Kurdistan Journal of Applied Research (KJAR)
Print-ISSN: 2411-7684 | Electronic-ISSN: 2411-7706

Website: Kjar.spu.edu.iq | Email: kjar@spu.edu.iq

A Secure Image Steganography Using Shark Smell Optimization and Edge Detection Technique

Pshtiwan J. Karim
Department of Computer Science
College of Science
University of Garmian
Kalar, Iraq
Pshtiwan.jabar@garmian.edu.krd

Omar Y. Abdulhammed
Department of Computer Science
College of Science
University of Garmian
Kalar, Iraq
Omar.y@garmian.edu.krd

Dashne R. Arif
Computer Center
Sulaimani Technical Institute
Sulaimani Polytechnic University
Sulaymaniyah, Iraq
Dashne.raouf@spu.edu.iq

Twana S. Ali
Department of Computer Science
College of Science
University of Sulaimani
Sulaymaniyah, Iraq
Twana.ali@univsul.edu.iq

Avin O. Abdalrahman
Department of Civil Engineering
College of Engineering
University of Garmian
Kalar, Iraq
Aveen.othman@garmian.edu.krd

Arkan A. Saffer
Department of Information Technology
Kalar Technical College
Sulaimani Polytechnic University
Kalar, Iraq
Arkan.saffer@spu.edu.iq

Volume 7-Issue 2- December 2022

DOI: 10.24017/Science.2022.2.2

Article history:

Received 25/07/2022
Accepted 20/09/2022

Keywords:

steganography, security, payload, shark smell optimization, edge detection

ABSTRACT

The steganographic system provides premium secrecy and ability of conserving the secret information from gaining stalked or cracked. The suggested method consists of five phases which are masking and divided image, edge detection, apply shark smell optimization (SSO), embedding and extraction. This paper concentrated on three significant basic parts which are payload, quality, and security also introduces a new steganography method through using edge detection algorithm and SSO. The process of concealment is carried out through the following steps: Firstly, to promote the hiding ability and to realize altitude standard of secrecy the secret message is separated into four parts and the cover image is masked and divided into four sections, then the edge detection algorithm and SSO is performed on each section respectively. Edge prospectors were utilized to produce edge pixels in every section to hide secret message and attain the best payload. To increase security, the shark smell optimization is used to select the best pixels among edge pixels based on its

nature in motion, then reflect these best pixels on original cover image. Finally the secret message bits are hidden in the selected edge best pixels by using lest significant bit technique. The experimental out comes appreciated utilizing several image fitness appreciation fashion, it displays best hiding ability, achieve higher image quality with least standard of deformation and provide altitude standard of secrecy, also the results shows that the suggested method exceeds previous approaches in term of the PSNSR and MSE, additionally demonstrate that the secret information cannot be retrieved from Stego image without knowing the algorithms and the values of parameters used

1. INTRODUCTION

With the fast development of internet and technology life [1] and advancement of image purports, the difficulty of protecting secrecy of such purports through the network has become a main apprehension in the recent years. Using effective image retrieval techniques, the intruders constantly attempt to access relevant image content [2] before launching a surprise attack using image malware [3, 4].So, the field of data and multimedia secrecy has become very important and the field of its applications is extending [5]. Various ways were utilized to maintain the message through transportation like ciphering and steganography [6]. Ciphering is the process of transforming the sensitive information into unintelligible format but with observable existence via cipher algorithms [7]. The scrambled information in an unreadable format can be indicated to as encrypted message, whereas the genuine mystery text is recognized as normal message. In cryptography, there are two steps: ciphering and deciphering. Ciphering changes original message to encrypt message by stratifying an appropriate encryption method at the dispatcher aspect. While deciphering performs the opposite of encryption, turning encrypted message to original message at the recipient aspect. The network hacker might still make an attempt to change the encryption message to plain text. Additionally, the frequency of offensive on the web has no decreased because the adversary might readily deduce that the network is carrying some sensitive information. [8,9]. Data hiding is the actual tendency for safe connection [10], it is the procedure of hiding mystery data inside a media wanting alteration its perceptual quality [8,11]. The significant method which is utilized in concealment is steganography [12]. Steganography conceals the secret message into an carrier (digital media) while preserving the un predestine existence of mystery message [13,14]. Images, videos, audio, and other types of digital media are all possible. Cover media is the name given to the original digital media. Stego-media is the name for the form of media that conceals sensitive information. It is important to keep the Stego media's quality high so that it doesn't alert any unauthorized users to any hidden information. [15], therefore, in order to increase communication security, steganography is consequently important for many computer applications [9]. The cover image, hidden message, Stego image and Stego Key are the primary elements of the steganography data concealment strategy. [16, 17]. The original image that contains the hidden message [18] is called a cover image. The cover media may be a still image or a video in several formats, including digital devices [19], server or chat programs [20]. Secret message refers to the text that the transmitter inserts in the carrier image to create the Stego image and transmits to the receiving end across an unsafe connection path

[16],any file type, including text, images, audio files, and videos, can be used for the hidden message. A voluntary motif that perhaps employed to strengthen the secrecy of the data

concealment is the encryption key. [21]. Stego image is the primarily carrier media that includes the mystery data hidden [22]. Stego Key may refer to a key or to the algorithm used to embed or retrieve the secret message [23]. The hidden message is concealed inside the cover image created by the sender using an embedding method. The receiver side receives the Stego media. The mystery text is extractor from the Stego media on a receiver's side using an extraction technique [22,24]. The fundamental benefit of steganography is the ability to hide information in image with a way that a human visual system cannot see, making it challenging to retrieve information without knowing the proper steps [25]. In order to carry out image steganography, a variety of techniques are available. These methods have either been developed in a spatial (SD)or transformed domain (TD) [26]. Using (SD) methods that forth right hide the bits of the mystery textin original image's pixel is the simplest way to conceal the pixels of the mystery image in (LSBs) of the cover image's pixel [27]. Other spatial domain techniques (PVD) [28] and (EMD) [29]. Generally, the spatial steganography method has minimal computing complexity, a reasonably high embedding capacity, and is easy to apply [30]. The original image will be altered by using (DCT) or (DWT), while the hidden image will be inserted by modulating coefficients in the relevant domain in the modified domain (DFT) [27]. The spatial domain system is more vulnerable to attacks than the transform domain method. As opposed to that, it has a high computational time complexity and offers less room for message embedding. Any stenographic scheme must meet the following four crucial evaluation criteria: payload, quality, robustness, and embedding effectiveness [2]. The quantity of information that is encoded within the carrier media is indicated by the payload, which is also known as capacity. On the other hand, the quality of the Stego image is crucial for imperceptibility, which determines whether the genuine carrier media and the mystery data could be distinguished [31]. The term robustness refers to the ability to withstand various types of attacks, hacker attacks, and other intrusion-related manipulations. The number of cover pixel modifications required for a specific embedding rate is known as the embedding efficiency [2].

2. RELATED WORK

A lot of data hiding approaches for telemedicine applications and other fields have been proposed in the past decade. In this section, the literature review of the existing works has been done. Kich et al. in [32] suggested a novel method that replicated the hidden information in the edge pixels. It was based on over-segmenting images using Modified Simple Linear Iterative Clustering, which allowed for the split of each image into a set of K regions known as a super pixel. The approach was superior in terms of embedding ability and imperceptibility, according to experimental results. The primary drawback of this strategy was the fact that it wasn't secure against all kinds of Stego analysis assaults. Dube et al. in [33] proposed a revolutionary edge-based Steganography technique where the images' sharp edge areas were utilized to merely conceal the data. For this, the image was divided into groups of two pixels each, and the variation in pixel values between those groups was noted. The combination was utilized to conceal the data if this difference exceeded a predetermined value. Compared to previous LSB and PVD techniques, this method produced better results, and enhanced the Stego image's quality. This approach was unable to resist off outside Stego attacks. Gujjunoori et al. [34] suggested a reversible edge detection and data embedding method based on difference expansion (DE). The DER scheme, DER layer-2 scheme, and DEED scheme were the three suggested schemes that were used. Despite the simplicity of the approach, the payload and PSNR were low and complexity was substantial. Suneetha [35] the method of Canny edge detection was utilized. The key was retrieved after the message had been encoded using encryption methods. Its edge image was obtained in order to conceal this key in the cover image. From this edge image, Fibonacci pixels were chosen. Then, these edge pixels were used to conceal the encryption key. Fibonacci calculations added complexity to the process, which resulted in decreased PSNR. Wang et al. in [36] proposed an approach to increase the ability for health care images that scramble a cover image using the logistic map

before embedding the data while preserving the image's seed points (ROI). It is manually excluded before to the embedding operation, and an adaptive embedding approach is used to conceal sensitive information inside the cover image utilizing the usual four least significant bits (4 LSB) of the cover image. Puteaux et al, [37] suggested a reversible data concealing approach utilizing two methods depend on correction error prediction and linear chaotic method to cipher pixels of cover image by utilizing a reserved room before encryption and vacating room after encryption principles. The authors utilized MSB concealing in the encrypted domain to avoid LSB attacks, and they achieved superior image quality with a high capacity on selected gray image only and does not use color images. Kordov and Stoyanov [38] suggested a new least significant bit stenography method depend on a Hitzl-Zele chaotic map to hide text in color images. They embedded three bits of the input sequence into the LSB of three-channel RGB and score a good visual image results compared with others similar methods but not mention to different geometric attacks analysis Elkamchouchi et al. [39] proposed a method for concealing an 8-bit grayscale image. In order to facilitate insertion, writers use both 1D and 2D chaotic maps for time-consuming and attack-robustness inside 24-bit true-color images in the selected spatial domain. To embed the hidden image in one or more LSBs on the chosen color channel, they used the red channel from the cover image's RGB color model. The authors only discussed the fundamental image quality metrics PSNR and MSE; other evaluations, such as SSIM, correlation degree, etc., are essential for higher perceptual quality

3. EDGE DETECTION

As the point where rapid changes in intensity value occur, the edge is realized as the disparities in intensities. Where the brightness of the image varies significantly between segments, the pixel values are recognized. The human visible system is extra critical to the sleek regions than the edge regions. The alteration in the edge regions are not visible because it has higher randomization properties. Canny, Sobel and laplace of gaussian (LoG) are the most often used edge detectors (ED) [25].

3.1 (LoG) for edge detector

Recognizing target outlines inside an image and grouping the pixels into edge and non-edge classes are the main tasks of the(ED) in the scope of image operation. Edges, which may be thought of as a collection of interconnected curve lines, are nothing more than an abrupt change in discontinuity of the density values of image's pixel. Numerous edge detectors, including Prewitt, Canny, Sobel, and (LoG), among others, have been proposed over the years [40]. Because pixels are extremely sensitive to noise, the Sobel and Prewitt operators' drawback is erroneous results for the edge area. Similar to this, the Canny operator deals with complicated calculations and false zero crossing. The (LoG) uses gaussian smoothing with a bigger sigma's value and has the noise invariant property. Additionally, the LoG operator tests a larger area surrounding the pixel and locates edges with greater accuracy. The Laplacian approach uses the second derivative of the image to determine edges by looking for zero crossings. The Laplacian is a metric of an image's second order spatial derivation that can be used to locate edges and other areas of abrupt change.. Due of the Laplacian filter's high sensitivity to noise in edge detection, Gaussian smoothing is added before Laplacian to mitigate its effects. The LoG operation is the name of this two-step procedure. The LaplacianL(z,y) for the image's pixel intensity values I(z,y) is as follows:

$$L(z, y) = \frac{\partial^2 I}{\partial z^2} + \frac{\partial^2 I}{\partial y^2} \quad \ldots \ldots \ldots \ldots \ldots (1)$$

There are various methods for locating a roughly discrete convolution kernel that approximates the Laplacian's effect. One potential kernel is

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

It is referred to as a negative Laplacian because the focalsalient is negatory. By switching the components' signs, the positive Laplacian can be established. The Laplace and Gaussian equations can be used to create the smoothing Gaussian filter as follows:

$$LoG(x,y) = -\frac{1}{\pi\sigma^2}\left[1 - \frac{x^2 + y^2}{2\sigma^2}\right]e^{-\frac{x^2+y^2}{2\sigma^2}} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

The image's homogenous area results in LoG being zero. The LoG now responds positively on the murkierpart and negatively on the illuminationpart when change happens. The response is zero distance away, positive to one.negative to the other, and zero distance away from the edge itself when two regions are separated by a sharp edge [8].

4. SHARK SMELL OPTIMIZATION ALGORITHM (SSO)

The shark smell optimization approach, which was developed in 2014 and can be regarded as one of the best optimization tools [41]. It was modeled after the way sharks naturally seek for prey in the ocean. A shark is an apex predator with a keen sense of smell that allows it to find even the smallest amount of blood in the vast ocean. The keen noses are capable of quickly identifying the smell's source. Consequently, allow the shark to turn toward the location of possible prey. The shark's body has lateral lines that allow it to sense any pulses or vibrations made by its prey in the water. The ability of sharks to detect their prey and capture it is what allows them to survive in the ocean. Similar to PSO, SSO provides a straightforward formula that only needs the shark's updated position and velocity. The concentration of the damaged prey's odor has a significant impact on how the shark moves. This indicates that the shark will move ahead and rotate in order to approach an area with a higher concentration of the odor. With the advent of local search, searching has become more precise and effective. In addition, it is simple to include the algorithm into software. As a result, SSO method outperforms all previous algorithms. The SSO algorithm has so far been utilized in a broadscope of implementation such as the power, medical, and energy systems. In addition, it has undergone minor changes in a few editions to enhance its functionality. Sharks are noted for their foraging movements of forward and rotation, which enable them become a dominant predator in the ocean. They also have an excellent sense of smell. The initiation of the traditional SSO method starts when a shark looks for injured prey inside of a randomly generated initial position of the shark. One blood source is assumed to exist for each wounded prey. The current situation can be stated as follows:

$$x_i^l = [x_1^1, x_1^2, \ldots\ldots, x_1^{NP}] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

When a shark detects the smell of blood, it moves with a particular velocity that is determined by:

$$v_i^l = \left[x_1^{i,1}, x_1^{i,2}, \ldots\ldots, x_1^{i,ND}\right] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

When a shark detects a lot of blood odor, its speed rises. As a result, it is possible to conceptualize the smell concentration as a tendency of the optimization objective function. The gradient of this objective function is used to alter the velocity.

$$v_i^k = \eta k. R1. \frac{\delta(OF)}{\delta x_j} \mid x_i^k, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Where $j = 1, \ldots, ND,\ i = 1, \ldots, NP,\ k = 1, \ldots, kmax$. The ND indicates number of decision variables of the optimization problem, *NP* is population size and $kmax$ is number of iteration. Shark quickens at a particular velocity submissive to adormancyrestriction

$$v_i^k = \eta k. R1. \nabla(OF) \left| x_i^k + a_k. R2 . v_{i,j}^{k-1} \right. \ldots \ldots (6)$$

$a_k$is momentum rate. R1 and R2 in random number, the following equation describes a velocity limiter that restricts shark acceleration::

$$\left| v_i^k \right| = min\left[\left| \eta k. R1. \nabla(OF) \left| x_i^k + a_k. R2 . v_{i,j}^{k-1} \right| \right., \left| \beta_k . v_{i,j}^{k-1} \right| \right] \ldots \ldots (7)$$

βk is velocity limiter. The updated position of shark in forwarding motion is determined by:

$$Y_i^{k+1} = X_i^k + V_i^k . \nabla t_k \ldots \ldots (8)$$

Where $Y_i^{k+1}$is the new shark's location and $\nabla t_k$is time interval.On the contrary, when looking for a better candidate solution, sharks also use a circular motion for a local seeking at everyphase. The formula is provided by:

$$Z_i^{k+1,m} = Y_i^{k+1} + R_3 . Y_i^{k+1} \ldots \ldots (9)$$

Where $m = 1, \ldots$, $Mi = 1, \ldots, NP,\ k = 1, \ldots, kmax$. Where R_3 a random number and M is the overall spots in local seeking in rotational motion and m is the number of every rotation grade. When joining M spotsbesetment local seeking, a close contour as rotational motion of shark can be acquired. The next location of sharks is chosen depend on the better location gainedamidst forward motion, Y_i^{k+1} and rotational motion, $Z_i^{k+1,m}$until reach kmax [42]. The algorithm of SSO is summarized in algorithm (1)

```
Begin
Step1: Initialization
    Set parameters NP, ,, αk , βk , ( k = 1,2 … kmax )
    Generate individual's initial population
    Generate each decision variable randomly
    Initialize the stage counter k = 1
    For k = 1 :kmax
Step2: Forward movement
    Calculate the updated velocity vector.
    Gain new location of shark depend on the forward movement.
Step3: Rotational movement
    Obtain position of shark based on rotational movement,
Z_i^{k+1,m}(m = 1, … ,)
    Select next the best location of shark depend on the two movements, rotational
and forward movements.
    End for k
    Set k = k + 1
Step 3. Best position
Choose the best location of shark depend on the optimum objective function in the
last step of iteration.
End
```

Algorithm (1): SSO algorithm

5. SUGGESTED APPROACH

In this part, an effective approach for hiding the mystery information in the edges of the given cover media by using shark smell optimization is proposed by using java language. The proposed algorithm has 2 various parts, the transmitter' part and the recipient' part and comprises of three phases which are: edge detection, information hiding (embedding) and message extractor. The block scheme of the suggested method is displays in Figure (1)

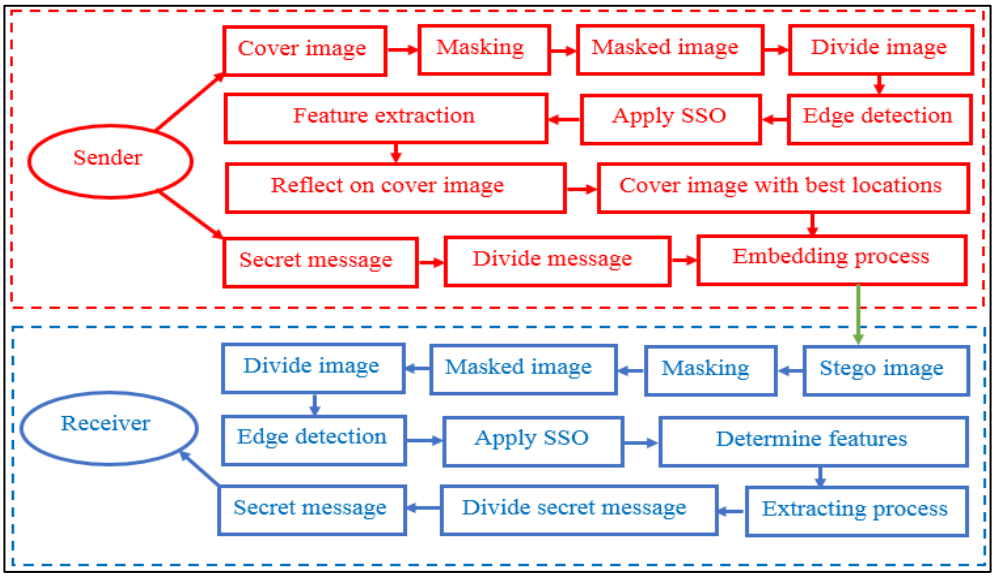


Figure 1: Block scheme of the suggested approach

5.1 Masking and divided image phase

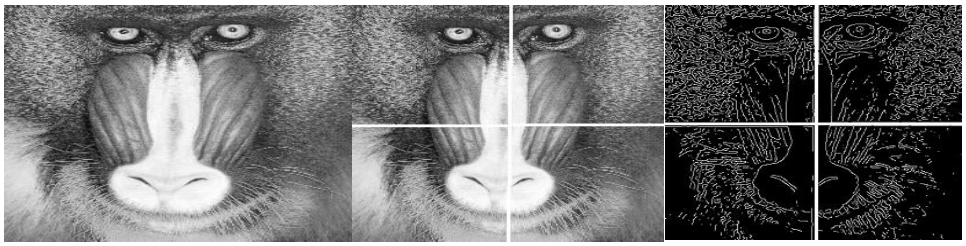
In order not to change the pixel values of the cover image and implement the hiding steps a mask of the cover image (CI)is taken and then divided it into four parts. Where a set of operations is performed on this temporary image (masked image) and the results of those operations are projected onto the cover image, where the main goal of dividing the image into four sections is to facilitate apply edge detection and sso algorithms on the image, reduce complexity and increase security

5.2 Edge detection phase

Edges, which can be described as a collection of interconnected curve lines, are nothing more than the abrupt change in discontinuities of the density pixels, values. Due to the human visual system's limitations in identifying differences in the edge region, the edges of the cover media are appropriate regions for hiding information, the original media (CI) is separated into four non-superposition blocks. To construct edges image, LoG is enforced on a four blocks masked image (MI) instead of the four block cover image (CI). A non-edge pixel cannot withstand as many embedding bits as an edge pixel can. The proper selection of the threshold value which directly affects how the edge detection procedure turns out and is the main element of edge detection in this case. If the threshold value is set very small, several thick and fake edges will be produced. On the opposite hand, many edges might not even be detected if the threshold value selected is very big and the detected edges might be excessively segmented. To ensure hide all bits of secret message a high value of the threshold was chosen then it is iteratively decreased until number of edges are greater or equal to bits of secret message. Next, whole of the traced edges' positions are identified. Coinciding to every of the edge position value discovered, mystery message bits is embedded in pixels of cover media staying at that specific position by executing the suggested embedding method. During this stage, it is made sure that no more edge data will be stored when secret bits are inserted into the CI's pixel data.

Consequently, the payload grows significantly without sacrificing the goodness of stego image. Figure 2 displays the cover media with dividing them to four sections and extracting their edges. Algorithm (2) shows the steps of split (MI) and its edge detection

(a) Lena image (a) Divided of lena(a) Edges detection of lena



(b) Baboon image (b) Divided of baboon (b) Edges detection of baboon

Pepper image (c) Divided of pepper (c) Edges detection of pepper (c)

(d) Boat image (d) Divided of boat(d) Edges detection of boat

(e) Airplane image (e) Divided of airplane (e) Edges detection of airplane

Figure 2: Divided and edges detection of cover images

Input cover image (CI)
Output edge image (EI)

Begin
Step1: read cover image (CI)
Step2: Perform pre-processing on the cover image (CI) to gain the (MI)
Step3: divide the (MI) into 2X2 non-overlapping blocks as (O), (M), (A) and (R)
Step3: determine edge of (O), (M), (A) and (R) blocks based on the variations in the values of its pixels
Step4: determine corner pixels of blocks (O), (M), (A) and (R) based on its intensity
Step5: set threshold (Ts) value based on the edges number (En) of (MI) and bits secret number (BSn) Where (BSn) < (En), where (Ts) used to control the number of edge pixels
Step6: apply fuzzy detector on (O), (M), (A) and (R)
Step7: get edge region blocks (FO), (FM), (FA) and (FR)

End

Algorithm (2): Steps of edge detection phase

5.3 Apply SSO and embedding phase

In this stage, the process of hiding a mystery text into the cover media is disputed.

- Firstly, secrecy data is changed into binary form and then split into four sections equally so that each section is hidden in a different section of the cover image.
- Secondly, store the edge pixels of the (EI) with its physical address of four block that determined by the LoG in a two-dimensional array (search spaces) as (Omn), (Mmn), (Amn), (Rmn) and (Pmn) for the physical address.
- Thirdly, find the fitness value of each pixels and the best (optimal) pixel for each of the four blocks based on fitness function.
- Fourthly, after the distinctive positions were determined by the shark smell optimization, these positions are assigned (reflect) onto the cover image in order to be used to hide secret data using least significant bit technique. After completing the process of hiding in the four blocks, these blocks are merged together and the stego image is obtained.

One of the major donating of the suggested method is chosen the positions of the optimal pixels in the all search spaces for the hiding procedure. This paper suggests the fitness function of the shark smell optimization to select the pixel location. The suggested fitness function based on the variance between optimal pixel and other pixels, entropy, and intensity of the seed points. The calculation of the variance, entropy, and intensity based on the mean of the adjacent seed points of the shark. Algorithm (2) shows the steps of embedding phase

Input edge region blocks (FO), (FM), (FA), (FR), secret message (Sm)
Output stego image (Si)

Begin

Step1: set parameters NP, ,, αk , βk , (k = 1,2 … $kmax$) of SSO
Step2: convert (Sm) into binary form (BSm)
Step3: divided the (BSm) into four equal parts (p1,p2,p3,p4)
Step4: store the blocks (FO), (FM), (FA) and (FR) in 2-D array (search spaces) as (FOA), (FMA), (FAA) and (FRA)
Step5: store the physical pixels address of each four blocks in two- dimension array as (PPA)
Step6: determine the number of pixels needed to hide the binary message
Step7: generate individual's initial population of SSO
Step8: assign one SSO for each (FOA), (FMA), (FAA) and (FRA)
Step9: determine the start point of each SSO in the (FOA, FMA, FAA, FRA)
Step10: define fitness function (Fn), where (Fn) = (intensity (I) + entropy (E) + variance (V))/3
Step11: rest LSB of each pixels
Step12: find best pixel in each (FOA), (FMA), (FAA) and (FRA) based on fitness function where variance equal to zero
Step13: find fitness values by apply SSO and using fitness function
Step14: update velocity, forward movement, rotational movement of SSO of each block
Step15: Repeat steps 10-14 until the optimal location (pixels) to achieve hiding gets selected
Step16: reflect the selected optimal pixels on the (CI) based on (PPA)
Step 17: divide secret message into four part
Step18: embed each part of secret message in the optimal pixels of (p1,p2,p3,p4) of the (CI) by using LSB technique
Step19: get Stego image

End

Algorithm (3): Steps of embedding phase

5.4 Extraction phase

The Stego and cover media have the same width, height and size of bits, without knowing the embedded algorithm, the recovered Stego image cannot be decoded. The extractor procedure is the opposite of the concealing procedure, the details of this phase is shown in algorithm (4)

Input stego image
Output secret message

Begin

Step1: read stego image
Step2: set parameters NP, ,, αk , βk , (k = 1,2 … $kmax$) of SSO
Step3: get four blocks (FO), (FM), (FA), (FR) from stego image
Step4: apply LoG edge detector on four blocks
Step5: store (FO), (FM), (FA) and (FR) in 2-D array (search spaces) as (FOA), (FMA), (FAA) and (FRA)
Step6: store the physical pixels addresses of each four blocks in two- dimension array as (PPA)
Step7: Generate individual's initial population of SSO
Step8: assign one SSO for each (FOA), (FMA), (FAA), (FRA)
Step9: determine the start point of each SSO in the (FOA), (FMA), (FAA) and (FRA)
Step10: define fitness function (Fn), where (Fn) = (intensity (I) + entropy (E) + variance (V))/3
Step11: rest LSB of each pixels
Step12: find best pixel in each (FOA), (FMA), (FAA), (FRA) based on fitness function where variance equal to zero
Step13: find fitness values by apply SSO on (FOA), (FMA), (FAA), (FRA) based on fitness function
Step14: update velocity, forward movement, rotational movement of the SSO of each block
Step15: Repeat steps 10-14 until selected all embedding positions
Step16: reflect the selected positions on the stego image based on (PPA)
Step17: extract secret message from each blocks by using LSB technique
Step18: aggregate secret message from blocks
Step19: get secret message

End

Algorithm (4): Steps of extracting phase

6. RESULTS

Two widely accepted criteria, namely payload and Stego-image quality, have been considered so as to examine the effectiveness of the proposed system. The payload metric reveals how many hidden bits are concealed in each pixel of the original media of distance M x N, also the (PSNR) (MSE), correlation coefficient (CC), unified averaged changing intensity (UCAI), embedding capacity (payload), Entropy, and histogram have all been utilized to examine the goodness of a stego media. Five benchmark grayscale images with a dimension of 512 x 512 were utilizedto conduct the experiment. Figure (2) displays set of cover media, divide cover image and edge cover image of the "Lena", "Baboon", "Pepper", "Boat" and Airplane. As a result of the variation in image pixels, the number of edge pixels varies from one cover media to other. To visually examine the differences in pixel distribution between the original and stego images, histograms are used. In Figure (3) the histograms of the cover media and stego media are contrasted where the displayed the histograms' pixel distribution is similar and there is not discernible various amidst the original and Stego media.

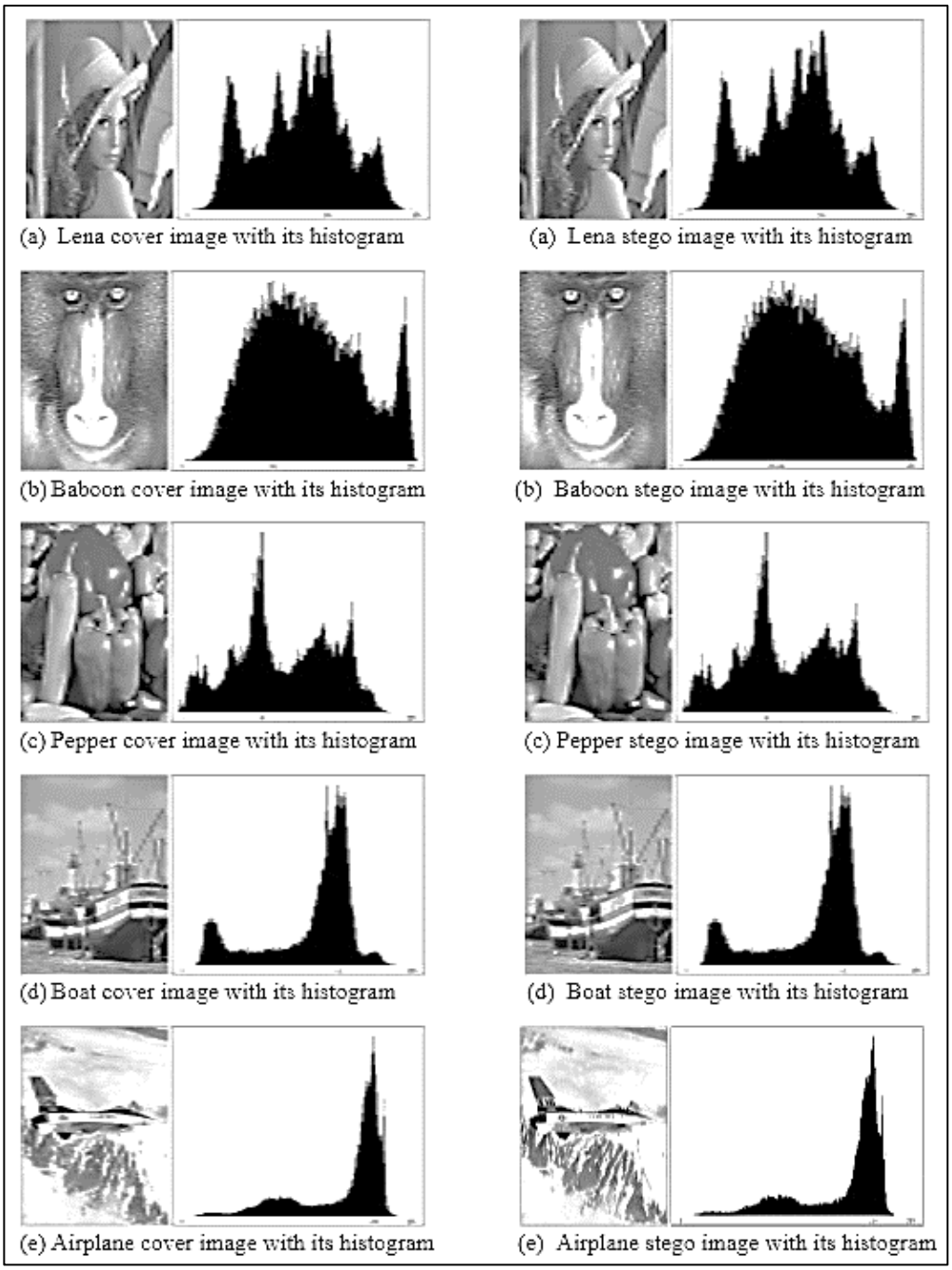


Figure 3: Cover images before and after divided and edges detection

The (PSNR) is calculated to gauge the visual goodness between the original media and Stego media. The larger PSNR value reference to best goodness of stego media while reverse reference to deformation, while the MSE represents the quality of the Stego media and it is smaller value reference to lower error rate. Correlation coefficient (CC) is a technique for promotion the grade of eventuality that a linear relation subsists amidst two menstruation amounts where the (CC) has the value equal to one when the two images are conformable, and the value equal to zero when two images not conformable. The UCAI test calculates the average intensity change amidst plain media and a Stego media also used to analyze and test

the Stego image resistance against differential attacks. The concealing payloadis measurement by the utmost number of concealing bitsper pixel (BPP). Entropy is use to assessment the amount data of an image and to contrast the difference of data of plain media and Stego media. Table (1) shows the results of the measures that were applied on five images in evaluating the proposed system. The results proved the strength and effectiveness of the proposed system

Table 1: Metric results

image	MSE	PSNR	CC	UACI	Entropy
Lena	0.6512	49.99	0.999868	0.04170	5.22209
Baboon	0.7763	49.23	0.999843	0.04330	5.22212
Pepper	1.0353	47.97	0.999790	0.04998	5.22219
Airplane	0.9824	48.20	0.999801	0.04816	5.22214
Boat	0.8433	48.87	0.999829	0.04498	5.22213

The effectiveness of the suggested approach is contrasted with another approaches [43, 44, 45, 46, 47] in idioms of capacity and PSNR on 'Lena', 'Baboon', 'Pepper'' images which have been outlined in table 2 and figure (4). Where the suggested approachrealizedbestoutcomes than another approaches, where it could hide more bits of information with decreased image fineness castration. Nevertheless, the entire PSNR values guarantee that the stego-mediagoodness deviation is very low and that watcher cannot readily distinguish amidst the cover media and the stego media

Table 2: Compare between suggested approach and other approaches

Methods	C & PSNR	Lena image	Baboon image	Pepper image
Arham et al. [43]	C	0.74	0.72	0.74
	PSNR	42.06	31.68	38.63
Wang et al. [44]	C	0.74	0.72	0.74
	PSNR	44.8	31.33	39.82
Parah et al. [45]	C	0.75	0.75	0.75
	PSNR	46.36	46.37	46.12
Parah et al. [46]	C	0.75	0.75	0.75
	PSNR	46.37	46.37	46.38
Govind et al [47]	C	0.75	0.75	0.75
	PSNR	48.01	48.21	47.69
Proposed method	C	0.75	0.75	0.75
	PSNR	49.99	49.23	47.97

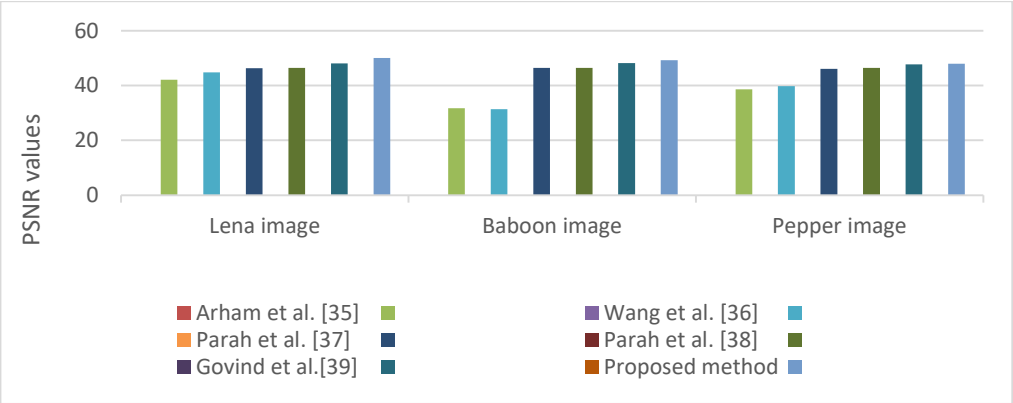


Figure 4: comparison between proposed method and other methods in the terms of PSNR and payload

7. CONCLUSION

In this paper the steganography is executed using LoG and SSO algorithm, where the original image is disintegrated into four parts. LoG is applied on each block for finding edge areas, where hiding the secret message in severe edges causes minimal castration in compare to the sleek regions. SSO technique is used to fine the better pixels location in the edge area to hide the mystery information. The aim of using LoG algorithm is to raise the payload capability that can preserve the goodness of imperceptibility, while the aim of using SSO and divided the cover image into four parts is enhance the goodness of Stego media and raise the security where the secret message cannot be retrieved from the Stego image without knowing the algorithm used and its parameters. The empirical outcomes display that the suggested method do best results in idioms of PSNR, MES, UACI, CC, histogram and entropy also it confirm the efficacy of the suggested approach above some other approaches in idioms of payload and Stego-image goodness also enhance the concealing capability with an admit domain of imperceptibility, robustness and security.

REFERENCE

[1] B. T. Ahmed and O. Y. Abdulhameed, "Fingerprint recognition based on shark smell optimization and genetic algorithm," International Journal of Advances in Intelligent Informatics, Vol. 6, No. 2, , pp. 123-134, https://doi.org/10.26555/ijain.v6i2.502, July 2020.

[2] A. Rezaei , L. Farzinvash and A. Farzamnia, " A Novel Steganography Algorithm using Edge Detection and MPC Algorithm," 16th International ISC Conference on Information Security and Cryptology, https://doi.org//10.1109/ISCISC48546.2019.8985150. 2019.

[3] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K.-H.Jung, "Image steganography in spatial domain: A survey," Signal Process. Image Commun., vol. 65, pp. 46–66, Jul. 2018.

[4] S. Sun,"A novel edge based image steganography with 2k correction and Huffman encoding", Inform. Process.Lett., vol. 116, no. 2, pp.93-99. 2016.

[5] A. A. Abdulla, H. Sellahewa and S. A. Jassim, "Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-019-7166-7.2019.

[6] O. Y. Abdulhammed, "A novel approach of steganography by using strong edge detection and chaos theory," Multimedia Tools and Applications. https://doi.org/10.1007/s11042-022-12643-3. 2022.

[7] O. Y. Abdulhammed, "strengthening steganography by using crow search algorithm of fingerprint image," Eastern-European Journal of Enterprise Technologies. DOI: 10.15587/1729-4061.2020.200282. 2020.

[8] S. K. Ghosal, J. K. Mandal and R. Sarkar, " High payload image steganography based on Laplacian of Gaussian (LoG) edge detector," Multimed Tools Appl, https://doi.org/10.1007/s11042-018-6126-y.2018.

[9] D. K. Sarmah , A. J. Kulkarni, "Image Steganography Capacity Improvement Using Cohort Intelligence and Modified Multi-Random Start Local Search Methods," Arab J Sci Eng, DOI 10.1007/s13369-017-2751-4.2017.

[10] Y. Alsalhi, " An accurate and high-efficient Qu Bits steganography scheme based on hybrid neural networks," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-018-7061-7. 2019.

[11] M. Suresh , S. Sam, "Optimal wavelet transform using Oppositional Grey Wolf Optimization for video steganography," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-020-09330-6.202.0

[12] C. Pac , J. Kim , K. An ,C. Kim , K. Kim , C. Pac, "A novel color image LSB steganography using improved 1D chaotic map," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-019-08103-0.2019.

[13] I. J. Kadhim , P. Premaratne , P. J. Vial and B. Halloran, "Comprehensive survey of image steganography: techniques, evaluations, and trends in future research," Neurocomputing 335:299–326. 2019.

[14] M. Hussain , Q. Riaz , S. Saleem , A. Ghafoor and K. Jung, " Enhanced adaptive data hiding method using LSB and pixel value differencing," Multimedia Tools and Applications https://doi.org/10.1007/s11042-021-10652-2. 2021.

[15] S. Mukhopadhyay ,S. Hossain, S. K. Ghosal and R. Sarkar, "Secured image steganography based on Catalan transform," Multimedia Tools and Applications, 80:14495–14520, https://doi.org/10.1007/s11042-020-10424-4. 2021.

[16] A. Nilizadeh,W. Mazurczyk, C. Zou and G. T. Leavens, "Information hiding in RGB images using an improved matrix pattern approach,". In: 2017 IEEE Conference on computer vision and pattern recognition workshops (CVPRW). IEEE, pp 1407–1415.2017.

[17] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," Multimed Tools Appl, 1–17.2019.

[18] P. Marwaha and P. Marwaha,"Visual cryptographic steganography in images," In: 2010 Second international conference on computing, communication and networking technologies. IEEE, pp 1–6. 2010.

[19] W. Mazurczyk and L. Caviglione"Steganography in modern smartphones and mitigation techniques," IEEE CommunSurv Tutor 17(1):334–357. 2014.
[20] J. Lu ,G. Zhou , C. Yang ,Z. Li and M. Lan, "Steganalysis of content-adaptive steganography based on massive datasets pre-classification and feature selection,". IEEE Access 7:21702–21711. 2019.
[21] M. A. Salama, M. F. M. Mursi and M. Aly, "Safeguarding images over insecure channel using master key visual cryptopgraphy,". Ain Shams Eng J 9(4):3001–3013. 2018.
[22] A. Cheddad , J. Condell , K. Curran and P. Mc Kevitt,"Digital image steganography: survey and analysis of current methods,". Signal Process 90(3):727–752.2010
[23] M. Hussain and M. Hussain, "A survey of image steganography techniques," Int J Adv Sci Techno 54:113–124. 2013.
[24] A. AbdelRaouf "A new data hiding approach for image steganography based on visual color sensitivity," Multimedia Tools and Applications https://doi.org/10.1007/s11042-020-10224-w. 2021.
[25] C. Vanmath and S. Prabu, "Image Steganography Using Fuzzy Logic and Chaotic for Large Payload and High Imperceptibility," Int. J. Fuzzy Syst. https://doi.org/10.1007/s40815-017-0420-0. 2017.
[26] A. Cheddad,J. Condell , K. Curran and P. M. Kevitt , "Digital image steganography: survey and analysis of current methods,". Signal Process 90:727–752. 2010.
[27] A. Banharnsakun, "Artificial bee colony approach for enhancing LSB based image steganography," Multimed Tools Applhttps://doi.org/10.1007/s11042-018-5933-5. 2018.
[28] A. K. Sahu and G. Swain G, "An optimal information hiding approach based on pixel value differencing and Modulus function,".WirelPersCommun 108:159–174. https://doi.org/10.1007/s11277-019-06393-z. 2019.
[29] C. Qin, C-C.Chang andT-J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images," Multimedia Tools Appl 74:5861–5872. https://doi.org/10.1007/ s11042-014-1894-5. 2015.
[30] Z. Hui andQ. Zhou Q, "A novel high payload steganography scheme based on absolute moment block truncation coding," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-020-09015-0. 2020
[31] S. I. Nipanikar, V. H. Deepthi and N. Kulkarni N, "A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform," Alexandria Engineering Journal, https://doi.org/10.1016/j.aej.2017.09.005. 2017.
[32] I Kich, ., EAmeeur and Y. Taouil "Image steganography based on edge detection algorithm".International conference on electronics, control, optimization and computer science (ICECOCS). Kenitra,Morocco.2018.
[33] R.R. Dube, M.A. Lalkot." Improved edge based steganography scheme for GrayScale images in spatial Domain". International Journal of Science and Research (IJSR) 5(6):1976–1978. 2016.
[34] S.Gujjunoori, M. Oruganti, "Difference expansion based reversible data embedding and edgedetection"Multimed Tools Appl 78:25889–25917. 2019.
[35] D.S Kumar, R. Kiran," Data hiding using Fibonacci EDGE based steganography for cloud data". Int JAppl Eng Res 12(16):5565–5569. 2017.
[36] D. Wang, D. Chen, B. Ma, L. Xu, J. Zhang,"A highcapacityspatial domain data hiding scheme formedicalimages". J Sign Process Syst, Springer Science +business Media New York. https://doi.org/10.1007/s11265-016-1169-7. 2016.
[37] U. Puteaux, W. Puech," An efficient MSB prediction-based method for high-capacity reversible datahiding in encrypted images". IEEE Transactions on Information Forensics and Security. https://doi.org/10. 1109/TIFS.2018.2799381. 2018.
[38] K. Kordov, B. Stoyanov, "Least significant bit steganography using Hitzl-Zele chaoticmap". International of electronics and telecommunications 63(4):417–422. https://doi.org/10.1515/eletel-2017-0061. 2017.
[39] H. Elkamchouchi, W. M. Salama and Y.Abouelseoud,"Data hiding in a digital cover image using chaotic maps and LSB technique".https://doi.org/10.1109/ICCES.2017.8275302.2017.
[40] H. W. Tseng and H. S. Leng, "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion," IET Image Process 8:647–654. 2014.
[41] B. T. Ahmed and O. Y. Abdulhameed, "Fingerprint Authentication using Shark Smell Optimization Algorithm," UHD Journal of Science and Technology, https://doi.org/10.21928/uhdjst. v4n2y2020.pp28-39. 2020
[42] N. A. Kamarzaman, S. I. Sulaiman and I. R. Ibrahim, "Adaptive Mechanism For Enhanced Performance Of Shark Smell Optimization," Journal Of Electrical And Electronic Systems Research, https://doi.org/10.24191/jeesr.v18i1.002. 2020.
[43] A. Arham ,H. A. Nugroho and T. B. Adji TB, "Multiple layer data hiding scheme based on difference expansion of quad," Signal Process 137:52–62. https://doi.org/10.1016/j.sigpro.2017.02.001. 2017.
[44] W. Wang, J. Ye, T. Wang and W. Wang,"A high capacity reversible data hiding scheme based on right-left shift," Signal Process 150:102–115. https://doi.org/10.1016/j.sigpro.2018.04.008. 2018.
[45] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan and G. M. Bhat, "A new reversible and high capacity data hiding technique for E-healthcare applications,"Multimedia Tools Appl 76(3):3943–3975. https://doi.org/ 10.1007/s11042-016-4196-2. 2016.
[46] S. A. Parah, F. Ahad, J. A. Sheikh and G. Bhat, "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique," J Biomed Inform 66:214–230. https://doi.org/10.1016/j.jbi.2017.01.006. 2017.
[47] P. V. Govind, B. M. Varghese, M. V. Judy, "A high imperceptible data hiding technique using quorum function," Multimedia Tools and Applications, https://doi.org/10.1007/s11042-021-10780-9. 2021.