March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

Performance Analysis on Various Heuristic Approaches Based on the Image Steganography Quality Improvement

1 Smitha.G.L., and 2 Dr.E.Baburaj
1 Research Scholar,Dept of CSE,Sathyabamauniversity,Chennai
2 Dept of CSE,Marian Engineering College, Trivandrum

Article Info
Volume 83
Page Number: 6901 - 6912
Publication Issue:
March - April 2020

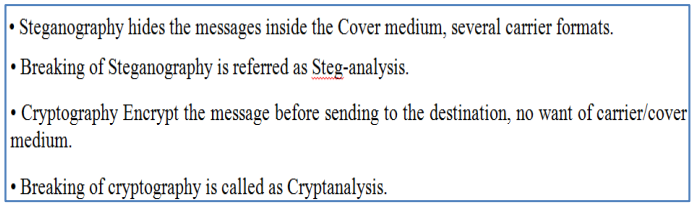
Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 05 April 2020*

Abstract:
Of all the various techniques, Image steganography is one such technique which is employed to broadcast a secret message on the internet. It secures the entire illegal client's private data. Steganography is a process that conceals a text data into a picture in which no one recognizes the subsistence of hidden data. Previously a variety of research works projects many techniques for data covering an image. However, the correctness attained is not ideal when the picture gets recreated. Same time, the accuracy of the image steganography is placing the secret message at right location of the cover image. Moreover, this paper prefers an enhanced method between different heuristic also me metaheuristic procedures applied for steganography. The techniques utilized in this paper for concealing data in the best possible position of the hidden picture are Genetic Algorithm (GA), Artificial Immune System (AIS), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) and Artificial Bee Colony (ABC) also they are recreated most favorably. Within MATLAB software entire procedures are researched. Thus the attained results are proved; furthermore they are evaluated among each other in tenures of picture excellence before and after data concealing also they are recreated correspondingly.

Keywords: *Steganography, Picture processing, Data Concealing, Surreptitious Data Transmission, Heuristic Procedures.*

I. INTRODUCTION

The word steganography derived from Greek words "STEGOS," it means to cover, and “GRAFIA” means writing [1], finally it means that covered writing. The process of steganography is hiding knowledge entirely in any multimedia data like image, video, and audio. This paper focused on hiding data on models. Steganography is a great and essential task of secret communication. It embeds secret message in an image, and it is invisible. The base image called the cover image, and the text is going to insert is steg-medium. The base data called cover-image, cover-text, and cover-audio. A stego-key used for employing the hiding, encoding and decoding processes to restrict the embedded data [2]. Steganography is differing from cryptography [3], by:



Similarly, fingerprint and watermarking are accompanying with steganography are usually in need of intellectual property protection. Embedding digital information in noise-tolerant signal information like image and audio data is called as digital watermarking. Watermarking leads to identifies the ownership of the cover image. A kind of signature embedded in the watermarking where the property of the data can ensure the copyright protection. In fingerprinting, numerous and exactsymbols embedded in the prints of the work that severalclients are supposed to get. In this circumstance, it is effortless for the stuff owner to get out such customers who contribute themselves the correct to violate their

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

authorizing authority when they illegally permit the property to other groups [1], [4]. The proposed techniques utilize various image-processing systems to detect locations in the cover image. Different optimization algorithms are applied to do steganography on cover images to determine optimal locations. The exact locations have browbeaten for embedding secret bits.

In this paper, it is aimed to decide a better suitable method for image steganography by applying and experiment various optimization methods, and the results verified. The entire contribution of the paper is:

• Read the input image, remove the noise and enhance the image.

• Optimal position on the cover image is obtained using GA

• Optimal place on the cover image is captured using AIS

• Optimal location on the cover image is obtained using PSO

• Optimal position on the cover image is obtained using ABC and

• Optimal place on the cover image is captured using ACO

• Experiment and evaluate the performance of the above methods by comparing the results. From the results choose the better approach for image steganography.

The following section provides a survey on various earlier approaches used in steganography to understand the problems faced. Also, it helps to understand the difficulties statement and create a new method for the image-steganography process.

II. Related Works

There are various algorithms studied here to understand the problems faced while steganography. The behavior and the results of the algorithms are depending on the file format. One of the excellent steganography method based on palette image discussed by the authors in [5], where it called "EZ Stego" system. It is used to embed and hide text messages by manipulating color palette. The limitation of EZ Stego system is, it rearranges the palettes before embedding, there will be a color adjust problem created, and it is not time effective. Also, due the palette is repositioned, there will be no drastic change in color. The authors in [6] proposed a steganography method where it chooses the pixels randomly and embeds. For all the selected pixels, the palette searches a closet color. The color of the random pixels has a same parity to the secret bit. Finally, the real color value replaced by the chosen color, and the parity is calculated using the following equation as:

$$P = (R + G + B) \oplus 2$$

But the color values of the cover image will not be original when recovering the secret message. The author in [7] proposed manipulating quantization process, whereas it makes a lot of data loss. To avoid data loss, authors in [6] used lossy compression method with more robust regarding specific image processing manipulations. To increase the efficiency in lossy compression, the authors in [8] proposed secret message transmission on internet based on the Joint Photographic Experts Group (JPEG) file format. This file formats use primarily discrete cosine transform (DCT) to accomplish the compression [5]. DCT process applied after splitting the images into blocks such as 8 x 8 pixels. Apart from these methods, so many approaches proposed for steganography such as Synonyms embedding [9], short message services (SMS) [10]. Secret messages replaced by synonyms of the words in other languages like Chinese, called as Efficient Substitution methods (ESM), High Efficient Substitution Method (HESM) [11], character substitution methods in [12], Least Significant Bit (LSB) [14] based steganography, Most Significant Bit (MSB) [15] found steganography and zero-overhead for hiding secret information in [13] proposed. Though there is a lack of time, recovery and cost.

2.1 Limitations of the Existing Research Works

From the literature survey and other approaches presented in other resources like digital libraries, it identified that there are various issues were faced in the existing systems like accuracy in cover image recovery, placing the secret image on the cover images, time of setting and cost. Also, the maximum size of the embedded data compared to the total data, and it is making sure the message is hidden and how much image/sound distortion is tolerable before the word lost in the noises. Size and protection are the other problems in steganography. Sending more padding around the secret messages is necessary. Hence the secret message doesn't stand out. Length of the hidden message is the next problem.

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

2.2 Problem Statement and Motivation

Steganography is a significant and essential task which requires networking based secret data transmission. In steganography, the hidden message doesn't stand out. The confidential message transmission is straightforward and practically undetectable. But it should ensure that the secret message cannot be stealing by any third party people. Also in recent days, due to the advancement of networking and digital images' format, it is necessary to develop an enhanced steganography method for the internet. This problem considered, and this paper motivated to design and implements an optimized secret message hiding in a cover image following the image format. There are various optimization algorithms are used in multiple earlier research works for an optimal placing of the mysterious picture on the cover image. The complete functionalities of this paper are illustrated in Figure-1 and Figure-2.

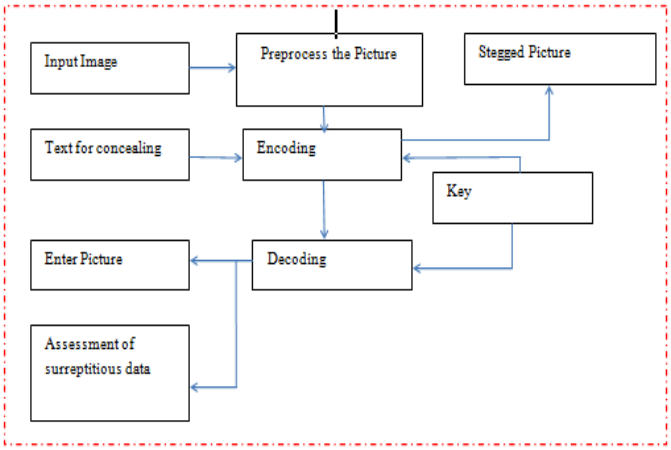


Figure-1: Overall Architecture

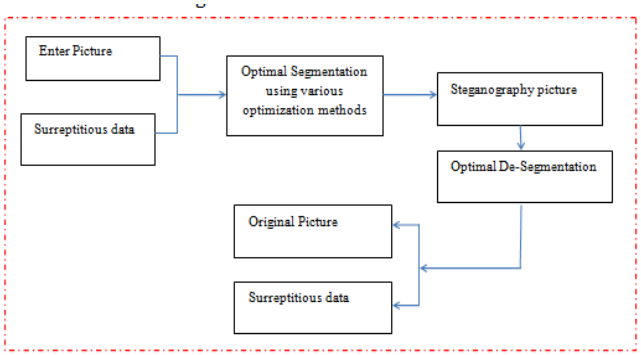


Figure-2: Heuristic Procedure Based Steganography

III. Proposed Embedding Procedure

A novel procedure represented for picture steganography for surmounting the competence flaw contrasted toward additional techniques similar to the one projected in [16].There are five optimization algorithms are used as a component of the host image to accomplish the objectives of this paper. Initially, to achieve this objective, we utilize an artificialimmune system algorithm also an element of the host picture by dividing the host picture into n-blocks of volume$\boldsymbol{w \times h}$ pixels.Embedding is sluggish, once the size of private data is enormous. This procedure prolonged while we employ meta-heuristic algorithms intended for discovering the optimal solution for embedding. To surmount this hitch, we exploit a component of host picture$\boldsymbol{p}$alsore volume thesurreptitiousdata$\boldsymbol{r}$so that the proportion of host picture pixel bits to hidden data bits even the percentage of $\boldsymbol{p}$pixel bits to r bits existidentically. The segmentedpicture divided into n-blocks $\boldsymbol{w \times h}$ pixels. Consider$\boldsymbol{C}$as a hosted picturein the volume of $\boldsymbol{w \times h}$ also$\boldsymbol{M}$ is a private data. Subsequently we divide$\boldsymbol{C}$ into $\boldsymbol{H/h \times W/w}$ blocks$\boldsymbol{C_{ij}}$ $\boldsymbol{(1 \leq i \leq H/h, 1 \leq j \leq W/w)}$ by$\boldsymbol{w \times h}$ pixels. We're volume$\boldsymbol{M}$ to $\boldsymbol{w_r \times h_r}$pixels also name it r. Furthermore, $\boldsymbol{M}$ is divided into *n*-blocks $\boldsymbol{m_{ij}(1 \leq i \leq H/h, 1 \leq j \leq W/w)}$ by$\boldsymbol{w_r \times h_r}$ pixel for embed algorithm.

Allow $\boldsymbol{C}$tobe the host picture of $\boldsymbol{n}$blocks $\boldsymbol{c_{k,t}}$through $\boldsymbol{w \times h}$ pixels in which $\boldsymbol{M}$ is employed as surreptitious databy$\boldsymbol{n}$blocks $\boldsymbol{m_{ij}}$ amid $\boldsymbol{w_r \times h_r}$ pixels also $\boldsymbol{r}$ re volume $\boldsymbol{M}$ by $\boldsymbol{w_r \times h_r}$pixels. Subsequently, we select a block $\boldsymbol{C_{ij}}$ so that it is the major component of host picture for AIS period. Consequently, we explicate the AIS, embedding and extorting period.

3.1 AIS Based Image Steganography

For picture steganography, a well-organized algorithm is represented in this paper based on Artificial Immune System (AIS) and host picture divider.A block of host picture is opt for our projected techniqueandutilizes AIS for discovering the optimalpattern also for embedding the message bits in the host picture pixels. As a result, our techniquediscovers the optimalpattern for quick embedding.

3.1.1 Artificial Immune System

The artificial immune system identifies the unknown materials which penetrate into the body. During the recent years, the field of Artificial Immune system (AIS)

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

has boomed [17-18]. The artificial immune system gets motivated by the perceptions of the human immune system to respond computational hitches also various studies have explained that AIS is a competent algorithm for discovering best possible hitch. AIS seek out a populace of antibodies for a possible solution gap, each of which is an encoded solution. A value allocated to every antibody and its condition is named based upon the presentation. An enhanced antibody acquires the maximum strength. The procedures entailed in AIS are decided, the clone also manic transformation. The manic transformations machinists in AIS are extremely significant as they modify the antibodies. Figure 1 depicts the machinists of AIS and explains the phases of AIS.

1. Initialization: AIS constraints for example populace volume, selection speed, and clonal speed also transformation speed are initialized. These constraints are clarified below:

a. Populace volume: the number of antibodies which toils in each creation.

b. Selection speed: the number of optimal antibodies which decided for clone machinist.

c. Clonal speed: this constraint is amid 0 and 1 which is employed to obtain the number of clones and antibody

d. Transformation Speed: this constraint is between 0 and 1 which is the possibility of a specified characteristic that will be transformed.

e. End: this constraint is amid 0 and 1 which is utilized for end algorithm.

2. Creation of original populace of antibodies erratically.

3. After embed volume ding surreptitious volume picture in a host picture block, the fitness rate is computed based on PSNR.

4. Based on selection speed the optimized antibodies are decided

5. Clone the decided antibodies from 4: the whole amount of clones created from an antibody is acquired in Equation:

$$\boldsymbol{round}\,(\boldsymbol{clonal-rate}\times\boldsymbol{populaiton}\\ -\boldsymbol{rate}\times\left(\frac{\boldsymbol{populationsize}-\boldsymbol{i}+\mathbf{1}}{\boldsymbol{populationsize}}\right)$$

In which $\boldsymbol{i}$ specifies the $\boldsymbol{i^{th}}$ maximum fitness antibody in populace and round(.) is the machinist that rounds its case. Therefore, antibodies with greatest fitness rates have the huge amount of clones.

6. Manic Transformation: the cloned antibody will be transformed. By altering the rate of certain bits, every clone will be transformed to discover its fellow feasible solutions. The amount of transferred bits is evaluated in an equation:

$$\boldsymbol{e^{-|Mutation-rate\times f|}}$$

In which $\boldsymbol{f}$ is the strength of an antibody standardized.

7. End state: the end state of this algorithm denotes the dissimilarity of standard existing populace strength also standard final populace strength is lesser than End constraint.

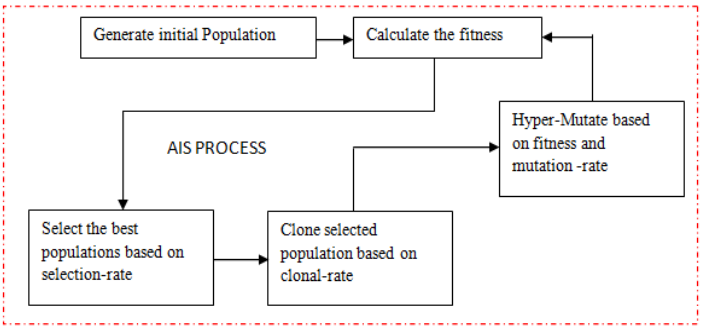


Figure-3: Block Diagram of Artificial Immune System

3.1.2 AIS phase

Initially, the antibodies presentations are illustrated furthermore, based on the block form in figure 2,the method of discovering the optimum antibody for embed period is shown.

3.1.2.1 Antibody presentation

Let us deem an antibody with 7 components. As the route of pixel examining has 16 feasible positions. Therefore we present it as a component by 4 bits span. For everyone, preliminary area is presented as two components together with bits X-offset also Y-offset by 4 bits span based on the volume of block $\boldsymbol{c_{ij}}$. In [19], 8 bits are deemed for X-offset along by 8 bits which are believed for Y-offset. Least Significant Bit (LSB) planes are employed for Bit-Planes embedded in host pixels that are suitable for integrating the private data in host picture pixels. In Table-I available rates for Bit-Planes are illustrated. SB-Pole is utilized to resolve surreptitious Bits-Pole, SB-Dire is exploited to decide the route of

hidden data bits also the final component is BP-Dire which specifies the direction of LSB planes. Additional data of the final three components are shown in Table II. We could divide components in two unique sets, along with the accessible components in antibody. The primary set holds the components which indicate the introduction position of surreptitious data bits in host picture pixels. Also the second comprises of the components which generate certain modifications on secret data, to acclimatize more by the host picture.

3.1.2.2 Embedding Procedure

For locating the optimum antibody, the projected technique employs AIS. PSNR is utilized for manipulating the strength of an antibody also for manipulating PSNR we should embedrintoc_ij. The flowchart illustrated in Figure -4 integrates *r* into $\boldsymbol{c_{ij}}$ pixels. In the first phase, once$\boldsymbol{c_{ij}}$, is arranged, $\boldsymbol{r}$as well as the equivalent antibody, pixel bits are acquired by the component of the antibody. Based on comparable components (explicitly SB-Dire also SB-Pole) $\boldsymbol{r}$is furthermore changed to the surreptitious bits series. Subsequently, the number of pixel bits and surreptitious bits are contrasted as every pixel bits merely hold back one surreptitious bit. The connected antibody cannot in corporate$\boldsymbol{r}$into $\boldsymbol{c_{ij}}$if the amount of surreptitious bits is greater than pixel bits, following this the antibody is also immunizedlsoeverysurreptitious bit is embed into equivalent pixel bit, and finally the PSNR is evaluated.

3.1.2.3 Embedding phase

After AIS phase, we encompass the optimum antibody also surreptitious data $\boldsymbol{M}$is embedding into host picture $\boldsymbol{C}$based on the optimum antibody. To embed thedata, we introduce every block of surreptitious data $\boldsymbol{m_{k,t}}$ into anequivalent host picture block $\boldsymbol{c_{k,t}}$ based on the optimum antibody which was established in the AIS phase.

3.1.2.4 Extracting phase

Figure-5 depicts the block figure of removal procedure of the projected technique. For removing surreptitious information, from the existing pixel bits the employed antibody is also extorted the component is divided. Subsequently, theStego message $\boldsymbol{S}$ is divided into *n*-blocks $\boldsymbol{w \times h}$ pixels. The pixel bits series is acquired; along with the components of an antibody, it also accomplishes the unprocessedsurreptitious bits series by utilizing this. Based on antibody components we attain the last series of surreptitious bits moreover it creates the surreptitious picture consequently.

In our projected technique, we seek to surmount competence flaws of additional techniques employed in meta-heuristic algorithms. We compute the proportion of the amount of bit data to the number of pixel bits that are desired for embedding based on Bit-Plane component of feasible results also enhances feasible results if sufficient bits per pixel is not taken, the Bit-Planes are placed in an appropriate rate. For picture steganography, the projected process is an approximation algorithm. Based on evolutionary algorithms, the optimum antibody $\boldsymbol{Y}$ is obtained on a block of host picture $\boldsymbol{c_{ij}}$ also re volume the surreptitious data $\boldsymbol{r}$. In this technique we enhance competence and reserve rate, deem a block $\boldsymbol{c_{ij}}$of host picture with re volume surreptitious data $\boldsymbol{r}$, thus, based on request and condition we could alter the volume of host picture block and re volume surreptitious picture *r*. It is extremely significant that if the feature is optimum, we could utilize the entire pixels of host picture and surreptitious picture for acquiring the optimum antibody $\boldsymbol{Y}$; furthermore, there is a swapping among the optimum feature and obtaining maximum competence in chronological programming. At this juncture, we re-volume surreptitious picture as we need to seize a variety of bits rate to find a prototype with the optimum solution $\boldsymbol{Y}$ to employ in entire blocks of host pictures.

3.2 PSO based Image steganography

This paper proposed a technique for picture steganography by utilizing sparse presentation, Particle Swarm Optimization (PSO) as the next optimization technique, is employed for deciding proficient pixels intended for the function of embedding the surreptitious audio indication in the picture. PSO-based pixel series method exploits fitness utility which depends upon the rate utility

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

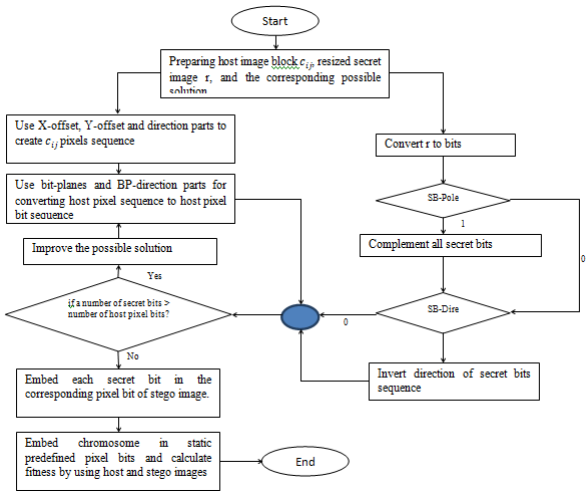


Figure-4: Flowchart of embedding r into c_{ij}

For calculating fitness, this rate utility estimates the rim, entropy, also the strength of the pixel. A model has created also the PSO is contrasted with the additional subsisting techniques in tenures of Peak-Signal-to- Noise-Ratio (PSNR) along with Mean Square Error (MSE) furthermore it concludes the projected PSO, as an efficient technique

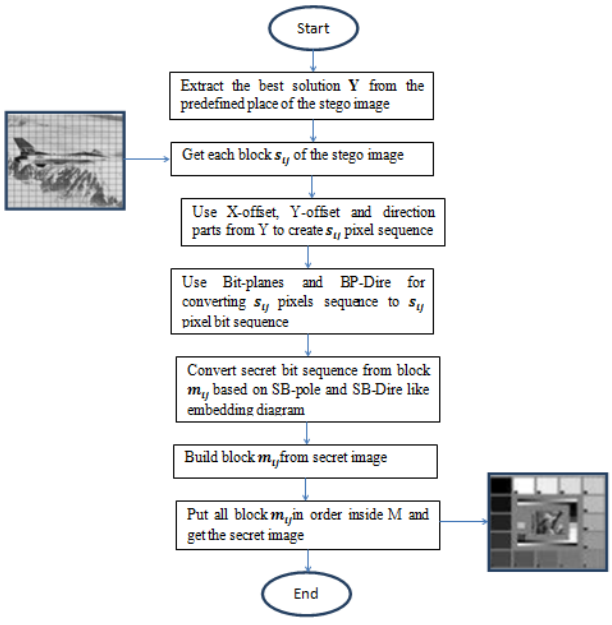


Figure-5: Removal procedure of the projected technique

Correspondingly, this projected technique accomplishes anoptimum47.6 dB PSNR rate also 0.75MSE rate.PSO–based pixel range for strength estimation: Deciding the location for the best possible pixel in embeds method is a major input to this research. This paper projects the rate utility for the PSO algorithm for deciding the pixel location also this utility depends on rim, entropy, also the strength of the kernel positions. The estimation of the rim, entropy, also strength depends on the mean of the adjoining kernel positions of the component.

Through the projected PSO algorithm the Steganographic study of the picture is represented. The steganography picture grants exceptional protection moreover ability in defending the surreptitious data from being concealed. The sparse technique is utilized for enhancing the protection of the image. In figure1the block diagrams illustrate the projected techniques. The picture steganography accomplishesthe projected representation in two procedures such as (1) also embedalso (2) the removal. Picture embedding needsthe cover pictureas well as the surreptitious speech indication.

In this research, the PSO algorithm finds the best possible location of the pixel [20]. Based upon the populace PSO is a stochastic optimization algorithm. This algorithm executes the startup procedurewith the arbitraryrange of components. Moreover it seeks the best possible solutionduring the locationrevise of entire components. Based upon the fitness utility this algorithm primarilyopts for the populaceerraticallyalso revises the location of entirecomponents in the populace.Subsequently, the overall optimumlocation gets recognized and revised to endure embedding.

Step 1: Startup Procedure

Let n be the amount of populace known as$\boldsymbol{P} = \{\boldsymbol{P_1}, \boldsymbol{P_2}, \dots, \boldsymbol{P_n}\}$there in the dimensional region of volume$\boldsymbol{X} \times \boldsymbol{Y}$. Every population transmits various components and hence, establishes the location also the related speed of entire components presented in $\boldsymbol{X} \times \boldsymbol{Y}$ dimensional region during the random range of the populace.

Step 2: Fitness Estimation

Step 3: Resolve the best possibleresult

Step 4: Revise the location

Step 5: Iteration

3.3 ABC algorithm based picture steganography

The primary purpose of the projected research is that it

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

resolves the best possible rates also the information's are embedded. IWT, as well as ABC algorithm, is utilized in this projected technique, in which the primary process is to interpret the color picture also the information that is required to hide. Integer Wavelet transform is executed upon color modules of the picture, the ABC algorithm is employe din addition to these altered coefficients, and it is termed as Artificial Bee Colony Algorithm to discover the optimal rate for concealing information. The fitness of the projected technique is exhibited through research which is executed upon surreptitious data also the test pictures provides the excellent visual feature with high embed information capability.

The projected work is executed in this segment. In this technique, primarily interpret surreptitious data, place in the color picture as a cover picture also from this color picture, remove R,G, and B modules. Subsequently, Integer wavelet transform pertains separately upon these components. Thirdly, with these altered modules, ABC algorithm is utilized to resolve best possible pixel rate for information embed. Fourthly, the information is translated to ASCII rate also embedded by best possible positions. Once embedded, Inverse IWT is at last executed to acquire stego picture on the dispatcher side. Upon the recipient side, the information is removed from stego picture during the reverse procedure of embed method. Figure 2 illustrates the flowchart for the projected technique.

3.3.1 Projected Algorithm

The subsequent algorithm is utilized to embed surreptitious information in a cover picture.

Input: Cover picture, manuscript file
Output: Stego picture
Step 1: Interpretkey in color picture alsosurreptitiousinformation to be concealed.
Step 2: Color picture is divided into R, G, B color group also the IWT has pertained to the entire color groupindividually.
Step 3: Artificial Bee Colony optimization (ABC) algorithm is employed to discover the best possiblepositions where the information gets concealed.
Step 4: Surreptitiousinformation is translated into ASCII rates.
Step 5: Information is concealedat the best possible solution.
Step 6: Subsequently, Inverse IWT is pertained to acquire stegopicture. The subsequent algorithm is employed to remove surreptitious information from a stegopicture.
Step 6: key instego picture
Step 7: Information is removed by a pertaining reverse process of embed method.
Step 8: Acquire surreptitious data from the cover picture.

3.4 GA Based Image Steganography

Based on the Darwinian laws of endurance and replication (Goldberg 1989), the Genetic algorithm is a method for exploring the best possible solution. The GA processes populace of genetic materials (entity), which reinstate one populace by another consecutively.

The genetic material in the GA is often seized in binary program. In the exploring gap, every genetic material presents an aspirant key. The GA frequentlyrequires a fitness utility to allocate a gain (fitness) to everygenetic material in the existing populace. The GA starts with initializing a population of individuals by guess. The entities progress during iterations termed generations. In every generation, every entity is estimated next to the fitness utility. Genetic machinists are employed for entities in the populace to create a subsequent generation of entities. The procedure is maintained until some condition sare met (for instance, certain strength is met) [21].

STEP 1: Encrypt the surreptitiousdata

STEP 2: Create random populace of volume L

(L=length of the SurreptitiousData) with everyentitycomponent having n genetic materials

(Appropriate solutions for the hitch)

STEP 3: [Fitness] Estimate the fitness f(x) of every genetic material entity in the populace

STEP 4: [Novel populace] Generate a novel populace by replicating subsequent steps until novel populace is absolute i.

[Deciding] Decide two blood relations from the populace with the optimum fitness point (the enhanced fitness, the betterpossibility to be decided)

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

ii. [Crossover] through a crossover possibility, cross over the blood relations to form novel progeny (children). If the crossover is not executed, progeny is a precisephotocopy of blood relations.

iii. [Mutation] with a mutation possibility, mutate novel progeny at every locus (position in genetic material).

iv. [Recognizing] position novelprogeny in a novel populace

STEP 5: [Replace] Creation of novel populace is employedfor additional usage of the algorithm; the case is the entire amount of characters enclosed in the surreptitious data. This populace, which is a position of random amounts, is created from the rates that would drop among the recognized least and highest rates.

The entities are clustered as a collection of genetic materials. To create two progeny, the two entities with the maximum fitness utility will crossover. The two progeny will endure mutation, and thenmight be allocated a fitness rate before re-opening into the populace. From the populace, the two smallest amountentities will be removed, asthe unique populacevolumeisrequired to be sustained. This will prolong until a best possible solution is acquired.

IV. Fitness Function

To obtain the entities that are good in shape, set machinists (i.e., Intersection A∩B) are employed to contrast the ASCII rates (components) which are the surreptitiousdata among those enclosed within the entities. The more values (elements) of the secret message contained in an individual, the higher the fitness function.

V. Mutation

Mutation procedure is utilized to set up scarce genetic materials to the populace. This is accomplished by exploiting the set machinist (such as,disparity) A-B: components in A which are not in B. In this phase B is the union of entirerates enclosed in eachentity in the populace. Also A is the rate in the surreptitiousdata. This is completed to obtain the scarce genetic materials that will be initiated to createprogeny. Erratically a genetic material in the created progeny will also be opted alternated using scarce genetic material. Everyprogeny is mutated before it isforeword to the populace. To make sure that the two minimum entities are not removed by genetic materials which are required for locating the best possible solution, set disparityprocedure is re pertained to obtain the scarce genetic material, [22].

3.5 ACO based Image Steganography

There are several methods in steganography, for example, LSB, are the usual techniques to embed information while the start of the picture; initially pixels are taken in order. This usual technique requires certain intellectual algorithms to provide more power also resistance so that they cannot be destroyed by any of the invaders. ACO is one kind of intellectual algorithm which is employed to improve picture steganography. This algorithm along with steganography tries to offer various benefits:

1. Reduced rate of MSE.

2. The high rate of PSNR.

3. Excess utilization of similar cover.

4. Additionalresistancemoreoverhitches in steg examination.

There are two algorithms employed in this segment such as ACO (ACS and MMAS). ACS also MMAS utilizes the similar method to conceal the surreptitious data. To identify which algorithm generates minimal MSE and maximal PSNR the results produced from ACS and MMAS are evaluated.To discover the best pixels, the applied techniques dependupon ACO algorithms designed for the Traveling Salesman Problem (TSP). The objective of utilizing ACO using TSP is to discover the shortest path to accomplish the target. The projected structure has blocks thathold the number of pixels.ACO algorithms are employed to locate a series of the best pixelinside a block by discovering the connection of colors among pixels. The entire procedure of the ACO algorithm is given below.

1- From the cover picture the blocks are decided.

2-A block encloses a series of pixels.

3-Source alsotarget,moreoverentire tour are decided erratically.

4- Merely once every pixelis visited.

5- To discover the best pixels among the connections

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

this process is employed.

The subsequentprocedures are the conditionwhichisoffered to ACO:

1. In sequence, cover picture is separated into blocks as seen in figure 2.The projected structure employs blocks (2*2) also (5*5).

2. Competence of a cover picture is discoveredby the number of blocks also the amount of surreptitiousdata bits;

Step1: Interpretsurreptitiousdataalsostack cover picture
Step2: w= amount of surreptitiousdata bits
Step3: ww = cover picture. breadth* cover picture .altitude
Step4: competence= ww / amount of pixel inside the block
Step5: IF competence> w then
Exit Utility
Else
Stackone more cover picture
End IF
Step6: Go to step3

3. Embedding surreptitiousdata bits, here is a procedure to embed surreptitiousdata bits in cover:

Single bit following the separation of the cover picture in blocks (n*n), there are the amount of pixels in the singleblock; single bit of the surreptitious data is embedded in each pixels blocks.

For instance (1), Assume the blocks are (2 * 2), Amount of pixels =4, Surreptitious data bit=1, 0, 0, 1 moreover persist until the conclusion of the surreptitious data bits. These steps are essential in step 4.

4. Heuristic calculation: this calculation is evaluatedby discovering MSE amongunique pixels after embedding the single bit of the surreptitiousdata as specified in equation (3):

= Eq. (3)

5. Amount of pixels in single block (n*n): utilization of blocks (2*2) also (5*5).

6. Amount of ants: Ant=3

7. The ants decide the pixels erratically in all the iteration.

8. Amount of iterations =5

9. Primary pheromone (Pher) = 0.1

10. Beta also Alpha = 2

11. Pheromone max (pherMax) = 10 and Pheromone min (pherMin) = 0.01 (pherMax , pherMin for deciding the highest alsolowest rates for pheromone track while utilizing MMAS). The advantageofpherMax also pherMinwhichrevise the pheromone tracknevergo beyond pherMax also pherMin.

12. In the productivityfolder the best pixels are accumulated.

All the above five algorithms are implemented and experimented in MATLAB software, and the results are verified. To evaluate the performance the Mean Square Error and PSNR values are calculated and compared. Also, the performance can be evaluated by changing the size of the images such as W and H.

Experimental Results and Discussion

Common to all the optimization algorithms the optimization parameter values are assigned and experimented and it is given in Table-1.A set of images associated with MATLAB image library are taken for experiment, and the implemented program is executed. All the five algorithms are executed separately, and the results are verified regarding output images and MSE, PSNR. The MSE and PSNR of all the images are calculated using the above-discussed optimization algorithms, and the obtained results are given in the following tables.

Table-1: Parameters and their values used in the experiment

Parameter	Value
Population Size	100
Selection rate	20
Mutation rate	.05
Replacement rate	20%
End	0.001
W	512
H	512

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

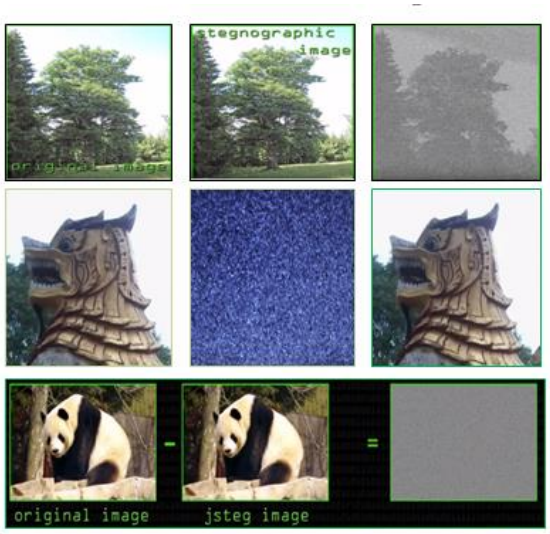


Figure -6: Results Obtained from Steganographic Method

Figure-6 shows the various input images, Stego images and after steganography process. Based on the width and height of the cover images, the embedding process provides the PSNR and time complexity. The size of the cover images and the block images are changed, and the results verified. The MSE and PSNR of the image are calculated using the following equations as:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right)$$

Where M and N are the numbers of rows and columns of the image. Here it is depicted the above said two parameters which determine the image quality. The quality of the images before and after steganography process is depending on the MSE and PSNR parameters. MSE determines the poor quality and PSNR determines the high quality of the image.

Table-2: Comparison of PSNR values obtained from the experiment

Secret Image (256×256)	PSNR (dB)					
	Stego image (512×512)	AIS w=h=512	ABO W=h=512	PSO W=h=512	GA W=h=512	ACO W=h=512
	Lena	45.12	71.59	**77.80**	38.23	50.94
	Jet	45.54	72.01	**78.22**	38.65	51.36
	Pepper	45.19	71.66	**77.87**	38.30	51.01
	Sailboat	45.26	71.73	**77.94**	37.17	51.08
	Baboon	45.43	71.90	**80.03**	38.54	51.25

The performance of the PSO is compared with the existing models, such as AIS, ABC, GA, ACO algorithms. By comparing the results, the PSO has outperformed the other existing models.

To determine the quality of image PSNR is used. If the image has high PSNR value, it indicates that the image has good quality. From the table, we infer that PSO produces the high PSNR value for the given Stego images. For Lena image PSO gives the 77.80 PSNR value, for Jet image PSO gives the 78.22 PSNR value, for pepper image it gives 77.87 PSNR value, for sailboat it gives 77.94 PSNR value, and for baboon image it gives 80.03 PSNR value which is higher than other methods. It has been analyzed that the difference of PSNR values from PSO and ABC 7%, PSO and ACO is 27%, PSO and AIS is 33%, and for PSO and GA is 40%. Here to notify that the ABC also produces the high values than other suggested methods. The difference value is about 7% only. Next to PSO method, ABC method is also outperforming with other methods

Table-3: Comparison of Compilation Time Complexity

Stego image (512×512)	Computation time				
	AIS	ABC	PSO	GA	ACO
Lena	0.37	0.32	0.28	0.49	0.41
Jet	0.40	0.31	0.31	0.51	0.45
Pepper	0.36	0.30	0.26	0.48	0.42
Sailboat	0.41	0.33	0.33	0.50	0.43
Baboon	0.42	0.32	0.28	0.50	0.42

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

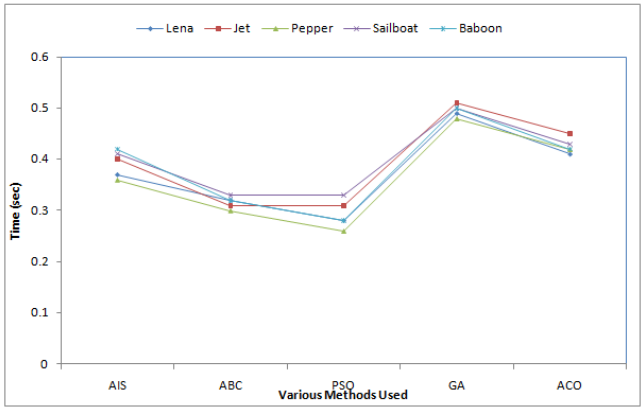


Figure-7: Performance Evaluation based on Time Complexity

It is necessary to optimize the Steganographic system; the total computation time for PSO is less when compare to other methods. The traditional algorithms like GA based testing each probable result to get best result which needs high computation time. Table shows that the computation time for AIS, ABC, PSO, GA and ACO. The computation time for GA is almost double than the PSO method. It is observed that ABC method also need less computation time when compare to others and it is given in Table-3 and shown in Figure-7. The computation time can be further improved by using faster computer such as Pentium III PC.

VI. Conclusion

The main objective of this paper is to decide a better suitable method for image steganography. From the problem statement it is initially decided that optimization methods brings more accuracy comparing with the existing methods. So, that this paper utilizes GA, AIS, PSO, ABC and ACO methods for image steganography. All the five methods are experimented and the results are verified in terms of PSNR, where PSNR is calculated from the MSE values. From the obtained result it is clear and noticed that PSO and ABC are decided as better approaches for image steganography. PSO outperforms than the other approaches and then ABC performs better. The loss of data verified is also very less using PSO and ABC. Hence this paper decided and concludes that PSO algorithm can be used for image steganography.

VII. REFERENCES

1. R.Anderson and F. Petitcolas, ”On the limits of steganography” IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
2. Niels Provos, Peter Honeyman, “Hide and Seek: An Introduction to Steganography,” IEEE computer society, 2003.
3. Chi-Kwong Chan, L.M. Cheng ,“Hiding data in images by simple LSB substitution”, Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.
4. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, “Hiding data in images by optimal moderately significant-bit replacement” IEE Electron. Lett. 36 (25) (2000), 20692070.
5. Johnson, N. F., &Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2), pp. 26-34.
6. Fridrich, J. (1999, April). A new steganographic method for palette-based images. In PICS (pp. 285-289).
7. Wang, X., Yao, Z., & Li, C. T. (2005). A palette-based image steganographic method using colourquantisation. In IEEE International Conference on Image Processing.,Vol. 2, pp. 1090.
8. Ashok, J., Raju, Y., Munishankaraiah, S., & Srinivas, K. (2010). Steganography: An overview. International Journal of Engineering Science and Technology, 2(10), pp. 5985-5992.
9. Shirali-Shahreza, M. (2008), “Text steganography by changing words spelling”, In 10th International Conference on Advanced Communication Technology, Vol. 3, pp. 1912-1913.
10. Rafat, K. F. (2009), “Enhanced text steganography in SMS”, In 2nd International Conference on Computer, Control and Communication, pp. 1-6.
11. Sun, X., Meng, P., Ye, Y., & Hang, L. (2010), “ Steganography in Chinese text”, In International Conference on Computer Application and System Modeling, Vol. 8, pp. V8- 651.
12. Changder, S., Ghosh, D., &Debnath, N. C. (2010), “LCS based text steganography through Indian Languages”, In 3rd IEEE International Conference on Computer Science and Information Technology, Vol. 8, pp. 53-57.
13. Shirali-Shahreza, M., &Shirali-Shahreza, S. (2008), “Persian/Arabic Unicode Text Steganography”, In Fourth International Conference on Information Assurance and

March-April 2020
ISSN: 0193-4120 Page No. 6901 - 6912

Security, pp. 62-66.

14. Thangadurai, K., and G. Sudha Devi, (2014), "An analysis of LSB based image steganography techniques", Computer Communication and Informatics (ICCCI), 2014 International Conference on, IEEE, 2014.
15. Islam, AmmadUl, et al. (2016), "An improved image steganography technique based on MSB using bit differencing", Innovative Computing Technology (INTECH), 2016 Sixth International Conference on. IEEE, 2016.
16. RashidyKanan, H., &Nazeri, B, (2014), " A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert systems with applications, 41, 6123-6130.
17. Chang, C.-C, Hsieh, Y.-P., & Lin, C.-H, (2008), "Sharing secrets in stego images with authentication", Pattern Recognition, 41(10), 3130-3137.
18. Wu, C.-C., Kao, S.-J, & Hwang, M. –S, (2011), "A high quality imagesharing with steganography and adaptive authentication scheme",Journalof System and Software, 84(12), 2196- 2207.
19. Fazli, S. &Kiamini, M, (2008), "A high performance steganographicmethod using JPEG and PSO algorithm", In Proceedings of the 12thIEEE International Multitopic Conference, Karachi, 100-105.
20. Fa.hd. Mohsen, MohinyHadhoud, Kamel Mostafa, KhalidAmin, "A new image segmentation method based on particleswarm optimization", Int. Arab J. Inform, Technol. 9 (5) (Sep.2012).
21. Westfeld, Andrew, "F5-a Steganographic algorithm: highcapacity despite better steg-analysis", In Proceedings ofthe 4th Information Hiding Workshop, volume 2137 of LNCS, pages 289-302. Springer, 2001.
22. Yu, Lifang., Zhao, Yao., Ni, Rongrong., and Shi, YunQ, "A high-performance yass-like scheme using randomized big-blocks", In Proceedings of the IEEEInternational Conference on Multimidea& Expo(ICME 2010), 2010.
23. "Text Hiding Using RSA and Blowfish Algorithms with Hash-Based LSB Tecnique", BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE), Vol. 3, Issue 4, pp. 5-12
24. "Heuristic Algorithm on Monte Carlo for Constrained Redundancy Optimization of Complex System", IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET), Vol. 2, Issue 5, pp. 65-72
25. "Hybrid Methodology to Analyze Web User Behavior in Web Mining and Fuzzy Networks", International Journal of Computer Science and Engineering (IJCSE), Vol. 3, Issue 3, pp. 157-166
26. "Initializing Ant (IA) As an Agent in Initializing Population of Genetic Algorithm on Fuzzy Shortest Path", International Journal of Applied Mathematics & Statistical Sciences (IJAMSS), Vol. 4, Issue 1, pp. 17-28
27. "Evaluation of Standard Time with the Application of Rank Positional Weighted Method in the Production Line", IJMPERD, Vol. 7, Issue 2, pp. 73-80
28. "Robust and Secure Pixel Domain Digital Image Steganography", IJMPERD, Vol. 7, Issue 1, pp. 41-52