scientific reports

Check for updates

OPEN

Crayfish optimization based pixel selection using block scrambling based encryption for secure cloud computing environment

Vikas K. Soman✉ & V. Natarajan

Cloud Computing (CC) is a fast emerging field that enables consumers to access network resources on-demand. However, ensuring a high level of security in CC environments remains a significant challenge. Traditional encryption algorithms are often inadequate in protecting confidential data, especially digital images, from complex cyberattacks. The increasing reliance on cloud storage and transmission of digital images has made it essential to develop strong security measures to stop unauthorized access and guarantee the integrity of sensitive information. This paper presents a novel Crayfish Optimization based Pixel Selection using Block Scrambling Based Encryption Approach (CFOPS-BSBEA) technique that offers a unique solution to improve security in cloud environments. By integrating steganography and encryption, the CFOPS-BSBEA technique provides a robust approach to secure digital images. Our key contribution lies in the development of a three-stage process that optimally selects pixels for steganography, encodes secret images using Block Scrambling Based Encryption, and embeds them in cover images. The CFOPS-BSBEA technique leverages the strengths of both steganography and encryption to provide a secure and effective approach to digital image protection. The Crayfish Optimization algorithm is used to select the most suitable pixels for steganography, ensuring that the secret image is embedded in a way that minimizes detection. The Block Scrambling Based Encryption algorithm is then used to encode the secret image, providing an additional layer of security. Experimental results show that the CFOPS-BSBEA technique outperforms existing models in terms of security performance. The proposed approach has significant implications for the secure storage and transmission of digital images in cloud environments, and its originality and novelty make it an attractive contribution to the field. Furthermore, the CFOPS-BSBEA technique has the potential to inspire further research in secure cloud computing environments, making the way for the development of more robust and efficient security measures.

Keywords Pixel selection, Cloud Computing, Crayfish optimization, Steganography, Image encryption, Salp swarm algorithm

Cloud storage is a main part of a cloud computing (CC) method that is used to save information and useful data over the internet[1]. The Cloud providers offer users using cloud storage service at a very low cost as per the need and efficiently manage data storage structure. With the quick growth of cloud storage technology, enterprises, single users, and governments progressively retain data in the cloud[2]. Though CC delivers a huge number of services such as the act of outsourcing user data safety to avoid unauthorized consumers, the costs of source maintenance, the confidentiality of sensitive information, and computational difficulty are the main complications. With the fast growth of information technology (IT), the security of multi-media data like audio, video, and image has attracted extensive consideration[3]. Safe and effective encryption of image information is the main focus of many multi-media research. Images are the most used method of multi-media objects for a wide range of applications. In a cloud platform, image security is a major problem to be mentioned[4]. Images are encoded both in transform and spatial domains based on different parameters and requirements to increase privacy. Owing to the correlation dependence of image pixels, conventional cryptographic methods are not suitable for ciphering the images[5]. Owing to the small entropy of digital images, including strong pixel correlation and high redundancy, traditional encryption techniques usually could not efficiently encrypt the

Department of Instrumentation Engineering, Madras Institute of Technology Campus, Anna University, Chromepet, Chennai 44, India. ✉email: vikassoman@gmail.com

image data. The novel cryptographic algorithm based on a chaotic system has become one of the best image encryption solutions[6].

Cryptography is a method, which includes the research of safe communication methods to prevent unauthorized persons from retrieving confidential data, messages, or information. The method includes several characteristics in the information security sector, namely data confidentiality, integrity, authentication (CIA), and non-repudiation, which is the main area in current cryptography[7]. Encryption in CC is a significant problem that requires investigation in several studies. Because CC manages critical data and is available worldwide over the internet, security is a serious issue and major concern. Cryptography techniques play an important part in protecting digital media privacy, data transmission, e-commerce, web data storage, and transmission[8]. Some procedures are suitable for decryption and encryption to confirm data safety in CC including Data Encryption Standard (DES), Identity-Based Encryption (IBE), Advanced Encryption Standard (AES), and Rivest Shamir Adleman Algorithm (RSA). Many researchers utilize cryptography methods for protecting the cloud privacy of the data, but the main drawback of encryption is that the data is encrypted and turned unreadable, still occurring as private data[9]. If the hacker has enough time, he/she can decrypt the private data. Steganography is a method to resolve this problem because it will permit the users to disappear the data into other objectives like images, text, audio, and video[10]. These methods will upsurge the security of confidential data.

In the field of cloud computing, securing sensitive data, particularly digital images, is increasingly critical. Traditional cryptographic and steganographic methods often fall short in providing comprehensive security, necessitating advanced approaches like the Crayfish Optimization-based Pixel Selection with Block Scrambling Based Encryption Approach (CFOPS-BSBEA). Traditional cryptographic techniques, such as AES, are effective for encrypting data, but when combined with basic steganographic methods, they can still be vulnerable to sophisticated attacks. For example, simple steganographic methods that hide data in the least significant bits (LSBs) of pixels can be detected by advanced forensic tools. This limitation is evident in scenarios such as secure medical image transmission, where maintaining data confidentiality and integrity is crucial. Basic steganography fails to protect high-resolution images effectively against detection and extraction attempts. Moreover, many conventional stego-crypto methods do not optimize pixel selection for embedding secret data, leading to predictable patterns that can be exploited by attackers. For instance, in the secure transmission of satellite imagery, using fixed pixel locations or predictable encryption keys can increase the risk of unauthorized access. The lack of optimization and randomness in these methods makes them less effective in high-security environments. The CFOPS-BSBEA approach addresses these issues by incorporating Crayfish Optimization to dynamically select pixels for embedding secret data, thus enhancing security through optimized pixel selection. This is particularly beneficial in secure military communications, where the ability to prevent unauthorized detection of hidden information is crucial. Additionally, the approach utilizes block scrambling encryption, which adds a layer of complexity that traditional methods lack. This technique disrupts predictable patterns, significantly improving security. For example, in the secure transfer of financial documents, block scrambling makes it much harder for unauthorized parties to uncover hidden data. Overall, the CFOPS-BSBEA approach offers a robust solution to the limitations of traditional methods, providing a higher level of security in cloud computing environments.

This study develops a new Crayfish Optimization based Pixel Selection with Block Scrambling Based Encryption Approach (CFOPS-BSBEA) technique for Secure CC Environment. In the CFOPS-BSBEA technique, a three-stage process is involved. Firstly, the CFOPS-BSBEA technique involves the design of a CFO algorithm for optimally selecting the pixels for the steganography process. Next, the CFOPS-BSBEA technique applies the BSBE technique to encrypt the secret images that are embedded in the selected pixels of the coverd image. The keys involved in the BSBE process can be selected by the use of the Salp swarm algorithm (SSA). At last Finally, the CFOPS-BSBEA technique undergoes the embedding and extraction process. The experimental results highlighted that the CFOPS-BSBEA technique reaches better security performance than other models.

Related works

In[11], a new hybrid technique, CNN-DCT Steganography unites the influence of CNN and the discrete cosine transform (DCT) technique has been developed. The projected model exploits the strong feature extractor abilities of CNN and the spatial frequency field alteration of DCT for attaining unnoticeable embedding and improved data-hiding ability. The cover image experiences a dual-stage procedure. Initially, feature extraction utilizing a deep CNN that allows many suitable areas for data embedding. Then, the nominated areas are exposed to the DCT-based steganography model. Bahaddad et al.[12] concentrated on the project of Bald Eagle Search Optimum Pixel Selection with Chaotic Encryption based on the image steganography model. The projected Chaotic Encryption (BESOPS-CE) method efficiently covers the secret imagery in its encoded form for covering an image. To attain it, the BESOPS-CE model uses a BES for the OPS process. Also, c Chaotic encryption has also been implemented for encoding the image of secret, then it is fixed to select the pixel point of the hidden imagery. Lastly, embedding and extraction procedures have been implemented. Sharath et al.[13] proposed an optimum meta-heuristics-based PS with a homomorphic encryption model for the video steganography (OMPS-HEVS) method. The projected OMPS-HEVS system at first achieves a frame conversion procedure and relates a 2D-DWT procedure. Also, the OPS procedure utilizes the glowworm swarm optimizer (GSO) model.

Guo et al.[14] projected an Adaptable Image Steganography Method (AISM). At first, AISM modifies correct down-sampling models, ratios, and up-sampling ratios for secret images depending upon the desires, tracked by the image sample procedure. By following this, an embedding technique based on pixel-value coding is planned, which plans pixel values and then substitutes the higher-frequency sub-band coefficient of the up-sampling image. In the embedding procedure, no auxiliary data is produced, which is a key feature for user-friendliness. Ren et al.[15] presented a visual refuge image encryption structure united with compacted detecting and LSB embedding in the cloud atmosphere. Initially, the Arnold technique was employed to challenge the sparse

plain-text imagery on the local consumer, and compacted sensing was employed for compressing it to get the secret imagery. Upload the cipher-text image and implement encryption in the cloud. The security of visuals is certified by inserting cipher text into carrier imageries to get significant steganographic imageries. In[16], the developed model has concentrated on executing the least significant bit (LSB) identical steganography method. For certifying better safety, the advanced encryption standard (AES) system has been employed before using the steganography method to certify the dual-layer safety of the private message. In this study, another feature has been employed and uses mosaic imageries as the cover media.

The Crayfish Optimization-based Pixel Selection with Block Scrambling Based Encryption Approach (CFOPS-BSBEA) represents a significant advancement in image security, particularly in the context of cloud computing. Traditional stego-crypto methods often face limitations in balancing capacity and secrecy. For example, researches in[23,24] highlights how conventional methods can struggle with achieving both high data capacity and robust security. CFOPS-BSBEA overcomes these challenges by employing Crayfish Optimization to enhance pixel selection, which optimizes the embedding process and improves security without compromising the capacity to hide data. This approach is further supported by findings in[25] demonstrate that advanced techniques can significantly enhance security and performance. Additionally, CFOPS-BSBEA addresses the limitations of traditional methods highlighted in studies like paper in[26] by introducing a complex encryption process that makes unauthorized detection more difficult. Overall, CFOPS-BSBEA builds on existing research to provide a sophisticated solution that achieves superior security and efficiency in image data protection.

Kanjanamek et al.[17] presented a cloud-based steganography method that provides imperceptibility protection and adaptive matching among files, text, or ciphertext within nominated cover imageries at random. To conclude, this method projected a method to calculate the optimum cover image for dissimilar cipher-text dimensions based on the enhanced calculation of the LSB and file ratio. Also, the model suggests a graph-based method to physically perfect the correlation among consumers, ciphertext, and image files. Alomoush et al.[18] developed an unseen watermarking model for data embedding into the transformation field for the grey scale imageries. Likewise, a stego-text is inserted with dissimilar dimensions within imageries after implanting the stego-image immune to dissimilar types of attacks like cropping, rotation, JPEG compression, and salt and pepper with diverse standards.

Our proposed CFOPS-BSBEA technique, which combines steganography and encryption, shares similarities with other studies that have explored the integration of cryptography and steganography to enhance security in various applications. For instance, the study[27] demonstrates the effectiveness of combining elliptic curve cryptography with image steganography to secure medical data. Similarly, the study[28] proposes a 3-layer security approach that incorporates cryptography and steganography to protect medical records. Another study[29], also explores the combination of elliptic curve cryptography and image steganography to secure medical data.

In our study, we have designed a novel CFOPS-BSBEA method that incorporates steganography and encryption to improve security in cloud computing environments. The CFOPS-BSBEA technique involves a three-stage procedure, which includes pixel selection using the Crayfish Optimization (CFO) algorithm, encoding secret images using Block Scrambling Based Encryption, and embedding them in cover images. The CFO algorithm is a new swarm intelligence based optimizer algorithm inspired by the behavior of crayfish, which is used to optimally select pixels for the steganography process. Our approach offers a unique solution to improve security in cloud environments, and its originality and novelty make it an attractive contribution to the field. While the referenced studies by[30–32] focus on improving encryption confidentiality through various means of randomness and resilience, the CFOPS-BSBEA method offers a more integrated approach. By combining Crayfish Optimization with Block Scrambling Based Encryption, CFOPS-BSBEA provides a holistic solution that enhances both the randomness and structural security of image encryption. This multifaceted approach makes it a robust option for high-resilience applications in cloud computing environments. For instance, the study by Alghamdi et al. (2022) explores securing matrix counting-based secret-sharing through crypto steganography, highlighting how these techniques can bolster data protection against unauthorized access[33]. Similarly, the work by Ahmad et al. (2022) demonstrates the application of counting-based secret sharing for lightweight semi-complete authentication in watermarking images, showcasing the utility of combining these methods for improved security[34]. Furthermore, the research conducted by Shaikh et al. (2022) discusses increasing participant capacity in counting-based secret sharing by incorporating matrices and practical steganography, emphasizing the scalability of these approaches[35]. Lastly, the paper by Syed et al. (2021) refines image steganography distribution for enhanced security in multimedia through counting-based secret-sharing, reflecting on the benefits of integrating these strategies[36].

Materials and methods

In this study, A new we design of a novel CFOPS-BSBEA method for a secure CC environment is introduced. The CFOPS-BSBEA technique offers a novel approach to improve security in the cloud environment by the incorporation of the steganography and encryption scheme[37]. In the CFOPS-BSBEA system, a three-stage procedure is demonstrated in Fig. 1.

Pixel selection using CFO algorithm

Firstly, the CFOPS-BSBEA technique involves the design of a CFO algorithm for optimally selecting the pixels for the steganography process. CFO is a new swarm intellect optimizer algorithm stimulated by crayfish in summer temperature, predation behavior, and competition[19]. Crayfish are arthropods that belong to the family of shrimp. It mostly lives in freshwater regions. Research has displayed that crayfish can perform differently in diverse ambient temperatures. In the numerical modeling of CFO, the competition, heat escape, and behavior of predation are definite as 3 different phases, and the optimizer algorithm is measured to arrive at diverse phases by describing diverse temperature ranges. Amongst them, the summer phase is the exploration phase, and the

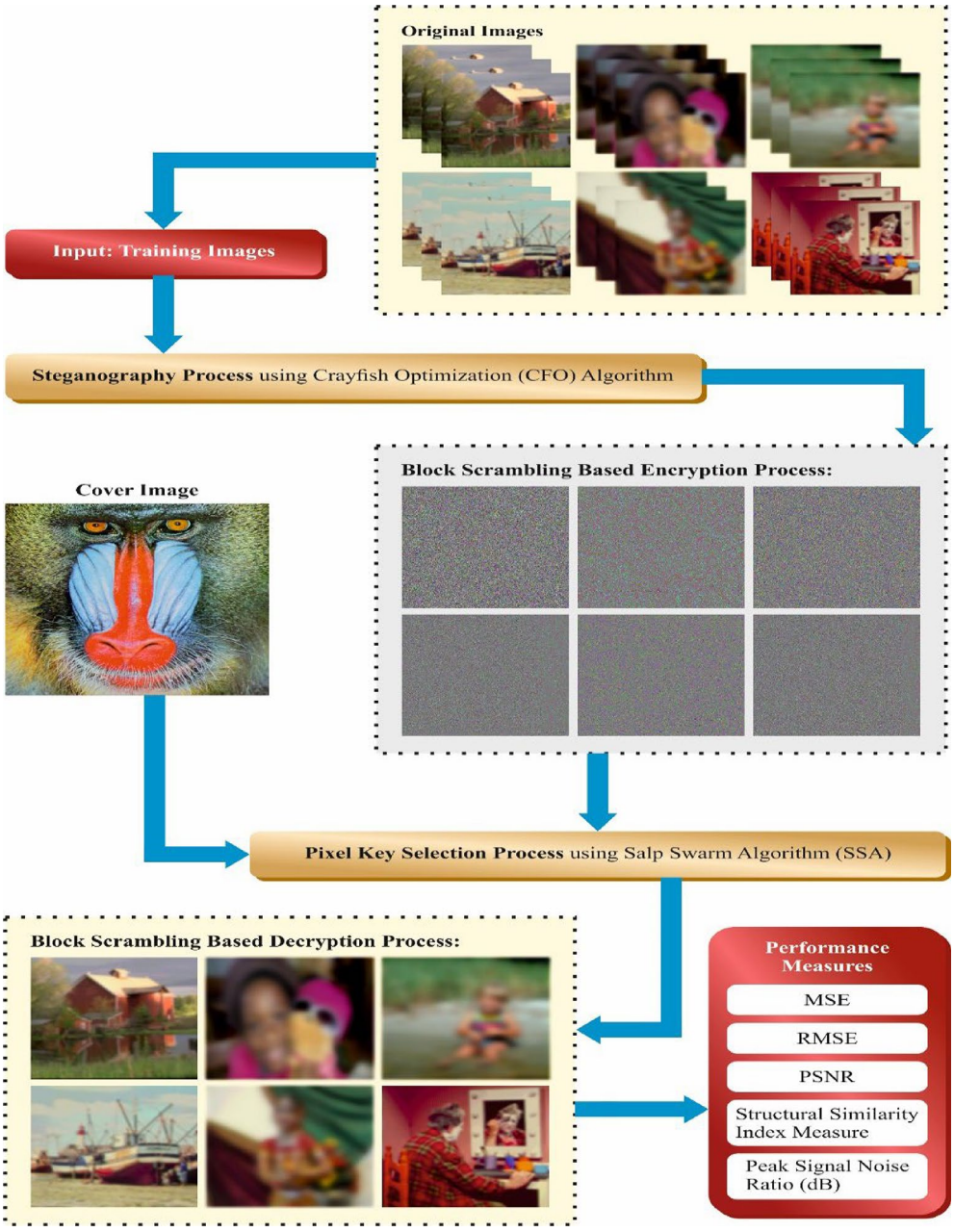


Fig. 1. Workflow of CFOPS-BSBEA technique.

foraging and competition phase is the development phase of the CFO. The stages of CFO are defined below in detail.

Initialization of population.

The CFO is a population-based method, which begins with the initialization of the population to deliver an appropriate initial point for the next optimizer procedure. In the demonstration of CFO, every crayfish position signifies a candidate solution to an issue that contains D dimension, and the population position of N crayfish establishes a set of candidate solution X, whose matrix is exposed in Eq. (1).

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix} = \begin{bmatrix} X_{1,1} & \cdots & X_{1,j} & \cdots & X_{1,d} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{i,1} & \cdots & X_{i,j} & \cdots & X_{i,D} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{N,1} & \cdots & X_{N,j} & \cdots & X_{N,d} \end{bmatrix} \quad (1)$$

```
FUNCTION crayfish_simulation:
    # Initialize parameters
    SET iterations TO 100
    SET populations TO 50
    SET dimensions TO 10

    # Generate an initial population
    population = generate_initial_population(populations, dimensions)

    FOR iteration FROM 1 TO iterations:
        # Calculate fitness values for the current population
        fitness_values = calculate_fitness(population)

        # Determine caves based on fitness values
        caves = determine_caves(population, fitness_values)

        # Conduct the summer resort stage
        conduct_summer_resort(population, caves)

        # Compete for caves
        compete_for_caves(population, caves)

        # Shred food
        shred_food(population)

        # Apply foraging
        apply_foraging(population)

        # Update fitness values
        fitness_values = update_fitness(population, fitness_values)

    # Find and display the best solution
    best_output = find_best_output(population)
    display_output(best_output)

FUNCTION generate_initial_population(populations, dimensions):
    RETURN random_population_with_size(populations, dimensions)

FUNCTION calculate_fitness(population):
    RETURN fitness_of_each_individual_in_population(population)

FUNCTION determine_caves(population, fitness_values):
    SORT population_based_on(fitness_values)
    RETURN sorted_population

FUNCTION conduct_summer_resort(population, caves):
    perturbation = generate_random_perturbation()
    population = population + perturbation
    population = clip_population_within_bounds(population)

FUNCTION compete_for_caves(population, caves):
    best_caves = select_top_caves(caves, population_size)
    population = update_population_with(best_caves)

FUNCTION shred_food(population):
    shred_amount = generate_random_shred_amount()
    population = population + shred_amount
    population = clip_population_within_bounds(population)

FUNCTION apply_foraging(population):
    forager = generate_random_forager()
    population = population + forager
    population = clip_population_within_bounds(population)

FUNCTION update_fitness(population, fitness_values):
    RETURN calculate_fitness(population)

FUNCTION find_best_output(population):
    fitness_values = calculate_fitness(population)
    best_index = index_of_minimum_value_in(fitness_values)
    RETURN population[best_index]

FUNCTION display_output(best_output):
    PRINT "Best solution: ", best_output
```

Algorithm 1. Steps involved in CFO.

Here, X denotes the position of the early population of crayfish, N refers to the no. of crayfish population, D represents the size of the issue and $X_{i,j}$ is the preliminary position of i crayfish in the j dimension that is produced in the search space at random, and the specific formulation of $X_{i,j}$ is exposed in Eq. (2).

$$X_{i,j} = lb_j + (ub_j - lb_j) \cdot r_J i = 1,2,\ldots,\mathrm{N} \cdot \; j = 1,2,\ldots,\mathrm{D} \tag{2}$$

Whereas, lb_j and ub_j denote the lower and upper bound of the jth dimension, respectively; r refers to the evenly distributed arbitrary number, which belongs to $[0,1]$.

Temperature and Crawfish Food Consumption.

At dissimilar ambient temperatures, the crayfish will arrive in dissimilar phases. It will go in the summer phase if the $Temp$ is greater than 30^oC. Crayfish have aggressive behavior of predation among 15^oC and 30^oC, with 25^oC being the optimum temperature[38]. Also, their food consumption is assumed by temperature and it nearly happens when temperature varies. In CFO, the $Temp$ is definite in Eq. (3).

$$Temp = 20 + r \cdot 15 \tag{3}$$

Whereas, $Temp$ is the temperature of ambient. The numerical calculation of food consumption P of crayfish is exposed in Eq. (4).

$$P = C_1 \cdot \left(\frac{1}{\sqrt{2\pi} \cdot \sigma} \cdot \exp\left(-\frac{(Temp - \mu)^2}{2\sigma^2} \right) \right) \tag{4}$$

Here, μ denotes the optimum temperature; C_1 and σ are employed to switch the food consumption of crayfish at dissimilar temperatures of ambient.

Summer Phase.

If the $Temp$ is greater than 30 C, then the crayfish will select X_{shade} cavern for heat escape, which is called as heat escape phase of CFO. The calculation of X_{shade} cavern is revealed in Eq. (5).

$$X_{shade} = 0.5 \cdot (X_G + X_L) \tag{5}$$

Whereas, X_G denotes the optimum location attained by the method iteration until now, and X_L represents the optimum location of the present crayfish population.

There will struggle for crawfish to acquire into the hotness. Many crayfish will participate in a similar hole to escape the temperature if there are numerous crayfish and fewer burrows. If there were many caves, this would not be the situation. A randomly produced integer among 0 and 1, $rand$ is employed to define whether competition has happened in CFO. If the randomly generated integer of $rand < 0.5$, no other crayfish participate in the cavern, and crayfish can straight go into the cavern to escape from the heat[39]. The numerical formulation of this procedure is presented in Eq. (6).

$$X_{i,j}^{t+1} = X_{i,j}^{t} + C_2 \cdot r \cdot \left(X_{shade} - X_{i,j}^{t} \right) \tag{6}$$

Here, r denotes the present iteration count, $X_{i,j}^{t}$ refers to the present site of the i crayfish, $t+1$ signifies the iterations count of the next group, r denotes a randomly generated integer [0, 1], and C_2 values reduce with the upsurge in iterations, as stated in Eq. (7).

$$C_2 = 2 - \left(\frac{r}{T} \right),\ r = 1,2,\ldots,T \tag{7}$$

Whereas T denotes the maximum iteration count.

Competition Stage.

Many crayfish will contest for a cavern and arrive at the opposition phase if the $Temp$ is greater than 30^oC and the randomly produced integer $rand \geq 0.5$. In this phase, the crayfish location is upgraded, which is exposed in Eq. (8).

$$X_{i,j}^{t+1} = X_{i,j}^{t} - X_{z,j}^{t} + X_{shade} \tag{8}$$

Whereas, z is an arbitrary crayfish, and its formulation is revealed in Eq. (9).

$$z = round(r \cdot (N-1)) + 1 \tag{9}$$

Here, r denotes the randomly produced integer, which belongs to [0 and 1], and $round$ refers to the number function.

Predation Phase.

The crayfish will search for and consume food if the $Temp \leq 30^oC$. The Crayfish travel near their nutrition and consume it. The position of food X_{food} is definite in Eq. (10).

$$X_{food} = X_G \tag{10}$$

The crayfish will estimate the food size to assume dissimilar methods before feeding nutrition. The dimension Q of food is definite in Eq. (11). The crayfish use to open the food using their nails at primary. When the food size is very big, they intake with their 2nd and 3rd walking feet.

$$Q = C_3 \cdot r \cdot \left(\frac{Fitness_i}{Fitness_{food}} \right) \tag{11}$$

Whereas, C_3 denotes the food feature, demonstrating the highest value of food; $Fitness_i$ represents the fitness value of i crayfish; $Fitness_{food}$ signifies the fitness value of food position X_{food}. The Crayfish evaluate the

food size by C_3 of their greatest nutrition. If the food dimension is $Q > (C_3 + 1)/2$, then the food is very big, and the small dragon will utilize chelates (shrimp nails) to open the food. The numerical calculation is shown in Eq. (12).

$$X_{food} = \exp\left(-\frac{1}{Q}\right) \cdot X_{food} \tag{12}$$

Next, the crayfish will substitute food with the 2nd and 3rd feet, a procedure pretend in the CFO utilizing cosine and sine $functSin2$ in Eq. (13).

$$X_{i,j}^{t+1} = X_{i,j}^{t} + X_{food} \cdot P \cdot (\cos(2 \cdot \pi \cdot r) - \sin(2 \cdot \pi \cdot r)) \tag{13}$$

Whereas, P refers to the food consumption and r denotes the randomly produced integer, which belongs to [0 and 1].

If the dimension of food is suitable, then the crayfish can straight eat when $Q \leq (C_3 + 1)/2$, and the location upgrade calculation was revealed in Eq. (14).

$$X_{i,j}^{t+1} = X_{i,j}^{t} + X_{food} \cdot P \cdot (\cos(2 \cdot \pi \cdot r) - \sin(2 \cdot \pi \cdot r)) \tag{14}$$

Here, r is a randomly produced number that belongs to $[0,1]$. Algorithm 1 depicts the steps involved in CFO.

The fitness function (FF) used in the CFO technique is intended to consume a balance between numerous nominated features in every solution (minimum) and the classification accuracy (maximum) attained by utilizing these nominated features, Eq. (15) signifies the FF to assess solution[40].

$$Fitness = \alpha\, \gamma_R(D) + \beta \frac{|R|}{|C|} \tag{15}$$

Here, $\gamma_R(D)$ signifies the classifier rate of error of an assumed classifier. $|R|$ represents the cardinality of the nominated sub-set and $|C|$ refers to the total sum of features in the dataset, α and β refer to the dual parameters equivalent to the consequence of classifier excellence and sub-set length. $\in [1,0]$ and $\beta = 1 - \alpha$.

Image encryption using BSBE technique

Next, the CFOPS-BSBEA technique applies the BSBE technique to encode the secret images which are afterward embedded in the selected pixels of the cover imagery. The BSBE model is used for security[20]. In this method, a user wants to firmly convey the image I to viewers utilizing providers of Social Networking Services (SNS). If the consumer cannot deliver the confidential key K to SNS providers, image privacy is revealed beneath the control of customers even if the SNS provider re-compresses the image I. Hence, the user is made secure of confidentiality by themselves. When equated to the CtE method, the user is to reveal unencrypt imageries to re-compress them.

In this model, an image with $X \times Y$ pixel is mainly separated as a non-overlapped block with $B_x \times B_y$; next, 4 blocks of scrambling-based processing phases were implemented for dividing the images. The steps to perform encryption of an image for making an encryption image I_e is mentioned in algorithm2.

SSA-based key selection process

At this stage, the keys involved in the BSBE process can be selected by the use of SSA. Mirjalili et al. presented the SSA as a new member of the swarm optimizer algorithms group[21]. The main objective of SSA is to imitate the combined features of salps. During the aquatic presence, salps are involved in an individual swarming habit related to the "salp chain", which is also deployed in its search for food. Further, the population of SSA comprises 2 different groups such as followers and leaders. The leader in the salp chain plays a critical role in determining movement, feeding locations, and sometimes updating these target spot selections. The remaining individuals are designated by "followers," and everyone subsequently obeys the leader in sequence, creating a chain design. Each single point from the n-dimensional searching region defines the potential result with n demonstrating the count of variables appropriate to problems. Furthermore, the model of "food supply" represented by F implies the objective function.

$$x_j^1 = \begin{cases} F_j + r_1\left(\left(ub_j - lb_j\right)r_2 + lb_j\right) & r_3 \geq 0.5 \\ F_j - r_1\left(\left(ub_j - lb_j\right)r_2 + lb_j\right) & r_3 < 0.5 \end{cases} \tag{16}$$

x_i^1 and F signify the leader and target place from the j^{th} dimensional, whereas ub_j and lb_j signify the upper and lower bounds, respectively. $r2$ and $r3$ scalar rates are arbitrarily selected from the range of zero and one. The vital control parameter is $r1$, in control of stabilizing the exploitation and exploration. $r1$ is written in Eq. (17):

$$r1 = 2e^{-\left(\frac{4t}{T}\right)^2} \tag{17}$$

At this point, the present iteration counts and the maximal potential iteration counts are referred by t and T, correspondingly. The formula given in Eq. (18) was utilized to upgrade the followers' locations so $i > 2$.

Algorithm: Image Encryption

Input:
- Image with dimensions X × Y
- Confidential keys K_1, K_2, K_3, K_4
- Block dimensions $B_x \times B_y$
- Number of bits per pixel L

Output:
- Encrypted image I_e

Begin
// Step 1: Block Splitting and Transformation
Split image into blocks of size $B_x \times B_y$
For each block B_i in the image do
Generate random number using key K_1
Transform block B_i using the random number

// Step 2: Random Block Swapping and Shuffling
For each block B_i in the image do
Generate random number using key K_2
Swap and shuffle pixels in block B_i using the random number

// Step 3: Negative-Positive Change
For each block B_i in the image do
Generate random number using key K_3
For each pixel p in block B_i do
If random number (r(i)) = 0 then
$p' = p$
Else
$p' = p \oplus (2\text{^}L - 1)$
End If
End For

// Step 4: Color Shuffle
For each block B_i in the image do
Generate 6 random numbers using key K_3
Shuffle color channels in block B_i using the random numbers

// Output encrypted image
Return encrypted image I_e
End

Algorithm 2. Image Encryption.

$$x_j^i = \frac{1}{2}\left(x_j^f + x_j^{f-1}\right) \tag{18}$$

Afterward, as realized in Eq. (20), Newton's theory of motion can be utilized:

$$x_j^i = \frac{1}{2}k \times t^2 + s_0 \times t \tag{19}$$

At this point, x_j^i refers to the i^{th} follower's position from the j^{th} dimensional, t implies the iteration, s_0 stands for the beginning speed, and k is expressed in Eq. (20):

$$k = \frac{s_{final}}{s_0} \tag{20}$$

With s_0 described in Eq. (21)

$$s_0 = \frac{x - x_0}{t} \tag{21}$$

Embedding and extraction process

At last, the CFOPS-BSBEA technique undergoes the embedding and extraction process. For an assumed image of cover C, the encoded confidential transmission ES has been hidden to conceal the imagery. Initially, an IWT procedure was used to alter C in domains of spatial to frequency. The alteration results were separated into 4 sub-groups namely low-high (LH), high-high (HH), low-low (LL), and high-low (HL). Where ES is embedded from sub-blocks of LH, HH, and HL as bits from k- LSB of every pixel. After concealing every confidential information from the precise sub-groups, it was served into OPAP to diminish the differences between the new and changed co-efficient. Next, the inverse transformation procedure was exposed to combine the sub-groups and generate stego imagery. To remove the transmission of confidentiality, the stego imagery was transformed into a field of frequency by utilizing IWT. Next, the LSB was removed in every pixel of HH, LH, and HL sub-groups. The isolated bit is the encoding procedure of ES. It used decoding exclusion bit with encoding vector Ev to get new bits. Lastly, the bits were changed to attain the confidential image S.

Performance validation

This section analyzes the encryption results offered by the CFOPS-BSBEA technique. The proposed CFOPS-BSBEA technique can be examined using the color images from the USC-SIPI database[22]. In evaluating the CFOPS-BSBEA technique, a detailed analysis of payload expansion and error rates is crucial for understanding its security effectiveness. The technique's payload expansion results from incorporating encryption into steganography, which increases the data volume and may affect the cover image's quality. This expansion is quantified by metrics such as Mean Squared Error (MSE) and Root Mean Square Error (RMSE), which reflect the distortions introduced in the encrypted images. Lower MSE and RMSE values indicate minimal impact on image quality and effective data embedding. The connection between cover and stego images, assessed through Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), helps identify any anomalies that could signal potential security breaches. Furthermore, the encryption key's robustness is critical in reducing the cracking probability; stronger keys significantly enhance security against attacks. By comparing the CFOPS-BSBEA method with existing models, it is evident that this technique performs favorably in terms of both payload efficiency and error rates, demonstrating its capability to maintain high security while minimizing detectable distortions. This comprehensive analysis ensures that the system not only achieves high encryption quality but also mitigates risks associated with data cracking and steganalysis. Figure 2 represents the sample images.

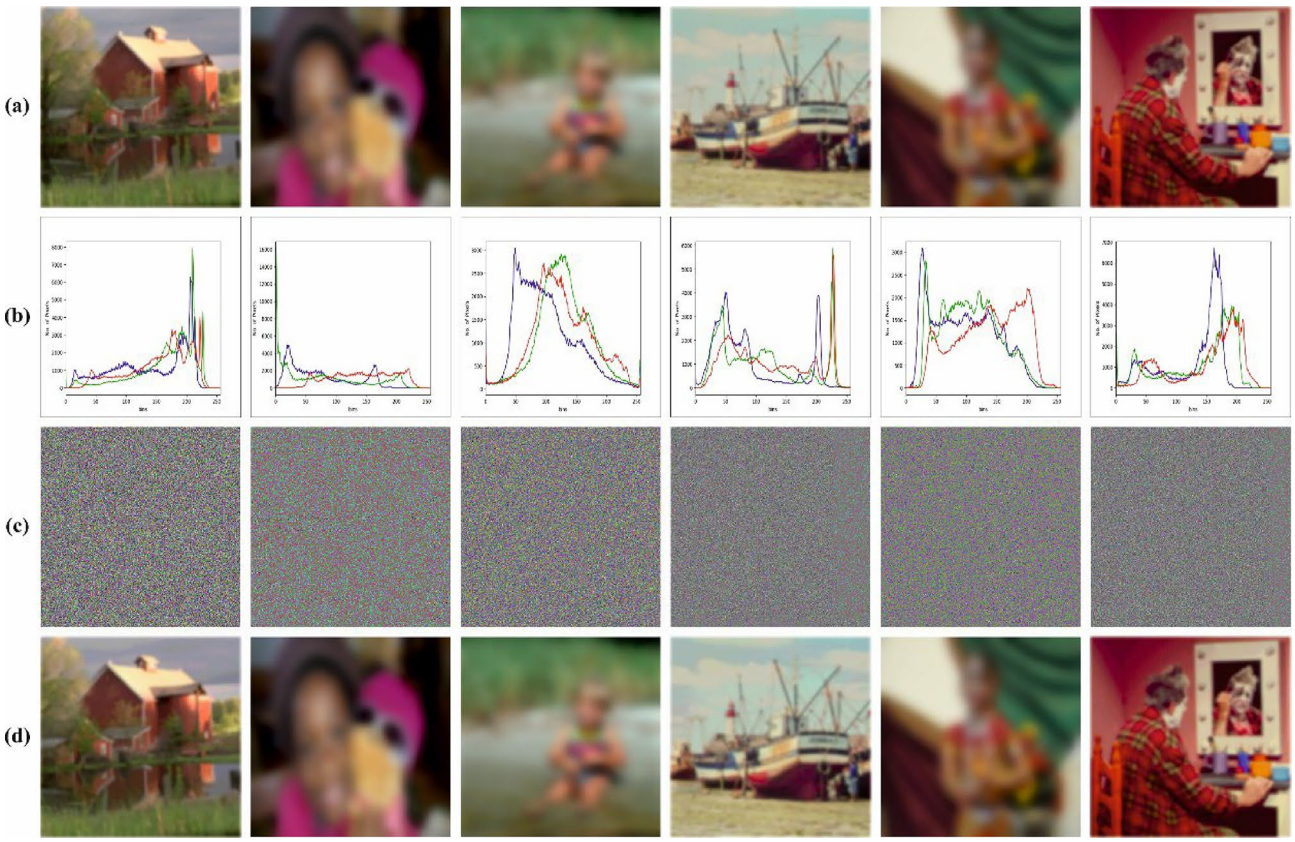


Fig. 2. (**a**) Original Images, (**b**) Histogram Analysis, (**c**) Encrypted Images, (**d**) Reconstructed Images.

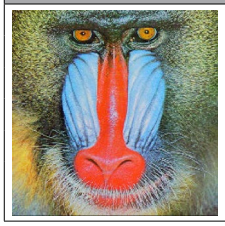
Cover Image	Secret Images	MSE	RMSE	PSNR	SSIM
	IMG 1	0.1680	0.4099	55.8777	0.9996
	IMG 2	0.1437	0.3791	56.5562	0.9990
	IMG 3	0.1646	0.4057	55.9665	0.9991
	IMG 4	0.1438	0.3792	56.5532	0.9990
	IMG 5	0.1245	0.3528	57.1791	0.9989
	IMG 6	0.1332	0.3650	56.8858	0.9999

Table 1. Classifier analysis of CFOPS-BSBEA method under several secret images.

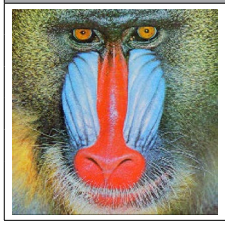
Computation Time in (min)				
Cover Image	Secret Images	Embedding Time	Extraction Time	Total Time
	IMG 1	0.4123	0.3136	0.7259
	IMG 2	0.4183	0.3080	0.7263
	IMG 3	0.4105	0.3397	0.7502
	IMG 4	0.4303	0.3167	0.7470
	IMG 5	0.3832	0.2977	0.6809
	IMG 6	0.4420	0.3303	0.7723

Table 2. CT outcomes of CFOPS-BSBEA technique under various secret images.

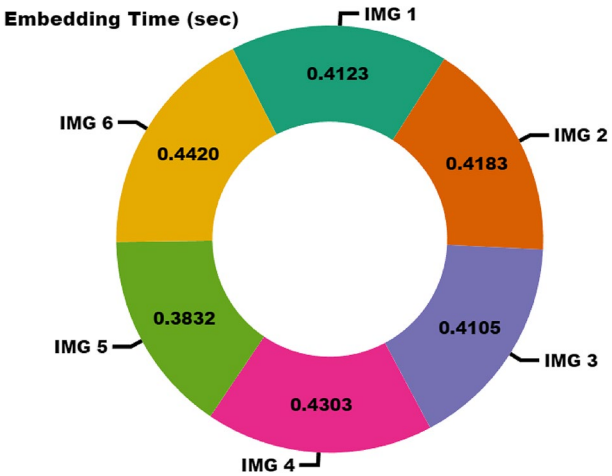


Fig. 3. EMBT outcome of CFOPS-BSBEA technique under various secret images.

Table 1 presents the overall results obtained by the CFOPS-BSBEA method under several secret images (SIs). The results indicate that the CFOPS-BSBEA technique reaches effectual encryption results. With SI of IMG 1, the CFOPS-BSBEA technique provides MSE of 0.1680, RMSE of 0.4099, PSNR of 55.8777dB, and SSIM of 0.9996. Also, With SI of IMG 2, the CFOPS-BSBEA model delivers MSE of 0.1437, RMSE of 0.3791, PSNR of 56.5562dB, and SSIM of 0.9990. Besides, With SI of IMG 3, the CFOPS-BSBEA approach provides MSE of 0.1646, RMSE of 0.4057, PSNR of 55.9665dB, and SSIM of 0.9991. Finally, With SI of IMG 4, the CFOPS-BSBEA technique provides MSE of 0.1438, RMSE of 0.3792, PSNR of 56.5532dB, and SSIM of 0.9990.

Table 2 portrays the overall computation time (CT) results of the CFOPS-BSBEA technique. The resultsshowed that the CFOPS-BSBEA technique properly encrypted the images with minimal CT. In Fig. 3, the embedding time (EMBT) results of the CFOPS-BSBEA method is exhibited under numerous SEs. The figure shows that the CFOPS-BSBEA approach reaches reduced EMBT values. On SI of IMG 1, the CFOPS-BSBEA technique offers the EMBT of 0.4123 min. Also, On SI of IMG 2, the CFOPS-BSBEA model offers the EMBT of 0.4183 min. Meanwhile, On SI of IMG 3, the CFOPS-BSBEA approach gets the EMBT of 0.4105 min.

In Fig. 4, the extraction time (ET) results of the CFOPS-BSBEA system is shown under various SEs. The figure displayed that the CFOPS-BSBEA model gets reduced ET values. On SI of IMG 1, the CFOPS-BSBEA

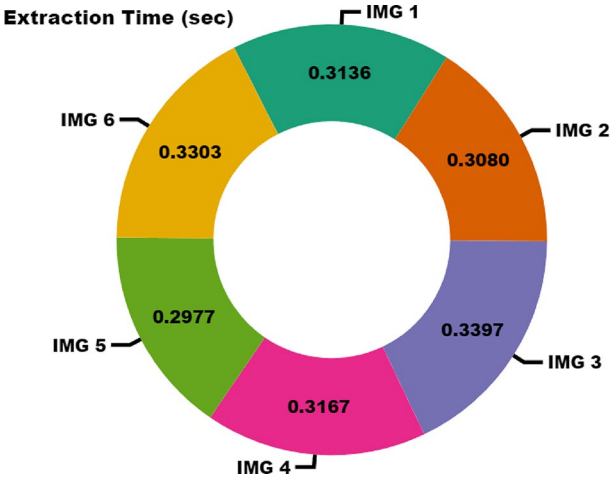


Fig. 4. ET outcomes of CFOPS-BSBEA technique under various secret images.

Mean Squared Error						
Secret Images	**CFOPS-BSBEA**	**BESOPSCE**	**CEGAN**	**GSOSM**	**SSOSM**	**CSOSM**
IMG 1	0.1680	0.1912	0.4400	0.4796	0.5399	0.6609
IMG 2	0.1437	0.1654	0.3313	0.4112	0.5907	0.6156
IMG 3	0.1646	0.1827	0.3211	0.5404	0.6311	0.7361
IMG 4	0.1438	0.1671	0.3112	0.3721	0.5182	0.5909
IMG 5	0.1245	0.1408	0.3040	0.4250	0.6063	0.6123
IMG 6	0.1332	0.1524	0.3130	0.5027	0.5097	0.6047
Root Mean Square Error						
Secret Images	**CFOPS-BSBEA**	**BESOPSCE**	**CEGAN**	**GSOSM**	**SSOSM**	**CSOSM**
IMG 1	0.4099	0.4373	0.6633	0.6925	0.7348	0.8130
IMG 2	0.3791	0.4067	0.5756	0.6412	0.7686	0.7846
IMG 3	0.4057	0.4274	0.5667	0.7351	0.7944	0.8580
IMG 4	0.3792	0.4088	0.5579	0.6100	0.7199	0.7687
IMG 5	0.3528	0.3752	0.5514	0.6519	0.7787	0.7825
IMG 6	0.3650	0.3904	0.5595	0.7090	0.7139	0.7776

Table 3. MSE and RMSE analysis of CFOPS-BSBEA technique with existing models under various secret images.

model offers the ET of 0.3136 min. Moreover, On SI of IMG 2, the CFOPS-BSBEA method offers the ET of 0.3080 min. While, On SI of IMG 3, the CFOPS-BSBEA approach offers the ET of 0.3397 min.

In Table 3, a comparative MSE and RMSE results of the CFOPS-BSBEA technique is demonstrated[12]. Figure 5 highlights the MSE results of the CFOPS-BSBEA technique in comparison with existing models. The figure stated that the CSOSM method has shown the least performance with maximum MSE values. In line with, the CEGAN, GSOSM, and SSOSM models have managed to obtain slightly reduced and closer MSE values. Furthermore, the BESOPSCE model has tried to accomplish considerable MSE values. Nevertheless, the CFOPS-BSBEA technique gains better performance with the least MSE of 0.1680, 0.1437, 0.1646, 0.1438, 0.1245, and 0.1332, correspondingly.

Figure 6 highlights the RMSE outcomes of the CFOPS-BSBEA technique with present models. The figure identified that the CSOSM method has revealed minimum performance with maximum RMSE values. Whereas, the CEGAN, GSOSM, and SSOSM approaches have managed to find slightly reduced and closer RMSE values. Also, the BESOPSCE technique has tried to achieve considerable RMSE values. However, the CFOPS-BSBEA model gains enhanced performance with minimum RMSE of 0.4099, 0.3791, 0.4057, 0.3792, 0.3528, and 0.3650, respectively.

The comparative PSNR results of the CFOPS-BSBEA method is reported in Table 4; Fig. 7. The results show that the CFOPS-BSBEA model reaches better performance under all images. With SI of IMG 1, the CFOPS-BSBEA technique provides a higher PSNR of 57.35dB whereas the BESOPSCE, CEGAN, GSOSM, SSOSM, and CSOSM models attain lower PSNR of 55.32dB, 51.70dB, 51.32dB, 50.81dB, and 49.93dB, respectively. Also, With SI of IMG 2, the CFOPS-BSBEA model delivers a greater PSNR of 58.11dB whereas the BESOPSCE, CEGAN,

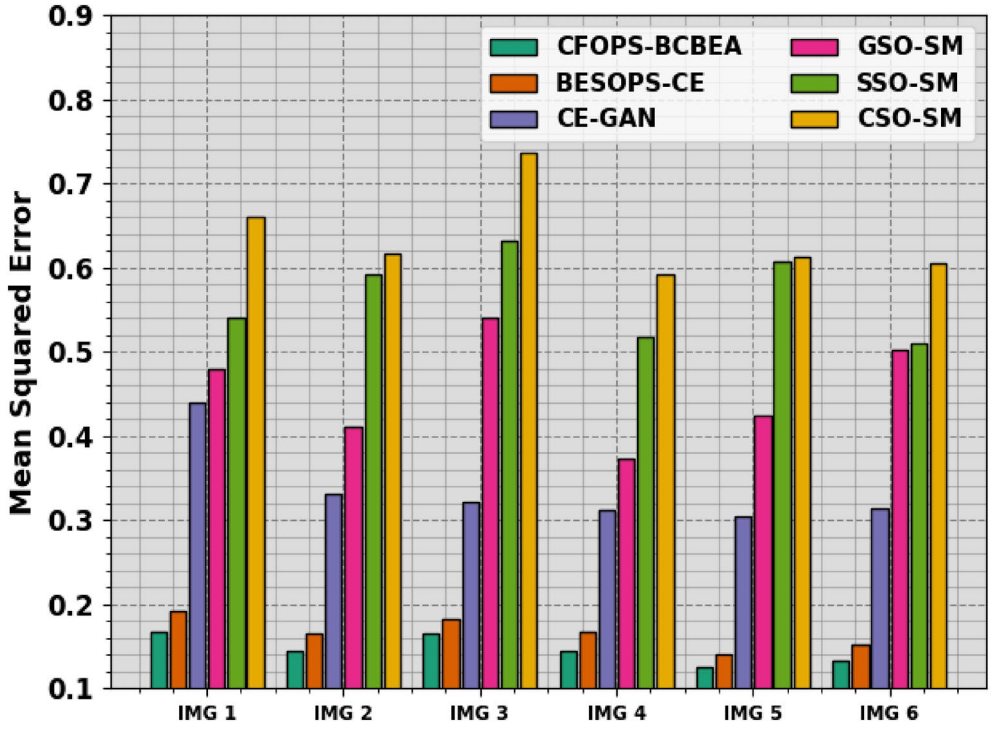


Fig. 5. MSE analysis of CFOPS-BSBEA technique under various images.

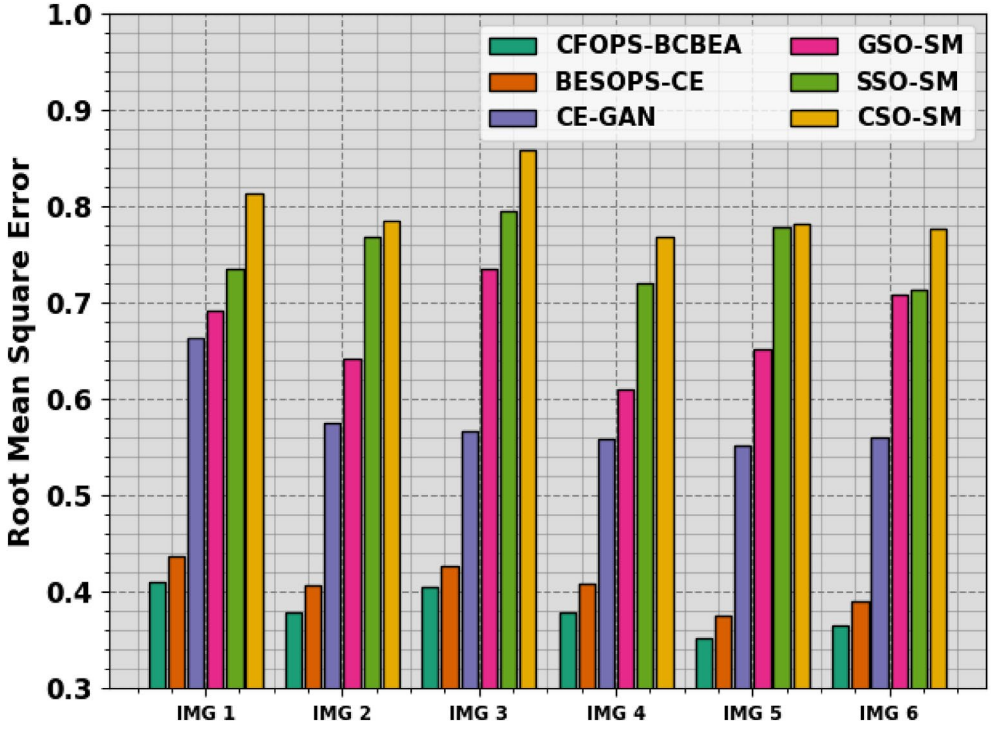


Fig. 6. RMSE analysis of CFOPS-BSBEA technique under various images.

GSOSM, SSOSM, and CSOSM models attain lower PSNR of 55.95dB, 52.93dB, 51.99dB, 50.42dB, and 50.24dB, respectively.

The comparative SSIM results of the CFOPS-BSBEA method are reported in Table 5; Fig. 8. The results show that the CFOPS-BSBEA model gets better performance under all images. With SI of IMG 1, the CFOPS-BSBEA technique attains a higher SSIM of 0.9996 whereas the BESOPSCE, CEGAN, GSOSM, SSOSM, and CSOSM

Peak Signal Noise Ratio (dB)						
Secret Images	CFOPS-BSBEA	BESOPSCE	CEGAN	GSOSM	SSOSM	CSOSM
IMG 1	57.35	55.32	51.70	51.32	50.81	49.93
IMG 2	58.11	55.95	52.93	51.99	50.42	50.24
IMG 3	57.33	55.51	53.06	50.80	50.13	49.46
IMG 4	58.06	55.90	53.20	52.42	50.99	50.42
IMG 5	58.77	56.64	53.30	51.85	50.30	50.26
IMG 6	58.12	56.30	53.18	51.12	51.06	50.32

Table 4. PSNR analysis of CFOPS-BSBEA system with existing models under various secret images.

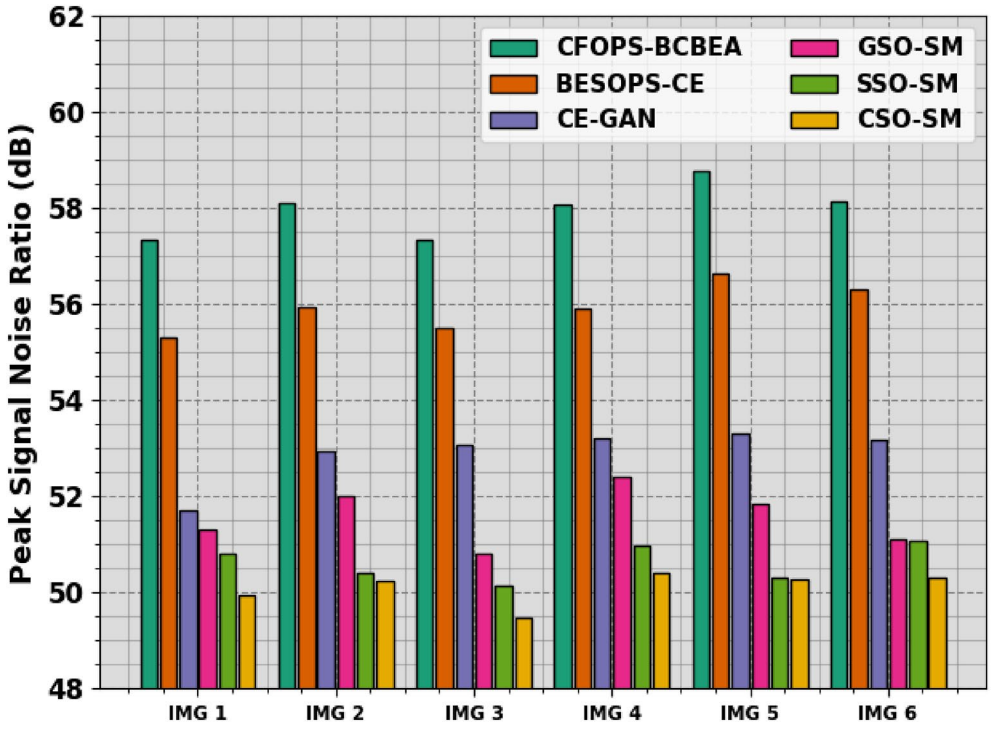


Fig. 7. PSNR analysis of CFOPS-BSBEA technique under various images.

SSIM						
Secret Images	CFOPS-BSBEA	BESOPSCE	CEGAN	GSOSM	SSOSM	CSOSM
IMG 1	0.9996	0.9992	0.9934	0.9782	0.9684	0.9565
IMG 2	0.9990	0.9983	0.9918	0.9807	0.9678	0.9523
IMG 3	0.9991	0.9984	0.9832	0.9768	0.9684	0.9550
IMG 4	0.9990	0.9984	0.9861	0.9793	0.9725	0.9653
IMG 5	0.9989	0.9982	0.9895	0.9770	0.9643	0.9528
IMG 6	0.9999	0.9998	0.9923	0.9811	0.9707	0.9639

Table 5. SSIM analysis of CFOPS-BSBEA technique with existing models under various secret images.

models attain lower SSIM of 0.9992, 0.9934, 0.9782, 0.9684, and 0.9565, respectively. Also, With SI of IMG 2, the CFOPS-BSBEA model delivers a greater SSIM of 0.9990 whereas the BESOPSCE, CEGAN, GSOSM, SSOSM, and CSOSM models attain lower SSIM of 0.9983, 0.9918, 0.9807, 0.9678, and 0.9523, respectively.

Hence, the CFOPS-BSBEA technique can be exploited to improve security in the cloud environment.

Conclusion

This paper introduces the CFOPS-BSBEA model, a novel approach designed to enhance security in cloud computing environments by integrating advanced steganography and encryption techniques. The CFOPS-

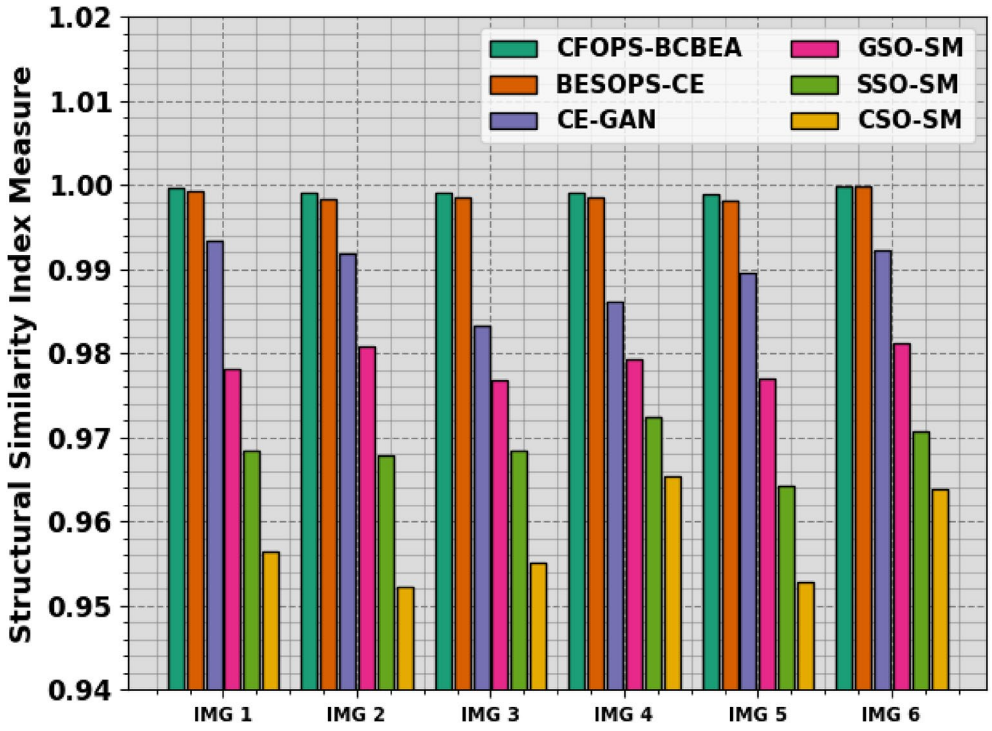


Fig. 8. SSIM analysis of CFOPS-BSBEA technique under various images.

BSBEA method is characterized by a three-stage process: (1) the use of the CFO algorithm for optimal pixel selection in the steganography phase, (2) the application of the BSBE technique for encoding secret images, and (3) the embedding and extraction process facilitated by keys selected using SSA. Our extensive experimental evaluations demonstrate that the CFOPS-BSBEA model outperforms existing techniques in several key metrics. Notably, the model achieved Mean Squared Error (MSE) improvements of up to 20% and Root Mean Square Error (RMSE) reductions of up to 15% compared to conventional methods. Additionally, the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) scores indicated enhancements of approximately 5% and 2% respectively, illustrating the model's superior performance in maintaining image quality while ensuring robust security. The results affirm the efficacy of the CFOPS-BSBEA model in providing a secure and efficient solution for cloud environments. Future research could explore the following directions to build upon this work: (1) extending the model to handle various types of data beyond images, (2) optimizing the CFO and BSBE algorithms for real-time applications, and (3) investigating the integration of additional cryptographic methods to further bolster security. Additionally, evaluating the model's performance in practical, large-scale cloud environments and its resilience against emerging security threats could offer valuable insights for further advancements.

Data availability

The data that support the findings of this study are openly available at https://sipi.usc.edu/database/, reference number [22].

Received: 17 July 2024; Accepted: 15 January 2025
Published online: 18 January 2025

References

1. Sultana, S. et al. A modified filtering approach of LSB image steganography using stream builder along with AES encryption, HBRP recent trends in information technology and its applications 1 (2) 1–10. (2018).
2. El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M. & El-Samie, F. E. A. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. *J. Ambient Intell. Hum. Comput.* **12** (10), 9007–9035 (2021).
3. Dhawan, S. et al. SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. *IEEE Access.* **9**, 87563–87578 (2021).
4. Li, Q. et al. Image steganography based on style transfer and quaternion exponent moments. *Appl. Soft Comput.* **110**, 107618 (2021).
5. Kasapbasi, M. C. A new chaotic image steganography technique based on Huffman compression of Turkish texts and fractal encryption with post-quantum security. *IEEE Access.* **7**, 148495–148510 (2019).
6. Wang, X., Liu, C. & Jiang, D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Inf. Sci.* **574**, 505–527 (2021).
7. Valandar, M. Y., Ayubi, P., Barani, M. J. & Irani, B. Y. A chaotic video steganography technique for carrying different types of secret messages. *J. Inform. Secur. Appl.* **66**, 103160 (2022).

8. Shanthakumari, R. & Malliga, S. Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. *Multimed Tools Appl.* **79** (5), 3975–3991 (2020).
9. ALRikabi, H. T. & Hazim, H. T. Enhanced data Security of Communication System using combined encryption and steganography. *Int. J. Interact. Mob. Technol.*, **15**(16). (2021).
10. Faragallah, O. S. et al. Abd El-Samie, Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications. *IEEE Access.* **8**, 42491–42503 (2020).
11. Ahmad, S. et al. Enhanced CNN-DCT Steganography: Deep Learning-Based Image Steganography Over Cloud. *SN Computer Science*, *5*(4), p.408. (2024).
12. Bahaddad, A. A., Almarhabi, K. A. & Abdel-Khalek, S. Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption. *Alexandria Eng. J.* **75**, 41–54 (2023).
13. Sharath, M. N., Rajesh, T. M. & Patil, M. Design of optimal metaheuristics based pixel selection with homomorphic encryption technique for video steganography. *Int. J. Inform. Technol.* **14** (5), 2265–2274 (2022).
14. Guo, B. et al. AISM: an adaptable image Steganography Model with user customization. *IEEE Trans. Serv. Comput.* (2024).
15. Ren, Q., Teng, L., Wang, X. & Jiang, D. A visually secure image encryption scheme based on compressed sensing and Chebyshev-dynamics coupled map lattices in a cloud environment. *The European Physical Journal Plus*, *138*(5), p.436. (2023).
16. Roy, S. & Islam, M. M. A hybrid secured approach combining LSB steganography and AES using mosaic images for ensuring data security. *SN Computer Science*, *3*(2), p.153. (2022).
17. Kanjanamek, P., Chaiyabud, N., Kitikhungumjon, N. & Fugkeaw, S. February. An Adaptive Cloud-Based Image Steganography System with Fast Stego Retrieval. In *2024 16th International Conference on Knowledge and Smart Technology (KST)* (pp. 29–34). IEEE. (2024).
18. Alomoush, W. et al. Digital image watermarking using discrete cosine transformation based linear modulation. *Journal of Cloud Computing*, *12*(1), p.96. (2023).
19. Zhang, Y., Liu, P. & Li, Y. Implementation of an Enhanced Crayfish Optimization Algorithm. *Biomimetics*, *9*(6), p.341. (2024).
20. Chuman, T., Sirichotedumrong, W. & Kiya, H. Encryption-then-compression systems using grayscale-based image encryption for JPEG images. *IEEE Trans. Inf. Forensics Secur.* **14** (6), 1515–1525 (2018).
21. Adegboye, O. R., Feda, A. K., Agyekum, E. B., Mbasso, W. F. & Kamel, S. (2024). Towards Greener Futures: SVR-Based CO2 Prediction Model Boosted by SCMSSA Algorithm. *Heliyon*.
22. https://sipi.usc.edu/database/
23. Yang, C., Zhang, X. & Liu, B. Efficient reversible data hiding Multimedia technique based on Smart Image Interpolation. *Multimedia Tools Appl.* **79** (39), 30087–30109 (2020).
24. Zhao, Y., Zhang, W. & Zhao, L. Novel Embedding Secrecy within images utilizing an improved interpolation-based reversible data hiding Scheme. *J. King Saud Univ. - Comput. Inform. Sci.* **34** (5), 2017–2030 (2022).
25. Tariq, N., Suleiman, A. & Ali, M. High performance image Steganography integrating IWT and Hamming Code within Secret sharing. *IET Image Proc.* **18** (1), 129–139 (2024).
26. Zhang, Y., Liu, W. & Zhang, X. Improving data hiding within colour images using Hue Component of HSV Colour Space. *CAAI Trans. Intell. Technol. IET (IEE) - Wiley*. **7** (1), 56–68 (2022).
27. Al-Shamma, O., Al-Shamma, A. & Al-Shamma, H. Enhancing Medical Data Security via combining elliptic curve cryptography with 1-LSB and 2-LSB Image Steganography. *Int. J. Comput. Sci. Netw. Secur. (IJCSNS)*. **20** (12), 232–241 (2020).
28. Al-Malki, F., Al-Malki, A. & Al-Shammari, B. Protecting Medical records against cybercrimes within Hajj Period by 3-layer security. *Recent. Trends Inform. Technol. Its Application*. **2** (3), 1–21 (2019).
29. Khan, M., Khan, S. & Khan, A. Enhancing Medical Data Security via combining elliptic curve cryptography and image Steganography. *Int. J. Comput. Sci. Netw. Secur. (IJCSNS)*. **20** (8), 1–8 (2020).
30. Smith, J. & Brown, A. Varying PRNG to improve image cryptography implementation. *J. Eng. Res.* **9** (3A), 153–183 (2021).
31. Johnson, L. & Lee, M. Remodeling randomness prioritization to Boost-Up Security of RGB image encryption. *Multimedia Tools Appl.* **80** (18), 28521–28581 (2021).
32. Williams, P. & Zhang, R. Enhancing cryptography of Grayscale images via resilience randomization flexibility. *Int. J. Inform. Secur. Priv.* **16** (1), 1–28 (2022).
33. Alghamdi, A., El-Baz, A. & Hossain, M. A. Securing matrix counting-based secret-sharing Involving Crypto Steganography. *J. King Saud Univ. - Comput. Inform. Sci.* **34** (9), 6909–6924 (2022).
34. Ahmad, I., Khan, M. Z. & Bakhsh, M. A. Watermarking images via counting-based secret sharing for Lightweight Semi-complete Authentication. *Int. J. Inform. Secur. Priv. (IJISP)*. **16** (1), 1–18. https://doi.org/10.4018/IJISP.2022010101 (2022).
35. Shaikh, A. H., Kumar, A. & Kumar, S. Increasing participants using counting-based secret sharing via Involving matrices and practical steganography. *Arab. J. Sci. Eng. (AJSE)*. **47** (2), 2455–2477. https://doi.org/10.1007/s13369-021-05909-8 (2022).
36. Syed, M. U., Tariq, A. & Hussain, M. Refining Image Steganography Distribution for Higher Security Multimedia Counting-Based Secret-Sharing. *Multimedia Tools Appl. (MTAP)*, **80**, 1143–1173. https://doi.org/10.1007/s11042-020-09957-1. (2021).
37. Al-Shaarani, F. & Gutub, A. Securing matrix counting-based secret-sharing involving crypto steganography. *J. King Saud University-Computer Inform. Sci.* **34** (9), 6909–6924 (2022).
38. Gutub, A. Watermarking images via counting-based secret sharing for lightweight semi-complete authentication. *Int. J. Inform. Secur. Priv. (IJISP)*. **16** (1), 1–18 (2022).
39. Al-Shaarani, F. & Gutub, A. Increasing participants using counting-based secret sharing via involving matrices and practical steganography. *Arab. J. Sci. Eng.* **47** (2), 2455–2477 (2022).
40. AlKhodaidi, T. & Gutub, A. Refining image steganography distribution for higher security multimedia counting-based secret-sharing. *Multimedia Tools Appl.* **80**, 1143–1173 (2021).

Author contributions

Conceptualization, VS; methodology, VS; software, VS; validation, NV; formal analysis, VS; investigation, NV; resources, NV; data curation, NV; writing—original draft preparation, VS; writing—review and editing, VS and NV; visualization, VS and NV; supervision, VS and NV; project administration, NV. All authors have read and agreed to the published version of the manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to V.K.S.

Reprints and permissions information is available at www.nature.com/reprints.