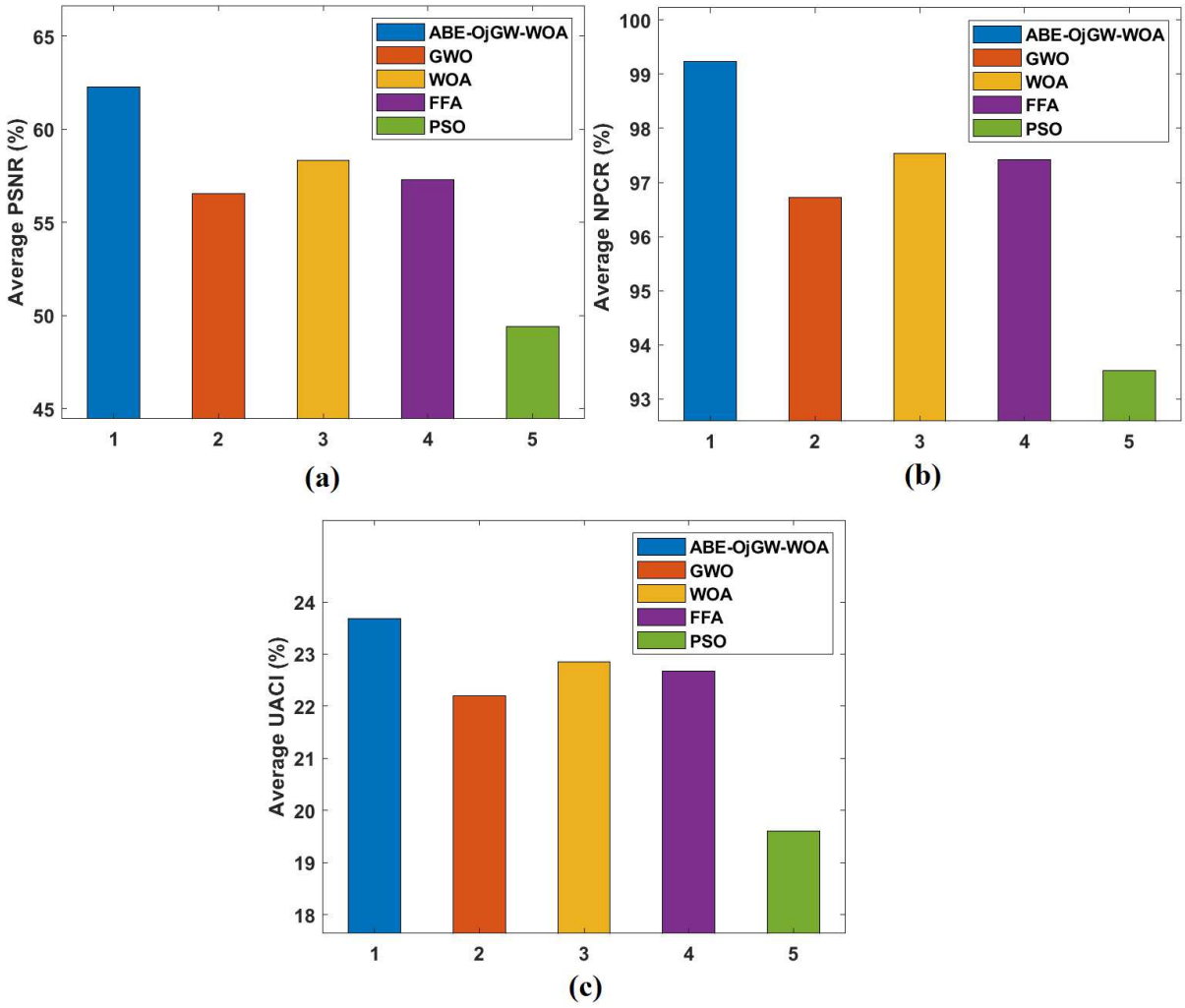


Fig. 10. Average results analysis of ABE-OjGW-WOA with compared methods

An average results analysis of the ABE-OjGW-WOA model with the existing models is carried out in Fig. 10. As depicted, the PSO algorithm has failed to show a better outcome over the existing methods. Followed by, the GWO algorithm has tried to outperform the PSO algorithm, but not higher than other algorithms. At the same time, the GWO and WOA models have depicted competitive results. But the proposed ABE-OjGW-WOA model has outperformed all the compared methods with the maximum PSNR, NPCR, and UACI.

4. Conclusion

This paper has developed a new medical image security model using ABE with OjGW-WOA. The ABE-OjGW-WOA method involves two major stages namely encryption and optimal key

generation. The presented ABE-OjGW-WOA model performs ABE, which is a lightweight encryption technique and finds useful for effective image security. Subsequently, the optimal key generation process gets executed where the optimal keys are chosen using OjGW-WOA. In addition, the OBL concept is applied to improve the convergence rate of the employed GWO and WOA algorithms. Furthermore, the hybridization of GWO and WOA in the global and local searching processes provides a way for an effective key generation process. The proposed encryption method is designed with a dynamic key generating model that generates the updated keys at every time period. An extensive experimentation process was carried out to ensure the superior performance of the ABE-OjGW-WOA model. The experimental results stated that the presented model has resulted to a higher PSNR of 62.29dB, NPCR of 99.23%, and UACI of 23.67%. In future, the performance of the ABE-OjGW-WOA model can be improved by the use of other encryption techniques and optimization algorithms.

Funding

The author(s) received no specific funding for this study.

Conflict of Interest

The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

Availability of data and material

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Code availability

Custom code

References

[1] Tan Y, Xue Y, Liang C, Zheng J, Zhang Q, Zheng J, Li Y (2018) A root privilege management scheme with revocable authorization for android devices. J Netw Comput Appl 107:69–82

[2] Cao Y, Zhou Z, Sun X, Gao C (2018) Coverless information hiding based on the molecular structure images of material. Computers, Materials and Continua 54(2):197–207

[3] Deng X, Chen Z, Zeng F, Zhang Y, Mao Y (2013) Authentication and recovery of medical diagnostic image using dual reversible digital watermarking. J Nanosci Nanotechnol 13(3):2099–2107

[4] Das S, Kundu MK (2012) Effective management of medical information through a novel blind watermarking technique. J Med Syst 36(5):3339–3351

[5] Kanso, A., and Ghebleh, M., An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation. 24:98–116, 2015.

[6] Lima, J. B., Madeiro, F., and Sales, F. J. R., Encryption of medical images based on the cosine number transform. Signal Process. Image Commun. 35:1–8, 2015.

[7] Mukhedkar, M., Powar, P., Gaikwad, P., Secure nonreal time image encryption algorithm development using cryptography & Steganography. In: India Conference (INDICON), 2015 Annual IEEE (pp. 1–6). IEEE, 2015.

[8] Daniel, R. M., Rajsingh, E. B. and Silas, S. A., Forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography. Journal of King Saud University-Computer and Information Sciences. 2018. https://doi. org/10.1016/j.jksuci.2018.02.004

[9] Nabil, E., A modified flower pollination algorithm for global optimization. Expert Syst. Appl. 57:192–203, 2016.

[10] Abdel-Basset, M., Manogaran, G. and Mohamed, M., Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. Future Generation Computer Systems. 86:614–628, 2018.

[11] Abdel-Basset, M., Manogaran, G., El-Shahat, D., and Mirjalili, S., A hybrid whale optimization algorithm based on local search strategy for the permutation flow shop scheduling problem. Futur. Gener. Comput. Syst. 85:129–145, 2018.

[12] Song, Y., Wang, H., Wei, X. and Wu, L., 2019. Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud. *Security and Communication Networks*, *2019*.

[13] Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanaprabu, S.K. and Shankar, K., 2018. Medical image security using dual encryption with oppositional based optimization algorithm. *Journal of medical systems*, *42*(11), p.208.

[14] Sivaram, M., Lydia, E.L., Pustokhina, I.V., Pustokhin, D.A., Elhoseny, M., Joshi, G.P. and Shankar, K., 2020. An optimal least square support vector machine based earnings prediction of blockchain financial products. *IEEE Access*, *8*, pp.120321-120330.

[15] Shankar, K., Lakshmanaprabu, S.K., Gupta, D., Khanna, A. and de Albuquerque, V.H.C., 2020. Adaptive optimal multi key based encryption for digital image security. *Concurrency and Computation: Practice and Experience*, *32*(4), p.e5122.

Figures

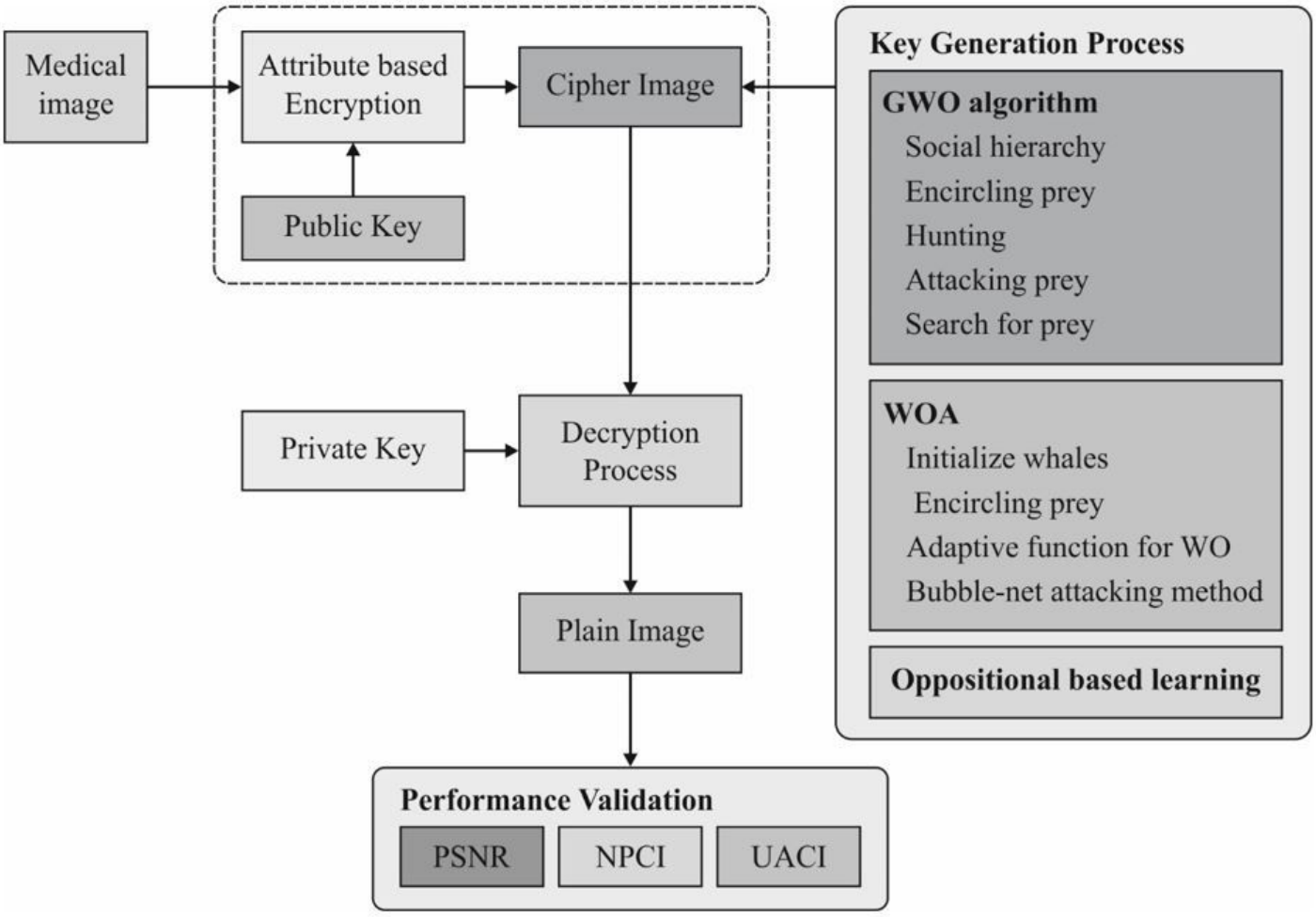


Figure 1

Block diagram of ABE-OjGW-WOA model

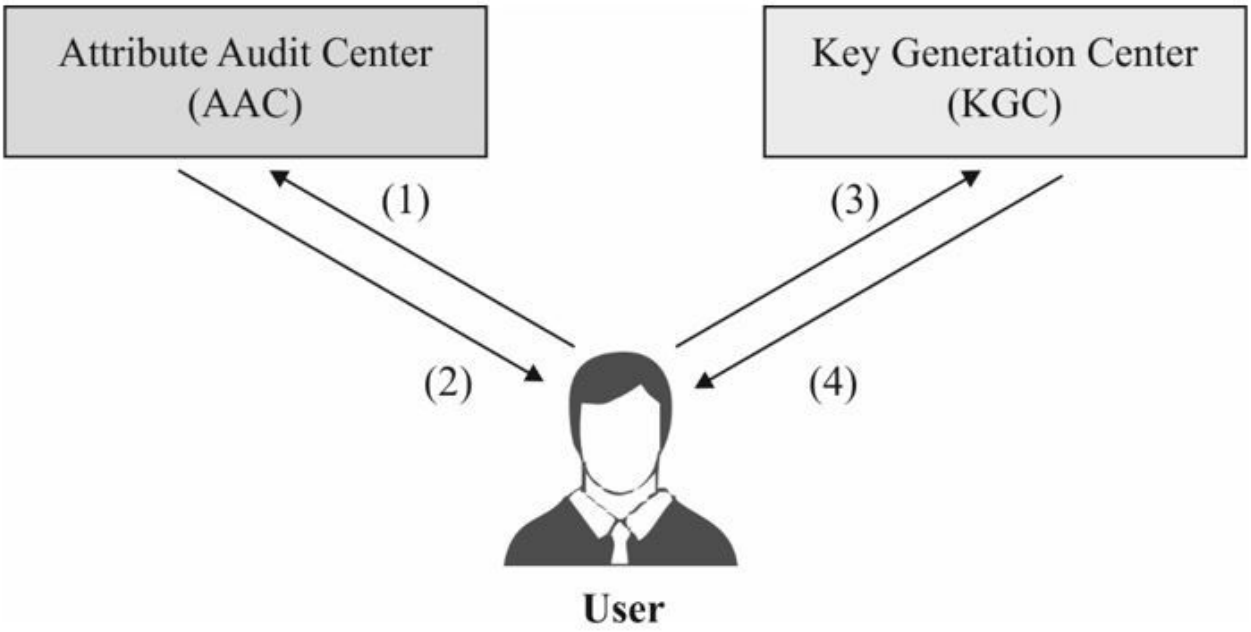


Figure 2

Structure of ABE

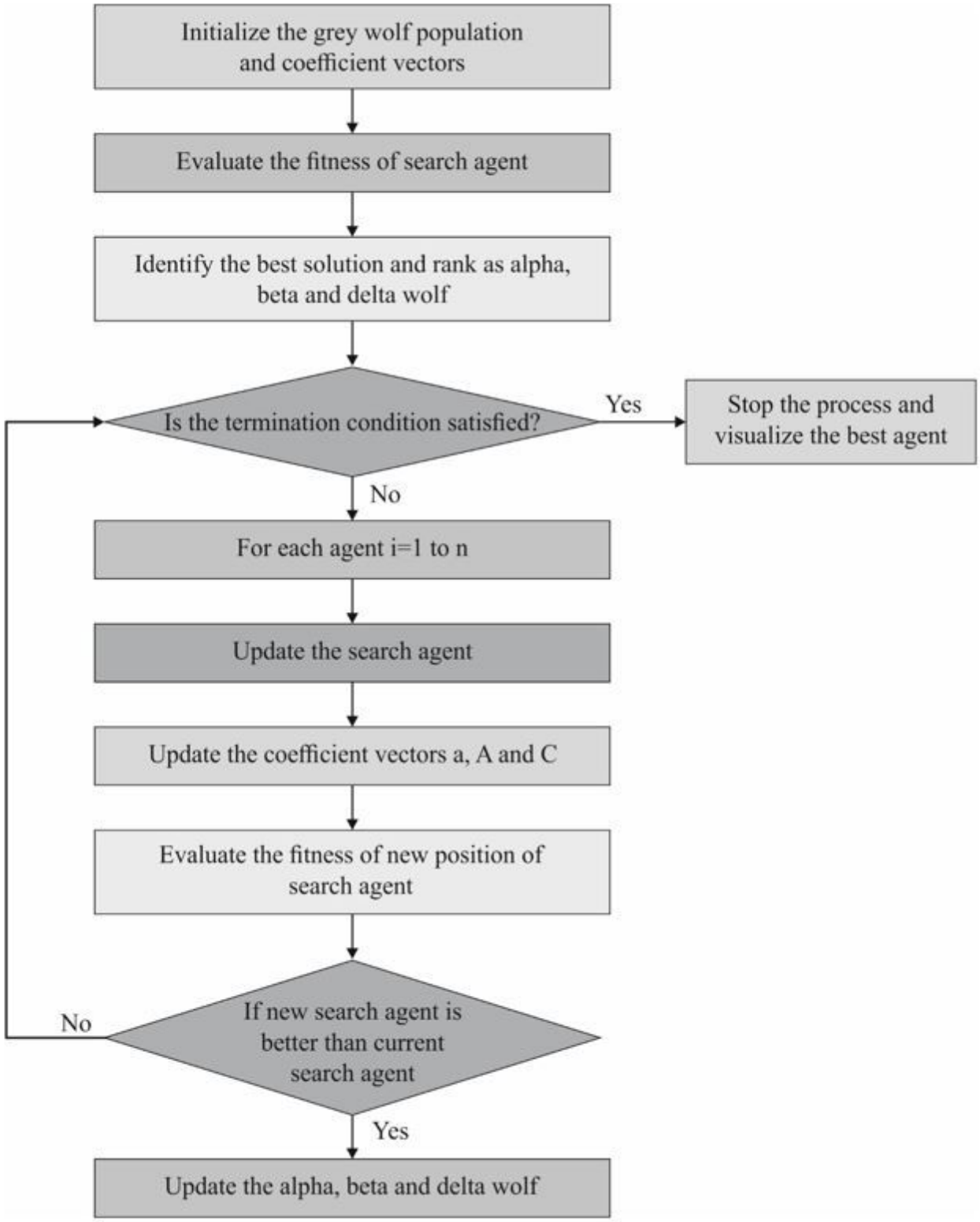


Figure 3

Flowchart of GWO algorithm

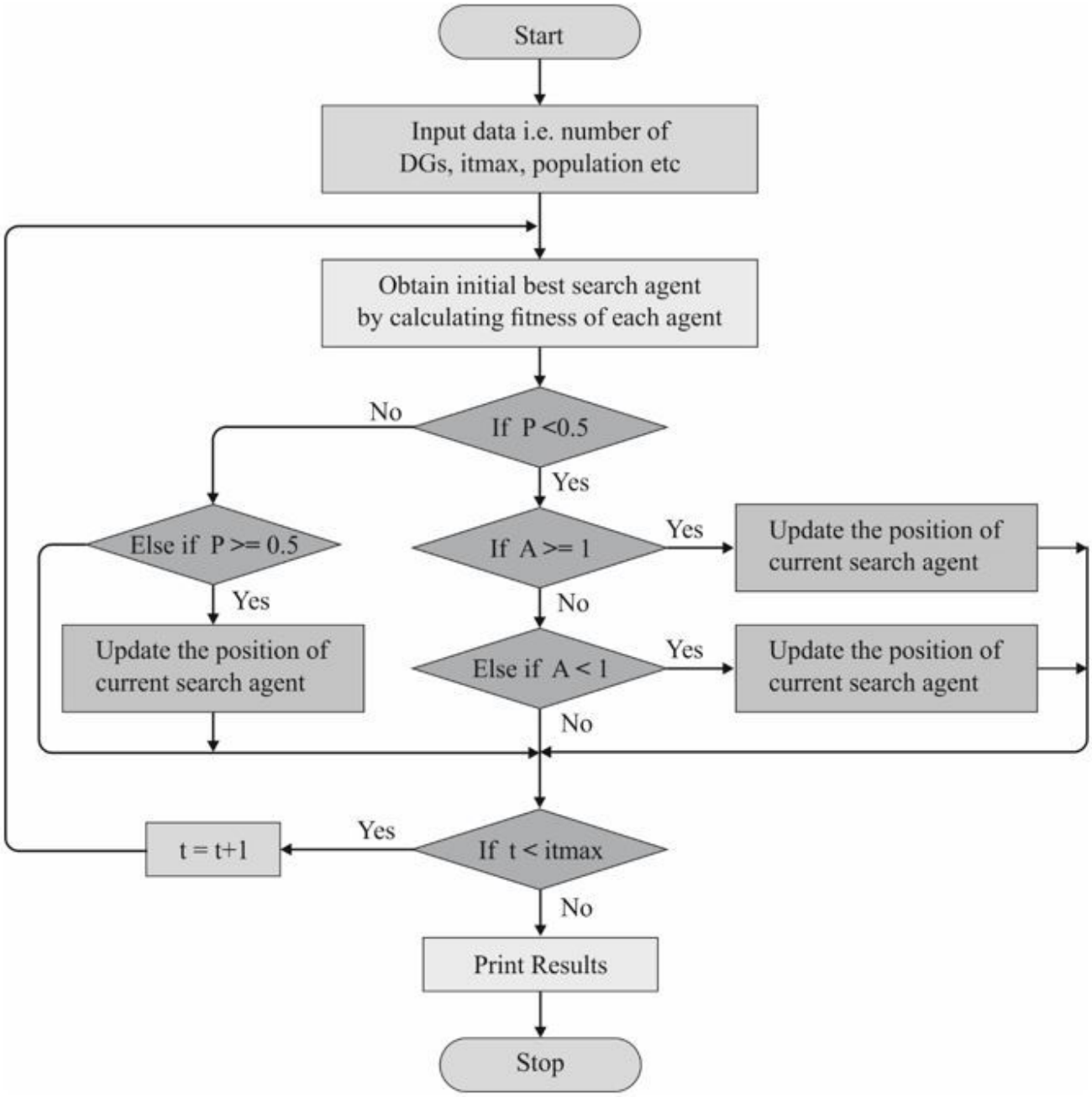


Figure 4

Flowchart of WOA

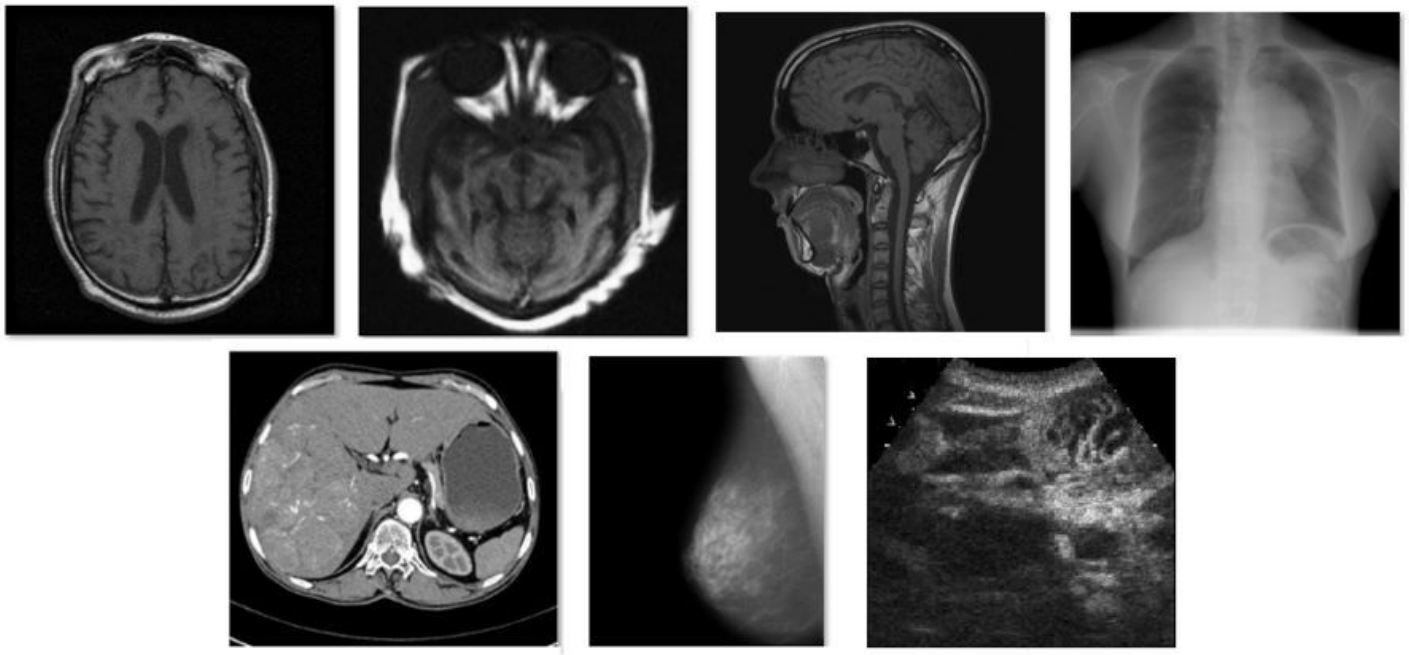


Figure 5

Sample Images (1) Brain 1 (2) Brain 2 (3) Brain 3 (4) Lung (5) Liver (6) Mammogram (7) Mitral Valve

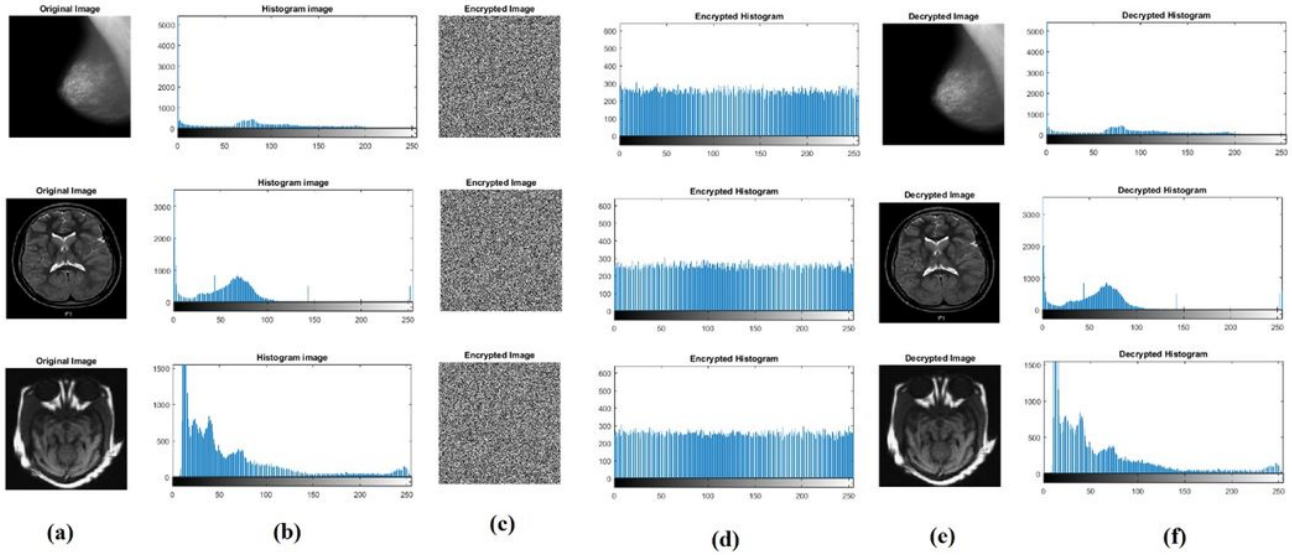


Figure 6

Visualization of Proposed Method a) Original Image b) Histogram of Original Image c) Encrypted Image d) Decrypted Image e) Histogram of Decrypted Image

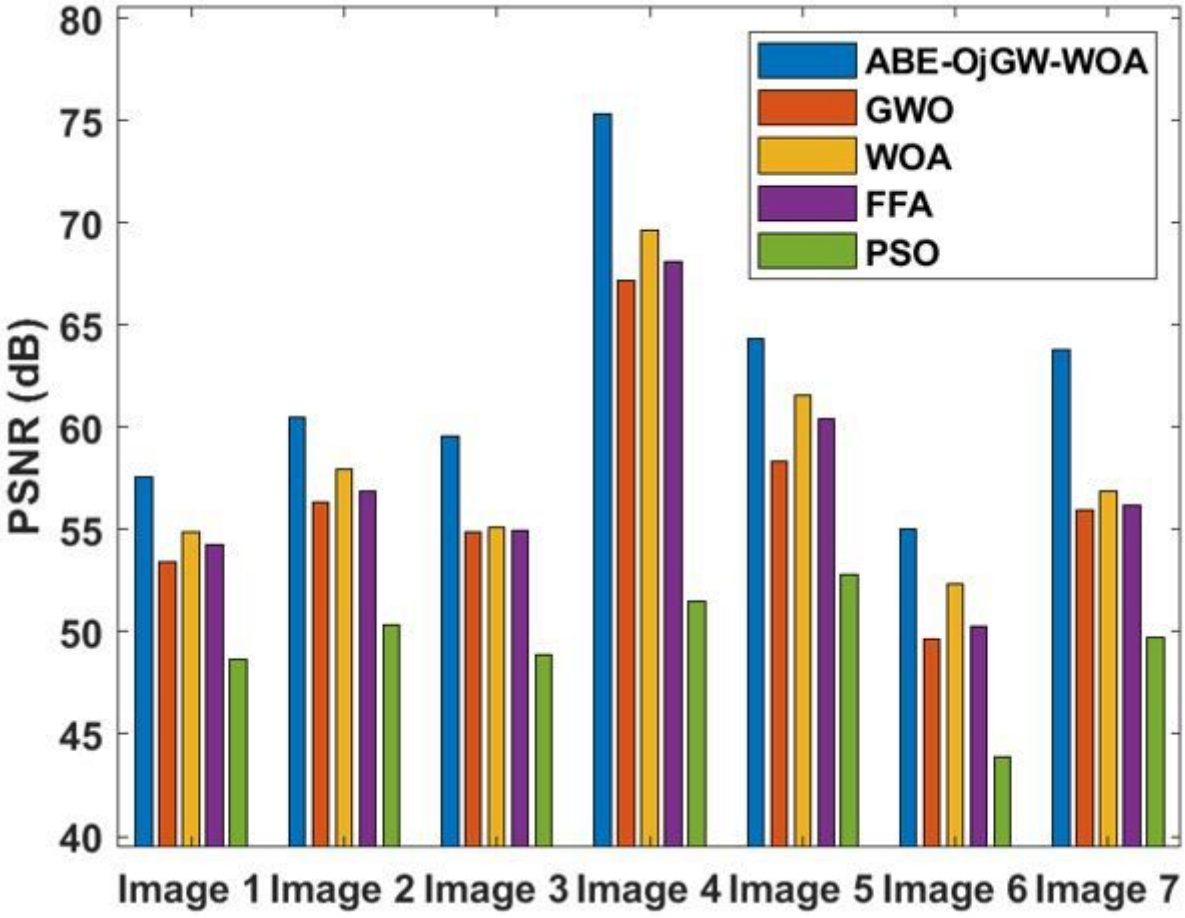


Figure 7

PSNR analysis of ABE-OjGW-WOA model

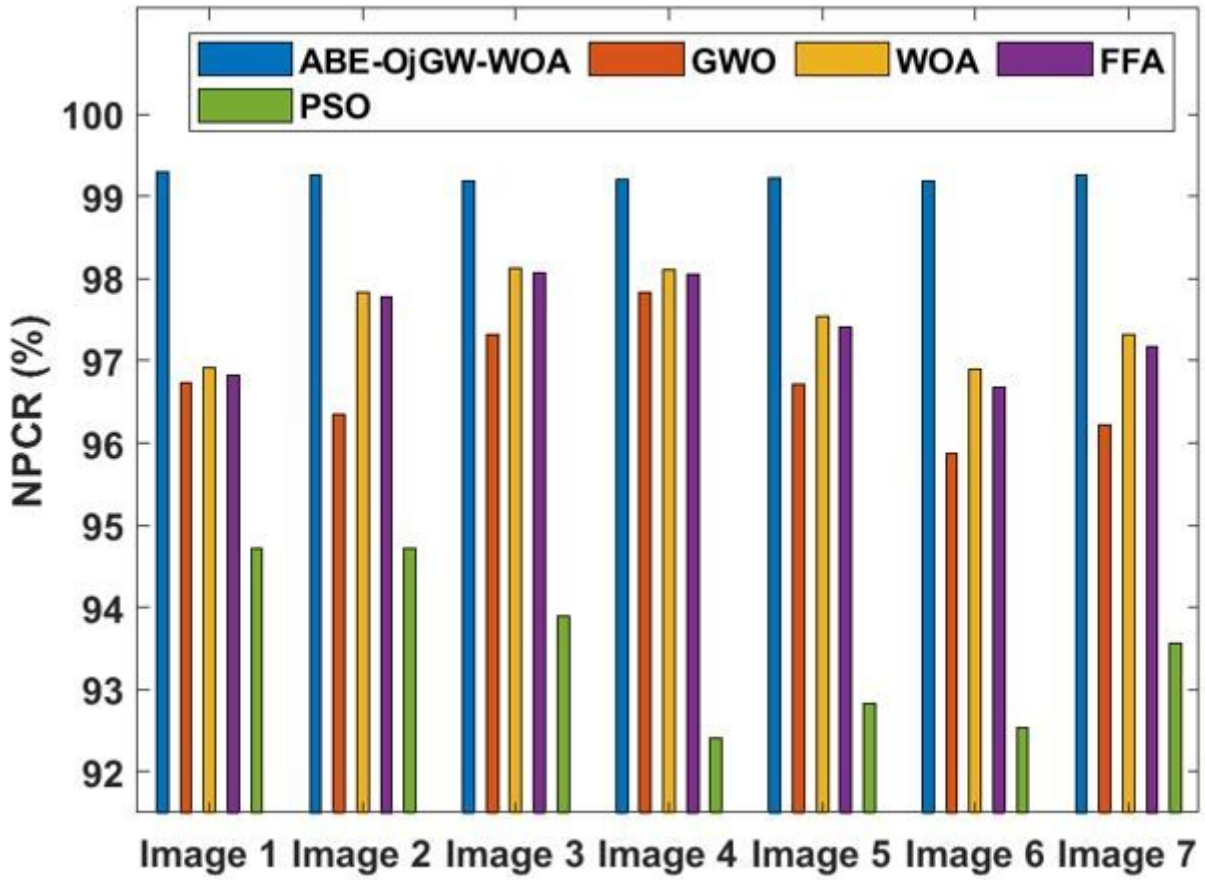


Figure 8

NPCR analysis of ABE-OjGW-WOA model

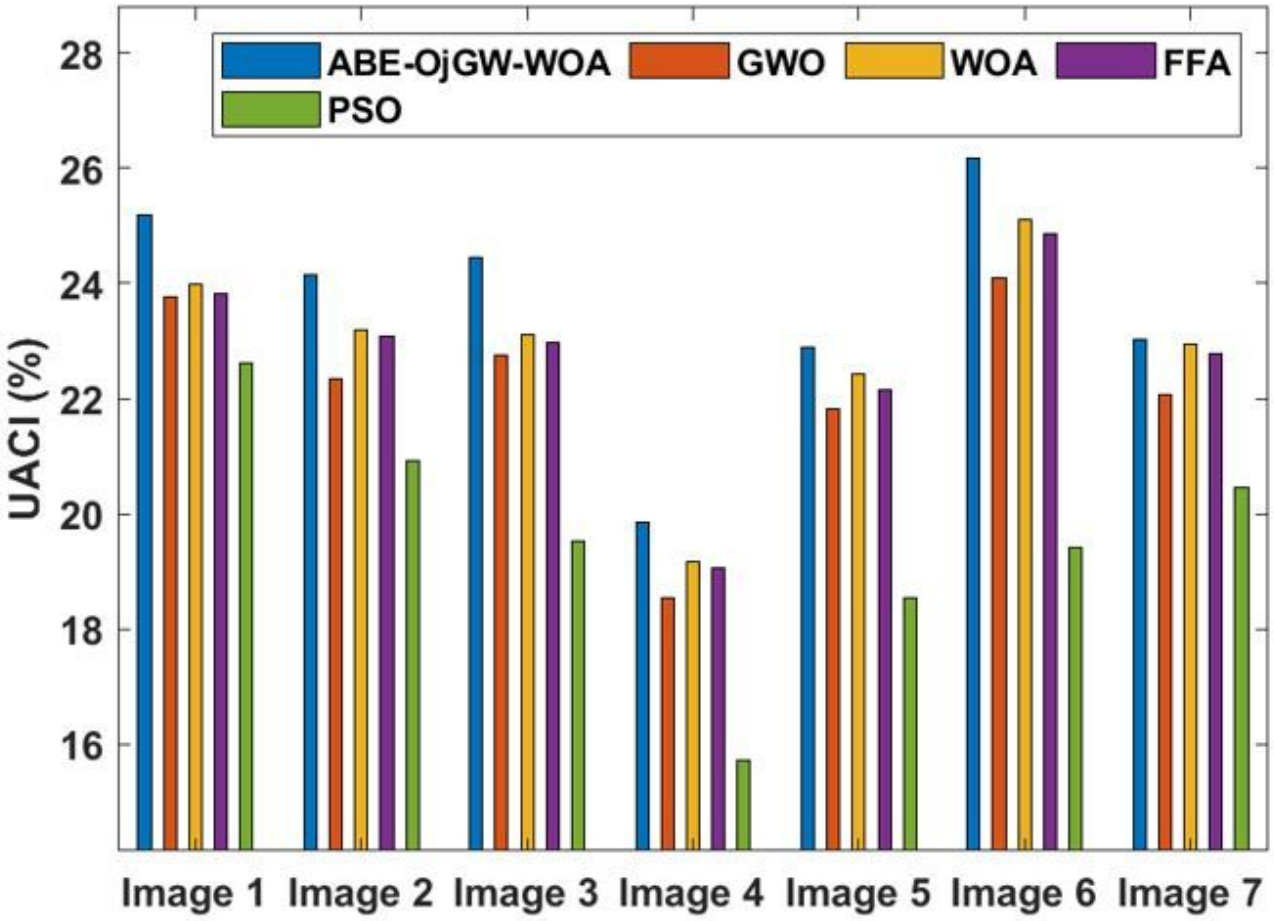


Figure 9

UACI analysis of ABE-OjGW-WOA model

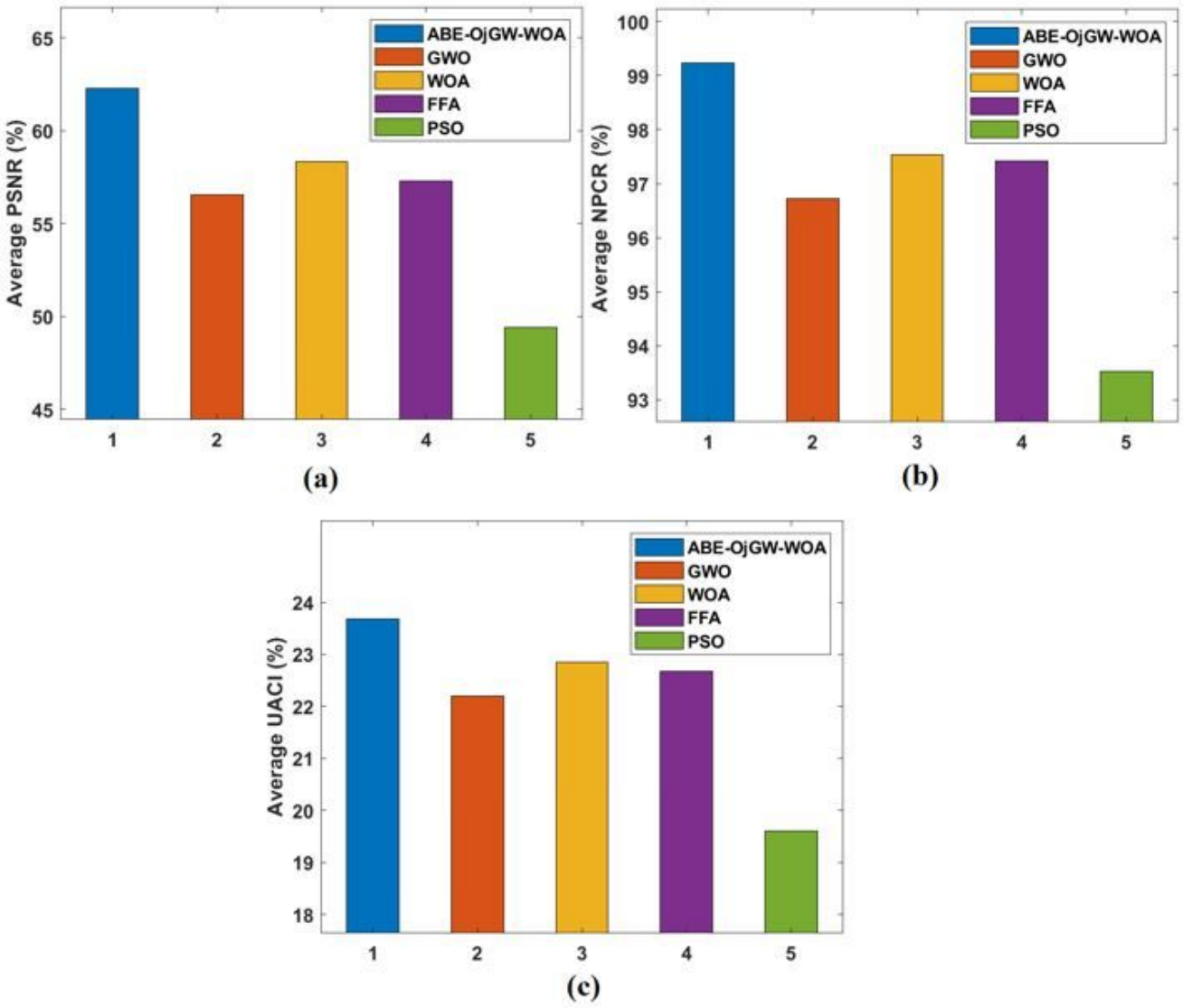


Figure 10

Average results analysis of ABE-OjGW-WOA with compared methods