IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received September 11, 2019, accepted October 8, 2019, date of publication October 25, 2019, date of current version December 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2949622

New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity

A. H. MOHSIN[1,2], A. A. ZAIDAN[1], B. B. ZAIDAN[1], O. S. ALBAHRI[1], A. S. ALBAHRI[3], M. A. ALSALEM[4], K. I. MOHAMMED[1], SHAHAD NIDHAL[5], NAWAR. S. JALOOD[6], ALI NAJM JASIM[7], AND ALI. H. SHAREEF[8]

[1]Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Tanjung Malim 35900, Malaysia
[2]Presidency of Ministries, Establishment of Martyrs, Baghdad 10096, Iraq
[3]Iraqi Commission for Computers and Informatics, Baghdad 10096, Iraq
[4]Department of Management Information System, College of Administration and Economic, University of Mosul, Mosul 41002, Iraq
[5]Department of Computer Technology Engineering, Dijlah University, Baghdad 10022, Iraq
[6]Ministry of Education, Nasiriyah 64001, Iraq
[7]Foundation of Alshuhda, Nasiriyah 64001, Iraq
[8]Department of Computer Science, Computer Science and Mathematics College, University of Thi-Qar, Nasiriyah 64001, Iraq

Corresponding author: B. B. Zaidan (bilalbahaa@fskik.upsi.edu.my)

ABSTRACT Steganography is a form of technology utilised to safeguard secret data during communication in addition to data repository. Numerous researchers have endeavoured to enhance the performance of steganography techniques through the development of an effective algorithm for the selection of the optimal pixel location within the host image for the concealment of secret bits, for the enhancement of the embedding capacity of the secret data, and for maintaining the visual quality of the host image (stego image) in an accepted rate after the concealment of the secret data. Therefore, steganography is perceived as a challenging task. Thus, the current study proposes a new technique for image steganography based on particle swarm optimisation (PSO) algorithm by using pixel selection for the concealment of a secret image in spatial domain, for the purpose of high embedment capacity. The stego possesses a high level of resistance against a steganalytic attack due to the security provided via image steganography. The function of PSO algorithm is to choose an optimal pixel in grey scale host image for the concealment of secret bits, as the PSO has the ability to achieve an efficient fitness calculation that depends on the cost matrix by dividing the host and secret images into four parts. First of all, the secret bits are modified, which are then embedded within the host image. Several locations in the host image are determined through the order of scanning the host pixels and starting point of the scanning for better least significant bits LSBs of each pixel. The PSO algorithm was utilised to ascertain the ideal initiating point and scanning order. Experimental results show that (1) the average peak signal to noise ratio PSNR value in the benchmark technique based on genetic algorithm for five standard stego images is 45.13%, whereas the result obtained from the recommended technique is 56.60%. (2) The proposed technique has an advantage over the benchmark with a percentage of 33.34%, which encompasses all associated issues within the checklist scenario. Therefore, the performance of the recommended technique is superior over existing techniques.

INDEX TERMS High capacity, image steganography, particle swarm optimisation, spatial domain.

I. INTRODUCTION

Information security is basically the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information [1]–[11]. Applications of different domains need a high level of safeguard for private data and cause explosive growth in several fields, including information hiding [6], [12]–[28]. Steganography entails embedding secret data in a host media, such as text, image, audio and video, for the purpose of safeguarding data from detection [29]–[36]. The term steganography is derived from the Greek word 'steganos' denoting 'hidden writing', where unapproved entities are unable to detect or recover secret data [24], [37]–[40]. Steganography

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

has emerged as an important method in the past 20 years as an increasing number of users utilise the Internet and communication networks environments [41]–[45]. Steganography conceals large amounts of data within a host media [46]–[51]. The chosen image for the embedment of secret data is termed as the 'host' or 'cover image', whereas the resulting image with embedded secret data is called the 'stego image' [33], [52]–[55]. Steganography has three goals. Firstly, a large secret data is required; the term 'payload' refers to the size of secret data that may be hidden within a host [56]–[61]. The second goal is resistance to attacks, and the third goal is a high level of security [62]–[68]. Hence, an optimal technique that utilised a host image for concealing secret data should be able to attain two important factors: high visual quality of the stego image and high embedding capacity [69]–[75]. The efficiency of any steganographic technique can be measured using certain engineering metrics, such as peak signal-to-noise ratio (PSNR) and histogram; these metrics evaluate the quality of a stego image [76], [78]–[81]. Moreover, the maximum number of secret data bits that may be concealed within an individual pixel of a host image at bits per pixel (BPP) for the purpose of measuring the concealment capacity of any recommended technique [42], [82]–[87]. The current research recommends a new technique for bit substitution to improve the concealment capacity of the host image without compromising the quality of the stego image and to lessen deterioration as much as possible. In this research, we aim to enhance the suggested steganography technique [88], which had utilised genetic algorithm (GA) for the selection of the optimal pixel position within the host image for embedding the secret bits. Complications occur in the execution of GA due to complicated coding and low convergence speed. However, our recommended technique based on partial swarm optimisation (PSO) algorithm is an evolutionary algorithm and easily executed. PSO has the ability to control its convergence by utilising certain parameters [89].

This algorithm is a computational model that relies on swarm intelligence. In their work, Kennedy and Elbe had improved PSO by simulating social behaviour [52]. Hence, we benefitted from the seeking capability of PSO in choosing the pixels for the optimal embedding data. The remainder of this paper is organised as follows. Section II presents the related works, and Section III comprehensively explains the recommended techniques. Section IV presents the results and discussion. Section V presents the main objectives and contributions. Finally, Section VI provides recommendations for future works and briefly concludes the paper.

II. RELATED WORK

In the current research, we have systematically reviewed and followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses PRISMA style which aims to help authors improve the reporting of systematic reviews and meta-analyses and to explore the existing steganography and related subject matter for the past five years that emphasise high embedding capacity, by searching in the most reliable databases, such as IEEE, Science Direct and Web of Science as in [90]–[98]. This study used advance search option in search engines, with the queries 'steganography', 'stego', 'data hiding', 'high embedding capacity' OR 'high embedding payload'. The preliminary results produced 262 articles. Afterwards, three filters were applied according to certain inclusion criteria [99]–[105]. Thus, the outcome of the query resulted in 93 articles. Next, a full-text reading was performed, where 35 articles were excluded. The remaining 58 articles represent the result of the filtering. However, a limited number of studies focused on metaheuristic-based image steganography. The steganography issues require modelling for search executions and optimisation for the purpose of embedding high payload within the host image, in addition to high visual quality. Some studies applied metaheuristic algorithms as the beginning phase, and particular local heuristics were used to create a set of candidate solutions. Next, these solutions are refined in each iteration according to specific gene criteria, where these genes were discovered in an extensive search space in the primary iterations, then these studies exploit this space with a view of refining the recommended resolution. Nonetheless, in these techniques, each subset of the genes are required to conduct categorisation on repetitively on numerous occasions, and consequently result in high computational expenses and high complexity. Thus, PSO persists to be the optimum technique among the different techniques in choosing the ideal gene location [106]–[110].

Insights drawn from scholarly literature show that efforts have been made to utilise PSO in relation to high embedding capacity in accordance with image steganography. Additionally, [52] had recommended a new steganography technique based on PSO algorithm used for the selection of the embedding area consistent with the size of the secret data, to enable the enhancement of the quality of a stego image via optimal substitution matrix for converting the secret data into the host images. This technique demonstrated a low-level image histogram quality. According to [111] and [112], new techniques were recommended, which are dependent upon the selection of the optimal locations of the host image and the embedment of the secret bits, in which the most significant bits (MSBs) of secret image pixels are used for concealment in the least significant bits (LSBs) of the host image pixels. Here, the capacity of the PSO algorithm is utilised to improve the concealment performance and the visual characteristics of the host image. In addition, [113] and [114] had suggested steganography techniques based on optimised adaptive neural networks for the purpose of removing noise. The application of this technique is utilised for the optimisation of the locations of particles where adaptive finite-element method (AFEM) is utilised to ascertain the estimated resolution of the second-order differential equation (SODE). Moreover, in [115], the steganographic technique was recommended by utilising the wavelet, PSO and least significant algorithms, through the analysis of a secret image into five levels using daubauchi-1 wavelet. In [116], a new embedding technique was recommended for the concealment of a secret audio signal within the host image by using PSO for selection of pixel and wavelet transform. Through [117], a hybrid steganography scheme was recommended, which is composed of a combination of noise visibility function and an optimal chaotic-based encryption scheme, for the purpose of increasing the payload capacity. Furthermore, through [118], a new scheme was recommended, where differences among neighbouring pixels in the host images were computed, in addition to the modulus function, and utilised in concealing and extracting secret data. Frequency domain steganography was used in [69] and [119] where optimisation methods such as GA and PSO ascertain which coefficients are suited for the concealment of the quick response coded secret data. Generally, these techniques require additional enhancements that pertain to the identification of added features extracted from neighbouring pixels which are utilised in the embedding process. The enhancements are meant to improve the capability of embedding and archiving huge embedding capacity and to maximise the PSNR value for the purpose of improving the quality of stego images. Hence, in this study, we aim to meet these objectives and prove that our recommended technique is more secured compared with the previous studies.

III. PROPOSED METHOD

Three approaches are utilised in steganography technique, namely, spatial, frequency and substitution domains. Firstly, the spatial domain approach offers a large size of secret data, which is required to be embedded in the host image with a low level of distortion in the stego image [20]–[23]. Hence, we used this approach in our proposed method, where the overall notion is to transform the steganography issue as a search and optimisation issue. The principle notion of PSO algorithm and the rationale of using this particular algorithm in this study will be explained in the next section.

A. PSO

PSO is an optimisation algorithm that has gained attention from researchers within the past 10 years. This algorithm was developed to define predictive controls by decreasing the constrained multivariable standard [121], [122]. This study utilised the PSO algorithm for optimising the position within the host image for the embedment of the secret bit. The initial recommendation of the PSO algorithm was for the constant valued search spaces, then expanded to segregate the valued search spaces. During the binary search, the recommended solutions are defined by particles, where the particle can be represented as Boolean vector. Next, the status of the particle is evaluated by calculating its speed.

The particle's location will determine whether the particular feature should be chosen [106]. In instances with n particles in M-dimensional size, the location vector for the ith particle is defined by vector $xi = (xi1, xi2, xi3, \ldots, xi\text{M})$, where $xi\text{M}$ is defined by the Mth dimension of the ith particle location. The speed vector of ith particle is defined as $Vi = (vi1, vi2, vi3, \ldots, vi\text{M})$. In addition, the ideal location of the ith particle is defined by vector $PBi = (pi1, pi2, pi3, \ldots, pi\text{M})$, and the global best location found is defined by the vector $GB = (g1, g2, g3, \ldots, g\text{M})$.

$$v_{id}^{k+1} = \left(wv_{id}^{k}\right) + r1 \quad C1\left(p_{id} - x_{id}\right) + r2C2\left(g_{d} - x_{id}\right), \tag{1}$$

where k defines kth iteration, w is inertia weight term and $r1$ and $r2$ are random numbers in the interval [0,1]; C1 ∈ [0,2] and C2 ∈ [0, 2] are two constants known as social and cognitive parameters, respectively. The location of the particle is updated as follows.

$$x_{id}^{k+1} = x_{id} + v_{id}^{k+1}. \tag{2}$$

Thus, the outcomes of the sigmoid function which has been performed on the speed used in order to updated of the particle locations. Where, the function for the particles speed can be defined as follows.

$$s\left(v_{id}^{k+1}\right) = \frac{1}{1 + e^{-v_{id}^{k+1}}}. \tag{3}$$

The random number produced in the domain [0.1] is defined as r. If the value of $s\left(v_{id}^{k+1}\right)$ is larger than r, then select the equivalent gene ootherwise, there is no gene selection. Whereas, the best location PB_i^k of the ith particle in nth iteration is calculated by:

$$PB_i^k = x_{argmin_{t \leq k}} \quad f\left(PB_t^k\right). \tag{4}$$

The best location GB^k in kth iteration is calculated as follows.

$$GB^k = PB^k_{argmin_t} \quad f\left(PB_t^k\right). \tag{5}$$

The PSO is useful and ideal due to its minimal parameter usage, and it can be used in numerous applications with different needs [123].

The use of PSO algorithm has several benefits:

1. PSO is easy to use due to the absence of crossover and mutation procedure in GA, and the SO algorithm is dependent upon the speed of particles. Thus, the data are transferred to the new particles solely through the optimal particles.

2. The PSO algorithm offers a historical record of the particle swarm movements due to its excellent memory.

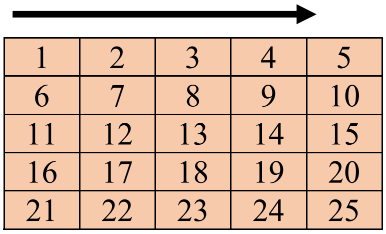
3. Only a small number of parameters is required to be used and adjusted in addition to the absence of complexity in the PSO algorithm structure compared with other metaheuristic algorithms.

4. The PSO algorithm possesses the capability to produce a precise outcome at the start of the search operation.

B. SCANNING ORDER IN HOST IMAGE

The best place signifies the position where an information may be concealed with the minimal probability of distortion. This technique determines the beginning pixel, the number of LSB used within an individual pixel, in addition to the succession of scanning image pixels to conceal the message bits. The raster order of pixels in the LSB substitution technique entails the sequence of the pixels in the host image.

The scanning order of these pixels begins from left to right, and from the first row to the last row for entire rows in the host image. If we have a 5 × 5 image, then the raster scan order is as illustrated in Figure 1.

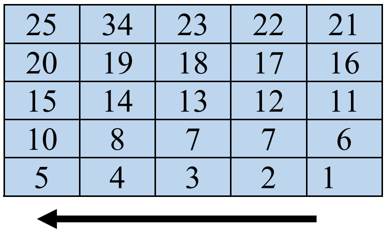


1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

FIGURE 1. Raster order.

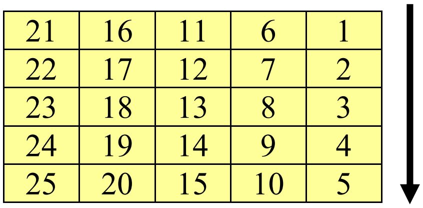
C. BENCHMARK METHOD

The overall notion of benchmarked method is in the transformation of the steganography issue into search and optimisation issue. Comprehensively, Figures 2 and 3 illustrate the probability of bit order in any image, which introduce a better order than the raster order, wherein the raster order is the order of pixels in the host image. Additionally, the raster order is detectable by scanning the host pixels row by row; individual rows are scanned from left to right. Consequently, numerous different orders and positions in the cover image that offers different PSNRs can be utilised for embedding the secret message. Hence, the challenge is in determining the best direction of pixel scanning. A total of 16 scanning plans are possible. In this study, we proposed a new method for finding all possible sequence orders to ascertain the best order for the cover image based on PSO algorithm to enhance the performance of the basic LSB steganography method.



25	34	23	22	21
20	19	18	17	16
15	14	13	12	11
10	8	7	7	6
5	4	3	2	1

FIGURE 2. Raster order 1.



21	16	11	6	1
22	17	12	7	2
23	18	13	8	3
24	19	14	9	4
25	20	15	10	5

FIGURE 3. Raster Order 2.

D. DEVELOPMENT OF BENCHMARK METHOD

Our recommended technique for image steganography uses the search component for the optimum position within the host image within the spatial domain for concealing the secret data, where the resulting image is known as a stego image. Our goals are to obtain good quality with the minimum level of deformation and high endurance against attacks. Figure 4 illustrates the sequence diagram of the recommended technique for embedding secret image data in a host image. This technique is based on PSO algorithm, and the embedding of the secret image procedure can be found here.

This benchmark method utilises a sequential technique for scanning image pixels (starting from columns on the right to the left or vice versa, and from top rows to bottom rows or vice versa) in the entire image, thereby making identification of the optimal location for data concealment extremely problematic. The reason is that scanning within a window of an image is superior compared with scanning within an entire image. Sequential scanning within an entire image was substituted with sequential scanning within four windows from the image with an appropriate size for the data to enhance the capacity of the technique. Consequently, the benchmark technique has emerged as a unique case compared with our recommended technique. The new technique is an enhancement of the benchmark technique, in which GA was substituted by PSO and utilises a different method of embedding secret bits.

1) PARTICLE DEFINITION

Nine particles, instead of seven genes, were used in the recommended technique, which were used in the benchmark technique. These particles are specified in the following variables:

Particle= [Direction X-offset, Y-offset, Bit-planes, SB-Pole, SB-Dire, BP-Dire, X-Side-Length, Y-Side-length]

Table 1 displays the nine particles that were used in the recommended technique.

The definitions of the last two particles are as follows.

X-Side-Length: The dimension of the window in the X-axis, where the minimum value is equal to ceil(sqrt(length(message)*8))
Y-Side-Length: The dimension of the window in the Y-axis, where the minimum value is equal to ceil(sqrt(length(message)*8))

Table 2 shows all probable cases of scanning. Furthermore, the two constraints should be fulfilled:

X-offset-Length<= number of the host columns.
Y-offset-Length < number of the host rows (strict inequality because the last line is used for hiding particle bits).

In the last row of the stego image, the particle bits are embedded for extraction during steganalysis. The scanning direction in the cover image pixels has 16 possible cases. The particle representation has a length of 4 bits in our recommended

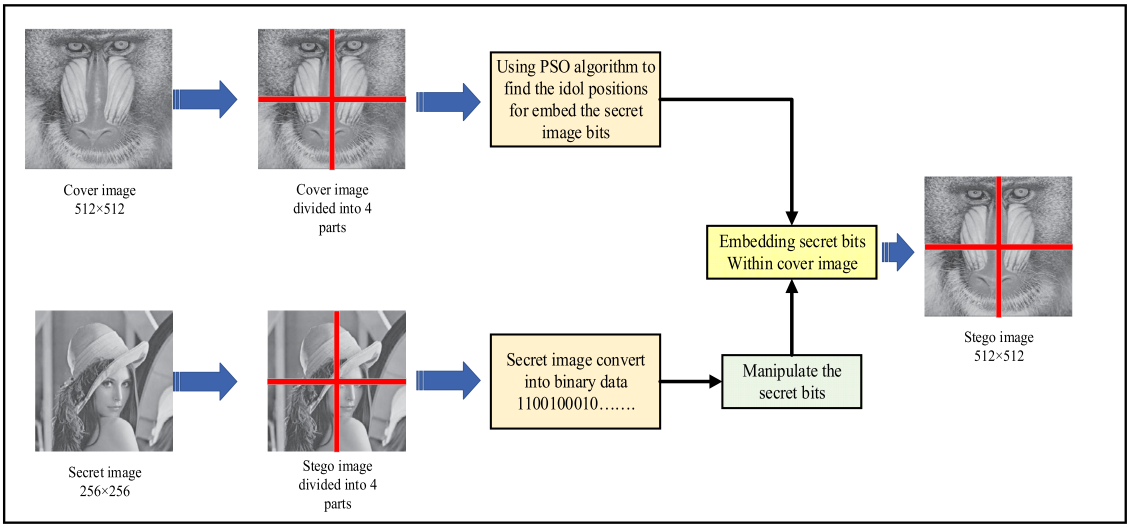


FIGURE 4. **Proposed method diagram.**

TABLE 1. **Particle representation.**

Particle name	Value range	Length	Description
Direction	0 to 15	4 bits	Direction of host image pixel scanning
X-Offset	0 to 225	8 bits	X-offset of starting point
Y-Offset	0 to 225	8 bits	Y-offset of starting point
Bit-Planes	0 to 15	4 bits	Used LSBs for insertion of secret bit
SB-Pole	0 to 1	1 bit	Pole of secret bits
SB-Dire	0 to 1	1 bit	Direction of secret bits
BP-Dire	0 to 1	1 bit	Direction of bit planes
X-Side-Length	0 to 225	8 bits	Dimension of window in the x-axis
Y-Side-Length	0 to 225	8 bits	Dimension of window in the y-axis

technique. The scanning starting point is represented as two particles, including X- and Y-offset, with a length of 8 bits individually. Table 3 shows all the possible cases of bit-planes to define LSB planes in the cover image pixels used particles (bit-planes).

The SB-Dire is utilised to determine the orientation of the message bits (secret data) in determining the secret bit-pole utilised (SB-Pole). The terminal particle is BP-Dire, which indicates the orientation of the LSB planes.

Table 4 indicates the last three particles. The particles may be categorised into two sets in our recommended technique as a result. Set 1 consists of the particles that focused on the insertion of the secret bits into the host image, and Set 2 constitutes the particles utilised to enable changes in the secret data to enhance the adaptability with the host image.

2) EMBEDDING SECRET IMAGE

These steps explain the embedding operation using our recommended technique:

Step 1: The host and secret images were prepared, followed by the reading of the host image 1 ($m \times n$) and the secret image S $(u \times v)$.

Step 2: The secret image was segregated into four 2×2 blocks, and the secret data array was developed for each part where the data are indicated in the most significant bit planes. Next, the MSB of each pixel was extracted in S and linked to obtain a string of bits W to be concealed in I. The length of W is *len.*

Step 3: The host image was segregated into four 2×2 blocks, as $I = 1.....$r. Hence, the number of secret bits in each block can be calculated as $n = len/r$.

Step 4: The PSO algorithm was applied to achieve good pixel positions in each block, where the ensuing procedure attain:

- Adjust the PSO parameters as:

ns (particle number)

iters (the maximum number of iterations)

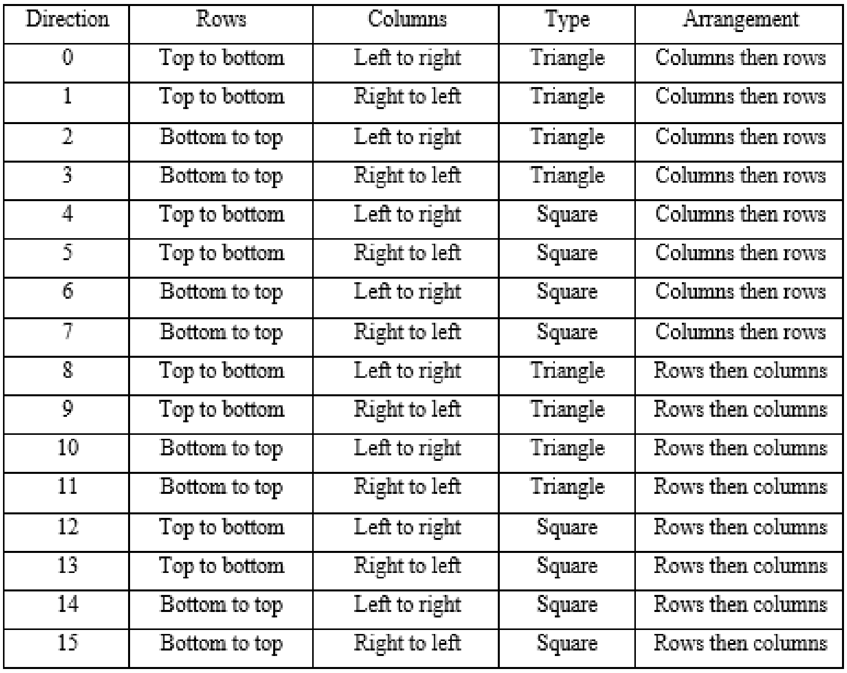
iw (inertia weight factor)

c1 and *c2* (cognitive and social acceleration factors)

r1 and *r2* (random numbers in the range [0,1])

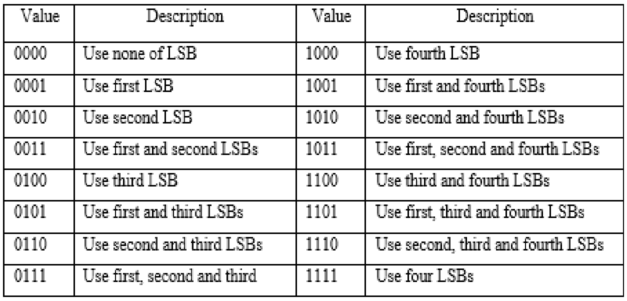
- Within the swarm, each block equals to the number of pixels in dimension should be determined for the embedment in each block. The number of secret data can be calculated in each block as in Step 3. Hence, 1 secret bit/pixel requires n pixels for each block, and the same context for

TABLE 2. Potential cases of scanning of the cover image.



Direction	Rows	Columns	Type	Arrangement
0	Top to bottom	Left to right	Triangle	Columns then rows
1	Top to bottom	Right to left	Triangle	Columns then rows
2	Bottom to top	Left to right	Triangle	Columns then rows
3	Bottom to top	Right to left	Triangle	Columns then rows
4	Top to bottom	Left to right	Square	Columns then rows
5	Top to bottom	Right to left	Square	Columns then rows
6	Bottom to top	Left to right	Square	Columns then rows
7	Bottom to top	Right to left	Square	Columns then rows
8	Top to bottom	Left to right	Triangle	Rows then columns
9	Top to bottom	Right to left	Triangle	Rows then columns
10	Bottom to top	Left to right	Triangle	Rows then columns
11	Bottom to top	Right to left	Triangle	Rows then columns
12	Top to bottom	Left to right	Square	Rows then columns
13	Top to bottom	Right to left	Square	Rows then columns
14	Bottom to top	Left to right	Square	Rows then columns
15	Bottom to top	Right to left	Square	Rows then columns

TABLE 3. Possible values for Bit-Plane particle.



Value	Description	Value	Description
0000	Use none of LSB	1000	Use fourth LSB
0001	Use first LSB	1001	Use first and fourth LSBs
0010	Use second LSB	1010	Use second and fourth LSBs
0011	Use first and second LSBs	1011	Use first, second and fourth LSBs
0100	Use third LSB	1100	Use third and fourth LSBs
0101	Use first and third LSBs	1101	Use first, third and fourth LSBs
0110	Use second and third LSBs	1110	Use second, third and fourth LSBs
0111	Use first, second and third	1111	Use four LSBs

2 secret bits/pixels requires *n/2* pixels for each block. In addition, 3 secret bits/pixels require *n/3* pixels for each block and so.

The secret bits are transformed into corresponding particles (i.e. SB-Dir and SB-Pole), then a comparison is made between the number of pixel bits with the secret bits in instances where the number of secret bits is larger than the pixel bits. This refer to, that the concerning particle cannot able to conceal the secret bit in the cover image.

Step 5: The secret bits were embedded, comprising the bits from secret data *W,* and are concealed in n_q pixels by using PSO algorithm computing.

Figure 5 shows the flowchart of the embedding procedure.

3) EXTRACTING SECRET IMAGE

The extraction of the embedded secret image may be implemented through the reverse procedure, as shown in Figure 6.

The extraction key used in the embedding procedure can be found in the last row of the stego image and can also be used in the extraction procedure for recovering the secret image. Each block $BI = 1....r$, of the stego image I', extracts the pixels and bits that were concealed in each of the pixel using the key. For example, for pixel D'_{ij}, the extracted secret bit will be *S,* where *S* can be calculated as:

$$S = \left\lfloor \frac{D'_{ij}}{w} \right\rfloor mod 2^q. \tag{6}$$

Hence, the secret bits can be generated through the concatenation with each other and implementing the inverse permutation transformation by converting *S* into a binary string of *q* bits. Finally, the secret image is obtained.

IV. RESULTS AND DISCUSSION

The performance evaluation of the recommended steganography method is conducted through the comparison with the benchmark method (GA) in addition to alternative additional methods. The benchmark technique is a steganography technique based on GA to ascertain the optimal location for concealing data within a host image. Whereby, the stego image quality is assessed using certain engineering metrics, which is illustrated as follows.

1. The value of PSNR metric between the stego and the host image is calculated using Equation 7

$$PSNR = 10 \times \log_{10} \frac{(255)^2}{MSE}, \tag{7}$$

where MSE is the mean square error between the host and stego images, and the dimension of the host image is $W \times H$.

TABLE 4. Possible values for SB-Pole, SB-Dire and BP-Dire particles.

Particle name	Value	Description
SB-Pole	0	In this case, the secret bits were unchanged.
	1	In this case, the secret bits were changed to be opposite.
SB-Dire	0	In this case, no change is made to secret bits
	1	In this case, secret bits are reversed from end to beginning
BP-Dire	0	In this case, bit-planes were used from MSB to LSB.
	1	In this case, bit-planes were used from MSB to LSB.

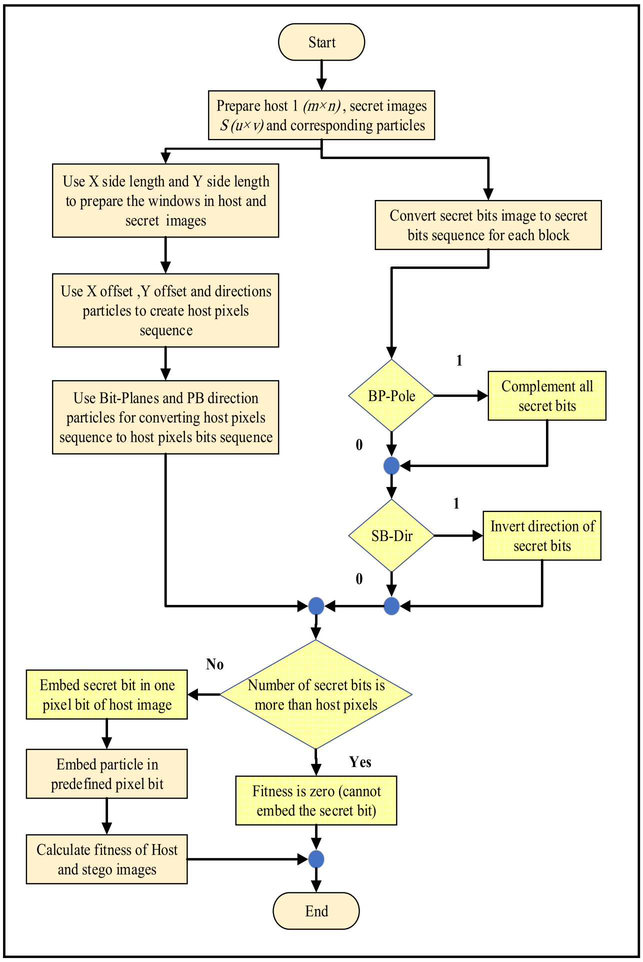

Start
Prepare host I (m×n), secret images S (u× v) and corresponding particles
Use X side length and Y side length to prepare the windows in host and secret images
Convert secret bits image to secret bits sequence for each block
Use X offset ,Y offset and directions particles to create host pixels sequence
Use Bit-Planes and PB direction particles for converting host pixels sequence to host pixels bits sequence
BP-Pole
1
Complement all secret bits
0
SB-Dir
1
Invert direction of secret bits
0
No
Embed secret bit in one pixel bit of host image
Number of secret bits is more than host pixels
Yes
Embed particle in predefined pixel bit
Fitness is zero (cannot embed the secret bit)
Calculate fitness of Host and stego images
End

FIGURE 5. Flowchart of embedding secret image.

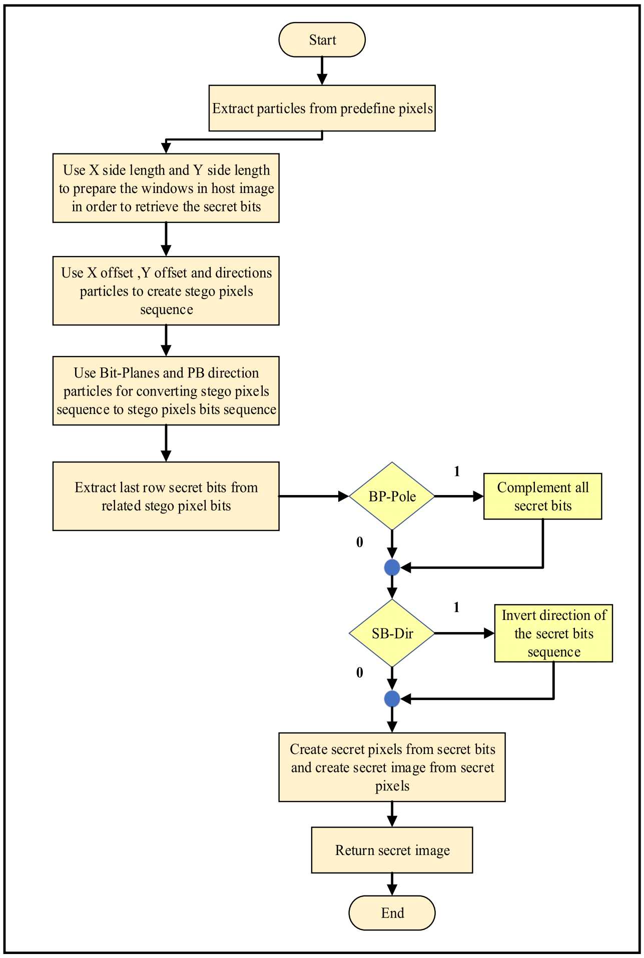

Start
Extract particles from predefine pixels
Use X side length and Y side length to prepare the windows in host image in order to retrieve the secret bits
Use X offset ,Y offset and directions particles to create stego pixels sequence
Use Bit-Planes and PB direction particles for converting stego pixels sequence to stego pixels bits sequence
Extract last row secret bits from related stego pixel bits
BP-Pole
1
Complement all secret bits
0
SB-Dir
1
Invert direction of the secret bits sequence
0
Create secret pixels from secret bits and create secret image from secret pixels
Return secret image
End

FIGURE 6. Flowchart of extracting secret image.

Equation 8 is utilised to calculate the MSE value:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{w} \sum_{j=1}^{H} \left(x_{i,j} - y_{i,j}\right)^2, \tag{8}$$

where the value of each pixel in the host image and stego image are x_{ij} and y_{ij}, respectively.

The evaluation is conducted using the famous 'Lena', which is the conventional 256 × 256 cover image and 'Jet', 'Pepper' and 'Baboon' as the secret images, as indicated in Figure 7.

If we change the dimension of the secret images 'Jet' and 'Baboon' into 64 × 64, 96 × 96, 128 × 128, 160 × 160 and 192 × 192, then the outcomes will indicate different storage capacities and PSNR values, as indicated in Table 5.

This technique was recommended for determining the optimal window that can maximise the PSNR value between

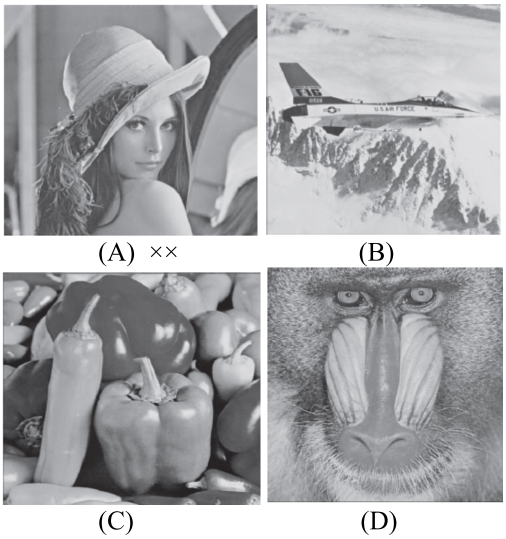


FIGURE 7. The host and secret images. (A) is the host image. (B)–(D) are the secret images.

TABLE 5. Relationship between storage capacity of secret image and PSNR.

Capacity			PSNR	
%	BPP	Size of secret images	Jet	Baboon
6.25	0.5	64 × 64	59.1227	58.7874
14	1.125	96 × 96	56.0313	55.9472
25	2	128 × 128	55.1344	55.1263
39	3.125	160 × 160	54.7347	54.7413
56	4.5	192 × 192	53.5900	53.3743

the original (host image) and the stego image in addition to providing an extensive embedding capacity. To achieve superior outcomes, the new notion is to segregate the secret message and the host image into four blocks in addition to the application of the PSO algorithm on each block. Through this method, each block will be addressed as an independent block. Our method improves the benchmark method that was based on GA by adding two particles instead of the seven genes that were utilised in the benchmark method. Hence, we adhere to the exact experimental procedural technique that was utilised in the benchmark technique to make a comparison and substantiate that our recommended technique is the superior form of steganography technique based on GA (benchmark method). We utilised a 256 × 256 pixel secret image (A), and four 512 × 512 pixel host images (B–E), which are, 'Lena', 'Jet', 'Pepper' and 'Baboon', as shown in Figure 8. Table 6 shows the comparison of PSNR outcomes between our recommended technique and the benchmark technique.

Based on the PSNR results, the PSNR value of our technique is superior over the benchmark method based on GA. Our technique surpasses all other techniques in the benchmark study, including the steganographic technique that was based on GA.

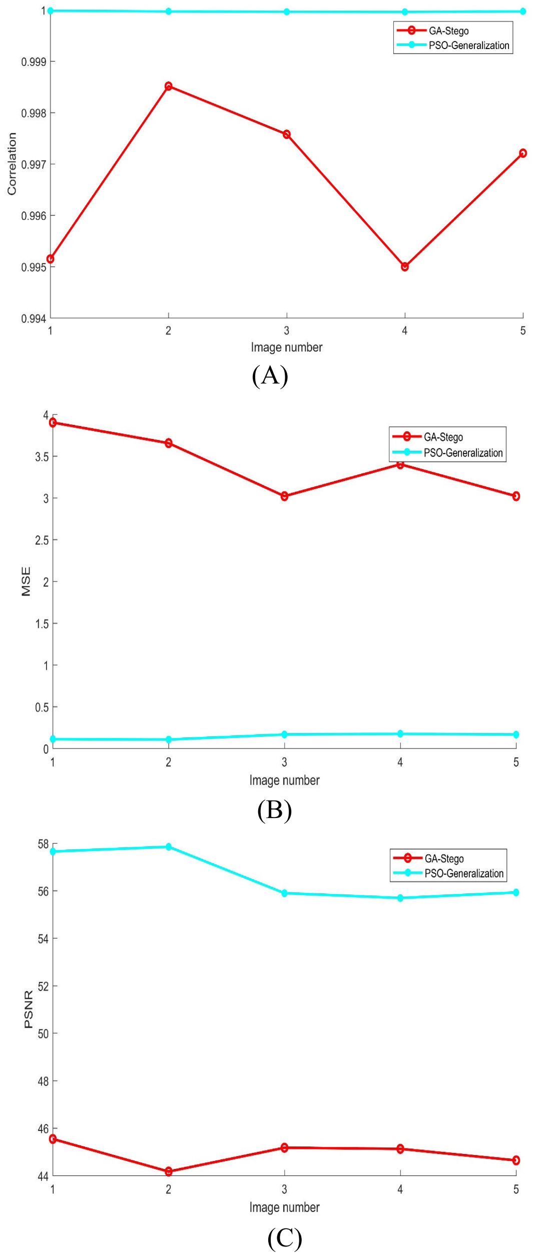
FIGURE 8. (A): Secret image, (B-E): Host images

TABLE 6. Performance comparison between the recommended technique (proposed method) and Steganography based on GA.

Image name	GA method	Proposed method
Lena	45.12	57.65
Jet	45.18	55.69
Pepper	45.13	55.92
Sailboat	45.10	55.89
Baboon	45.12	57.84
Average	**45.13**	**56.60**

The second evaluation perspective is the comparison made between our recommended technique and the benchmark technique, in relation to PSNR, MSE and the correlations as shown in Figure 9. The recommended technique indicated a high degree of performance compared with the benchmark technique. This technique has a high degree of security against hacking operations and a high degree of stego image visual quality.

Figure 9a shows the correlation between the stego and the cover images for our proposed and benchmark methods and shows a high level of correlation in the benchmark method, whereas our recommended technique requires a lower level of correlation. In the past 10 years, numerous active steganalysis techniques were generated. These techniques have the capacity to detect steganography by using statistical analysis, with numerous recent techniques encountering this particular challenge. The host with a small correlation with the stego image has a superior ability in improving the security of a steganographic technique [124]. Figure 9b indicates that our recommended technique has extremely little value of MSE compared with the benchmark method. Figure 9c indicates that our recommended technique possesses the optimum PSNR value compared with the benchmark technique. Moreover, a histogram is utilised to ascertain the distortion and deterioration in the stego images in Figure 10.



(A)

(B)

(C)

FIGURE 9. (A) Correlation, (B) MSE and (C) PSNR between proposed and benchmark methods.

The outcomes substantiated that the recommended technique demonstrates an extremely low degree of distortion in the stego image. As a result, the recommended technique produces a favourable quality of a stego image (less degree of distortion), which is a significant factor in steganographic techniques.

A. RESULTS AND COMPARISON CHECKLIST

A comparison of the recommended steganographic technique in this study is made against the most relevant study [88]. This work is perceived as the benchmark in association with the research on steganography. Table 7 presents the checklist comparison between the benchmark method and the recommended method.

The weight of each issue in Table 7 is 33.33%. The proposed steganography method covers all related issues of the evaluation stage 100%, whereas the benchmark steganography method covers only 66.66%, showing a difference of 33.34%.

For the purpose of proving the effectiveness of the proposed method, a comparison of the results with the modern methods is required, regardless of the type of techniques that were utilised pertaining the concealment of secret data. In this comparison, we will use only the common host images (Lena, Baboon and Pepper) that were utilised in the experimental part of our proposed method, in addition to other modern proposed methods, with a comparison made among the best and highest results only. Table 8 indicates the results.

These methods aim at enhancing PSNR and high embedding capacity, which represent the main objectives of steganography technique. According to the results in Table 8, our proposed method had succeeded in achieving a higher embedding capacity compared with other methods, except for [127], which demonstrates the same ability for concealing four BPP but with less value of PSNR. Furthermore, the proposed method achieved the highest value of PSNR by considering the number of bits that can be concealed in each pixel, as shown in Table 8.

For the purpose of evaluating and substantiating that our proposed method can be used for concealing large secret data, we conducted an experiment to conceal FV pattern for 106 users by utilising MMCBNU_6000 database through the selection of the left index image for each user. The results indicated that our proposed method is highly effective and achieved high PSNR value. Furthermore, the histogram indicated no degradation in the stego image and no visual difference between the host and the stego images. Appendix 1 displays the PSNR, MSE and correlation. Appendix 2 displays the stego images, host images and histogram.

B. TIME COMPLEXITY ANALYSIS

Our recommended steganography technique is based on PSO algorithm to select the optimal position of pixels to conceal the secret data. Therefore, we should estimate the time complexity of this algorithm to determine the time complexity for our proposed method, where the computation time represents the major factor in the pose tracking using PSO algorithm. This process usually needs seconds to minutes to estimate the pose in one frame if the implementation uses MATLAB. This means, the tracking sequence perhaps need to hours. Nevertheless, the computation time is significantly based on the number of likelihood evaluation and model rendering. Our proposed method utilised the standard PSO algorithm to find the optimum pixel position in static search space.

Conversely, the nature of dynamic space, which involves the search for a single optimum pixel position, requires a changeable dynamic computation time [130]. The distance

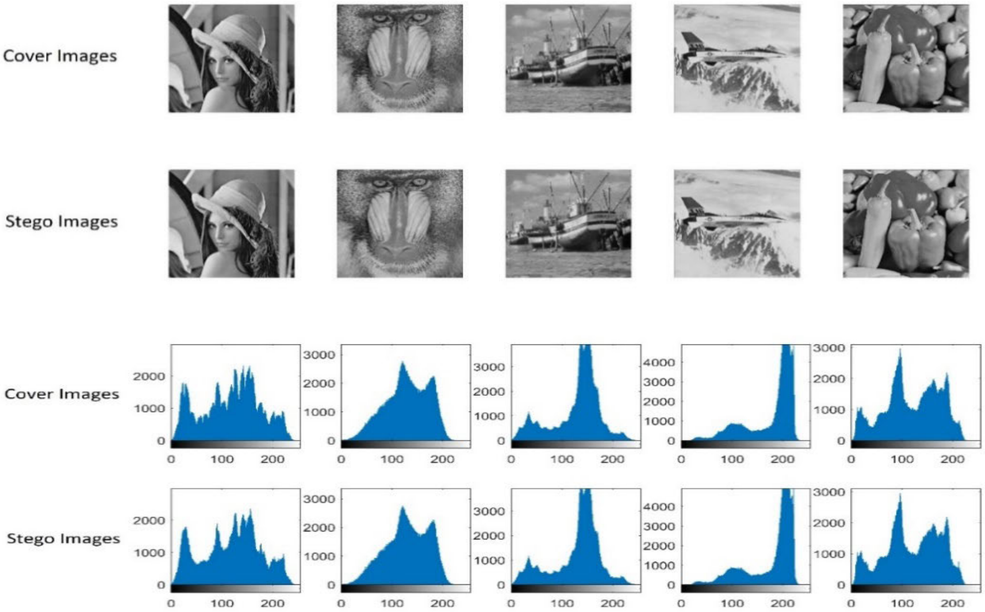


FIGURE 10. Virtual comparison between host and stego images.

TABLE 7. Checklist comparison between the benchmark and recommended methods.

Checklist issues	Benchmark method	Proposed method
PSNR	Supported Achieved value is 45.13%.	Supported Achieved value is 56.60 %.
MSE A low value for MSE means less error	Supported No clear results were shown.	Supported Figure 9b shows that this method has lower value of MSE than benchmark method.
Histogram	No consideration	Figure 10 shows that this method has impalpable differences between host and stego images.

between the particle's current position and the local best position is an important factor for the adjustment of an upper limit on the maximum value of the cognitive term. The absolute difference between the current location and local best location of the particles can be considered a particle's local distance for its d-th dimension. In the same context, it can be defined as the particle's global distance, which entails the difference between the current location and global location of particles [131], that is,

$$\text{Local distance} = \left|P_k^d - x_k^d\right| \tag{9}$$

$$\text{Global distance} \left|g^d - x_k^d\right| \tag{10}$$

where P_k^d and g^d are the particle's local best and the swarm's global best positions for the d-th dimension, respectively. $\mathrm{d} = 1, \cdots, D$ denote the particle's dimension index and $\mathrm{k} = 1, \cdots, N$ is the particle index.

Hence, with the small distance among the particles within static space, the PSO algorithm does not require the calculation of those terms to update velocity, and cognitive and social terms of the update equation for the d-th dimension will not be calculated, thereby reducing the size of the problem that we attempt to solve. Consequently, the large number of evaluation in terms of problem size is the optimal measure of time complexity, which is also known as scalability [132]. Certain metaheuristic algorithms require a few hundred or thousand iterations (with a large computational effort for each iteration) to gain favourable outcomes, whereas others require several million iterations (with only minimal computational effort for each iteration). Therefore, in this study, we utilised PSO algorithm instead of GA because PSO outperforms the GA with a large differential in computational efficiency especially when solving unconstrained nonlinear problems [133]. Finally, we can only compare the metaheuristics empirically through CPU time, or objective function evaluations. Experimentally utilised MATLAB\R2018a on a Windows 10 operating system with 4 GB RAM and 0.5 TB hard disk. The total time consumed for the embedment and

TABLE 8. Comparison of results between our recommended method and other modern methods.

Study	Brief description	Results using 512 × 512 images			
		Image name	PSNR	BPP	Capacity
[82]	This study proposed a steganography method entailing three group of bit substitution (3GBS) to hide three secret BPP.	Lena	44.37	3.0	786,432
		Baboon	44.40	3.0	786,432
		Pepper	44.37	3.0	786,432
[125]	This study attempted to improve the steganography technique through segregation into three variants, with each block consisting of two pixels that were used for concealing the secret data.	Lena	54.37	1.0	262,144
			42.95	2.0	524,288
		Baboon	54.40	1.0	262,144
			43.90	2.0	524,288
		Pepper	54.41	1.0	262,144
			44.96	2.0	524,288
[126]	This study proposed a new approach for steganography based on pixel value differencing and modulus function (PVDMF) in addition to the use of two variants for the concealment of secret bits via the readjustment of the pixel to reduce the distortion in the stego image.	Lena	42.98	2.1	556,401
			39.34	3.1	811,181
		Baboon	38.83	2.5	646,885
			36.68	3.0	793,183
		Pepper	43.23	2.1	551,069
			36.51	3.3	875,842
[127]	This study proposed a new steganography method through the utilisation of n-rightmost bit replacement technique to conceal the secret data.	Lena	51.25	1.0	262,144
			34.86	4.0	1,048,576
		Baboon	51.20	1.0	262,144
			34.79	4.0	1,048,576
[128]	This study proposed a bit-flipping method to conceal the secret data in the host image. This method utilised a block consisting of two pixels where two LSBs of each pixel were utilised. Thus, this method offers the concealment of four bits for a pair of pixels.	Lena	47.31	2.0	524,288
		Baboon	47.33	2.0	524,288
		Pepper	47.32	2.0	524,288
[129]	This study proposed a new steganography method based on two variants, which were 1) overlapped PVDMF, and (2) overlapped pixel value differencing (OPVD). The two variants concealed five secret bits in each 1 × 5 pixel block.	Pepper	36.43	3.15	824,610
			37.25	3.0	786,794
Our proposed image steganography method based on PSO algorithm		Lena	57.65	4.0	1,608,070
		Baboon	57.84	4.0	1,608,070
		Pepper	55.92	4.0	1,608,070

extraction of the secret data for five grey scale images was 4.735 s, as shown in Figure 10.

C. SECURITY ANALYSIS USING RS STEGANALYTIC ATTACK

The LSB substitution is susceptible to RS steganalytic attacks [129], [128]. This type of attack is based on statistical test, where the notion underlying this attack is as follows.

Assume that the pixel intensity value is $P_X = 40$ and $P_X = 2_X = 40$, then $x = 20$. When we attempted to conceal the secret bit value 0 in the LSB location of P_X, the value of this pixel will remain the same. However, when we conceal the secret bit value 1, the P_X value will increase to 41. This increase signifies 2_X+1 because 2_X will never become 2_X-1. In the same context, when $P_X = 2_X + 1 = 41$, and we attempted to conceal the secret bit value 0 in the LSB location of P_X, the value of P_X will then be 40. This means that $2_X + 1$ became 2_X, and it is not possible to be $2_X + 2$ nor $2\mathrm{x} - 1$. This type of attack endeavours to exploit this weakness point. Table 3 shows that our recommended method has 16 different possibilities that begin from 0000 to 1111. Hence, our technique demonstrates the capacity to resist these kinds of attacks. Consequently, our proposed method is secure.

V. CONTRIBUTIONS

The main objective of this study is to propose a new steganography method based on PSO algorithm for selecting the best pixel position in a host image. Other objectives include the embedment of the secret bits with the least possible distortion and the achievement of a high embedding capacity for secret information, as well as a high PSNR value by considering the

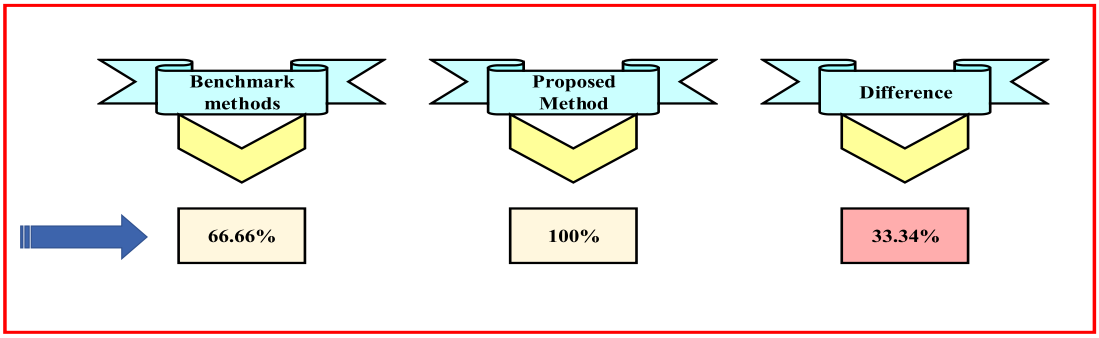


FIGURE 11. Differences in coverage percentages between the proposed and benchmark methods on specific related issues.

steganography problem as a search and optimisation problem. This study attempts to fill the the gap in literature because of the limited amount of studies that implement metaheuristics in steganography techniques.

The contributions of this study can be summarised in four parts. Firstly, we have investigated existing literature in the past five years to enhance the steganographic techniques pertaining the high embedding capacity. Secondly, we have proposed a method that enables the efficient concealment of secret bits in a host image, and the ability to extract these bits again in the recovery phase within an acceptable period. Thirdly, the proposed method offers a high embedding capacity for high payload concealment that can assist in concealing large secret data within a host image, as shown in Appendices 1 and 2. Lastly, the comparison in Table 8 indicates that our proposed method offers the ability to conceal four secret BPP as the maximum hiding capacity. Thus, a strong evidence exists that our proposed method can be considered a superior method compared with existing state-of-art techniques.

VI. CONCLUSION AND FUTURE WORK

This study proposed an efficient steganography method of using PSO algorithm-based pixel selection for concealing a secret image within a host image in the spatial domain. The proposed method has high resistance against hacking or attacks due to the security provided by image steganography. PSO was conducted to select an optimal pixel in the host image to embed secret bits. The PSO can achieve efficient fitness calculation that depends on the cost matrix by dividing the host and secret images into four parts. In the first part, the secret bits are altered. Then, these bits are embedded within the host image pixel. Several locations in the host image are specified via the order of scanning host pixels, the starting point of the scanning and the good LSBs of each pixel. The PSO algorithm was used to determine the optimum starting point and scanning order. The results indicated the effectiveness of the proposed method in producing good stego image quality and positive ability in retrieving a hidden image or data. The comparison between this method and the benchmark method, which was based on GA, in terms of PSNR, MSE and histogram, illustrated that the PSNR value in the benchmark method for five stego images is 45.13%. However, by utilising the proposed method for the same five images, the PSNR value is 56.60%. Moreover, the proposed method can be considered the best method compared with other modern methods in terms of the quality of the stego images and the capacity of embedding secret data. Our future work will focus on ascertaining a new approach for replacing the LSB approach through other appropriate algorithms and improving the PSNR and MSE value while maintaining the highest level of embedding capacity.

ACKNOWLEDGMENT

The authors thank Chonbuk National University in South Korea for offering their MMCBNU_6000 FV dataset.

REFERENCES

[1] B. B. Zaidan, A. A. Zaidan, and M. L. M. Kiah, "Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns," *Int. J. Pharmacol.*, vol. 7, no. 3, pp. 382–387, 2011.

[2] H. O. Alanazi, M. L. M. Kiah, A. A. Zaidan, B. B. Zaidan, and G. M. Alam, "Secure topology for electronic medical record transmissions," *Int. J. Pharmacol.*, vol. 6, no. 6, pp. 954–958, 2010.

[3] B. B. Zaidan, A. A. Zaidan, O. H. Alanzani, and R. Alnaqeib, "Towards corrosion detection system," *Int. J. Comput. Sci.*, vol. 7, no. 3, pp. 33–36, 2010.

[4] A. Taqa, A. A. Zaidan, and B. B. Zaidan, "New framework for high secure data hidden in the MPEG using AES encryption algorithm," *Int. J. Comput. Elect. Eng.*, vol. 1, no. 5, pp. 566–571, 2009.

[5] A. W. Naji, S. A. Hameed, W. F. Al-khateeb, O. O. Khalifa, and T. S. Gunawan, "Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques," *Int. J. Comput. Sci. Inf. Secur.*, vol. 3, no. 1, pp. 1–6, 2009.

[6] M. S. A. Nabi, M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, and G. M. Alam, "Suitability of SOAP protocol in securing transmissions of EMR database," *Int. J. Pharmacol.*, vol. 6, no. 6, pp. 959–964, 2010.

[7] G. M. Alam, M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, and H. O. Alanazi, "Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study," *Sci. Res. Essays*, vol. 5, no. 21, pp. 3254–3260, 2010.

[8] A. K. Hmood, Z. M. Kasirun, H. A. Jalab, G. M. Alam, A. A. Zaidan, and B. B. Zaidan, "On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates," *Int. J. Phys. Sci.*, vol. 5, no. 7, pp. 1054–1062, 2010.

[9] H. Alanazi, R. M. Noor, B. B. Zaidan, and A. A. Zaidan, "Intrusion detection system: Overview," *J. Comput.*, vol. 2, no. 3, pp. 1–5, 2010.

[10] H. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, ''New comparative study between DES, 3DES and AES within nine factors,'' *J. Comput.*, vol. 2, no. 3, pp. 1–5, 2010.

[11] M. Abomhara, O. Zakaria, O. O. Khalifa, A. A. Zaidan, and B. B. Zaidan, ''Enhancing selective encryption for H.264/AVC using advanced encryption standard,'' *Int. J. Comput. Elect. Eng.*, vol. 2, no. 2, p. 223, 2010.

[12] B. B. Zaidan, A. A. Zaidan, and H. Mwafak, ''New comprehensive study to assess comparatively the QKD, XKMS, KDM in the PKI encryption algorithms,'' *Int. J. Comput. Sci. Eng.*, vol. 1, no. 3, pp. 263–268, 2009.

[13] H. O. Alanazi, G. M. Alam, B. B. Zaidan, and A. A. Zaidan, ''Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance,'' *J. Med. Plants Res.*, vol. 4, no. 19, pp. 2059–2074, 2010.

[14] M. S. Nabi, M. L. M. Kiah, A. A. Zaidan, and B. B. Zaidan, ''Suitability of adopting S/MIME and OpenPGP email messages protocol to secure electronic medical records,'' in *Proc. 2nd Int. Conf. Future Gener. Commun. Technol. (FGCT)*, Nov. 2013, pp. 93–97.

[15] O. Enaizan, A. A. Zaidan, NH M. Alwi, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, and A. S. Albahri, ''Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis,'' *Health Technol.*, pp. 1–28, Nov. 2018.

[16] M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, and A. S. Albahri, ''Conceptual framework for the security of mobile health applications on Android platform,'' *Telemat. Inform.*, vol. 35, no. 5, pp. 1335–1354, 2018.

[17] H. O. Alanazi, A. A. Zaidan, B. B. Zaidan, M. L. M. Kiah, and S. H. Al-Bakri, ''Meeting the security requirements of electronic medical records in the ERA of high-speed computing,'' *J. Med. Syst.*, vol. 39, no. 1, p. 165, 2015.

[18] M. Hussain, A. Al-Haiqi, A. A. Zaidan, B. B. Zaidan, M. Kiah, S. Iqbal, S. Iqbal, and M. Abdulnabi, ''A security framework for mHealth apps on Android platform,'' *Comput. Secur.*, vol. 75, pp. 191–217, Jun. 2018.

[19] S. Iqbal, M. L. M. Kiah, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, and M. A. Alsalem, ''Real-time-based E-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients,'' *Health Technol.*, vol. 9, no. 2, pp. 93–111, Aug. 2018.

[20] B. B. Zaidan, A. Haiqi, A. A. Zaidan, M. Abdulnabi, M. L. M. Kiah, and H. Muzamel, ''A security framework for nationwide health information exchange based on telehealth strategy,'' *J. Med. Syst.*, vol. 39, no. 5, p. 51, 2015.

[21] M. Hussain, ''The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks,'' *Pervasive Mobile Comput.*, vol. 25, pp. 1–25, 2016.

[22] A. W. Naji, T. S. Gunawan, S. A. Hameed, B. B. Zaidan, and A. A. Zaidan, '''Stego-analysis chain, session one' investigations on steganography weakness vs stego-analysis system for multimedia file,'' in *Proc. Int. Assoc. Comput. Sci. Inf. Technol. Spring Conf. (IACSIT-SC)*, Apr. 2009, pp. 405–409.

[23] A. A. Zaidan, A. Majeed, and B. B. Zaidan, ''High securing cover-file of hidden data using statistical technique and AES encryption algorithm,'' *World Acad. Sci., Eng. Technol.*, vol. 54, pp. 463–474, Jun. 2009.

[24] W. F. Al-Khateeb and S. A. Hameed, ''New approach of hidden data in the portable executable file without change the size of carrier file using statistical technique,'' *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 7, pp. 218–224, 2009.

[25] A. Medani, A. Gani, O. Zakaria, A. A. Zaidan, and B. B. Zaidan, ''Review of mobile short message service security issues and techniques towards the solution,'' *Sci. Res. Essays*, vol. 6, no. 6, pp. 1147–1165, 2011.

[26] A. W. Naji, A. S. Housain, B. B. Zaidan, A. A. Zaidan, and S. A. Hameed, ''Security improvement of credit card online purchasing system,'' *Sci. Res. Essays*, vol. 6, no. 16, pp. 3357–3370, 2011.

[27] M. L. M. Kiah, M. S. Nabi, B. B. Zaidan, and A. A. Zaidan, ''An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1,'' *J. Med. Syst.*, vol. 37, no. 5, p. 9971, Oct. 2013.

[28] M. A. Watari, A. A. Zaidan, and B. B. Zaidan, ''Securing m-government transmission based on symmetric and asymmetric algorithms: A review,'' *Asian J. Sci. Res.*, vol. 8, pp. 80–94, Oct. 2013.

[29] A. Malik, G. Sikka, and H. K. Verma, ''A high capacity text steganography scheme based on LZW compression and color coding,'' *Eng. Sci. Technol. Int. J.*, vol. 20, no. 1, pp. 72–79, 2017.

[30] A. A. Zaidan and B. B. Zaidan, ''Novel approach for high secure data hidden in MPEG video using public key infrastructure,'' *Int. J. Comput. Netw. Secur.*, vol. 1, no. 1, pp. 1553–1985, 2009.

[31] B. B. Zaidan, A. A. Zaidan, and F. Othman, ''Enhancement of the amount of hidden data and the quality of image,'' Fac. Comput. Sci. Inf. Technol., Univ. Malaya, Kuala Lumpur, Malaysia, Tech. Rep., 2008.

[32] A. W. Naji, A. A. Zaidan, and B. B. Zaidan, ''Challenges of hidden data in the unused area two within executable files,'' *J. Comput. Sci.*, vol. 5, no. 11, pp. 890–897, 2009.

[33] A. A. Zaidan, A. W. Naji, S. A. Hameed, F. Othman, and B. B. Zaidan, ''Approved undetectable-antivirus steganography for multimedia information in PE-file,'' in *Proc. Int. Conf. IACSIT Spring Conf. (IACSIT-SC)*, vol. 9, Apr. 2009, pp. 425–429.

[34] B. B. Zaidan, A. A. Zaidan, A. Taqa, and F. Othman, ''Stego-image vs stego-analysis system,'' *Int. J. Comput. Elect. Eng.*, vol. 1, no. 5, pp. 1793–8163, 2009.

[35] A. A. Zaidan, B. Zaidan, and H. A. Jalab, ''A new system for hiding data within (unused area two+image page) of portable executable file using statistical technique and advance encryption Standared,'' *Int. J. Comput. Theory Eng.*, vol. 2, no. 2, p. 218, 2010.

[36] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed, ''Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard,'' *J. Med. Syst.*, vol. 43, no. 7, p. 192, Jul. 2019.

[37] Y. Y. A. Talib, B. B. Zaidan, A. A. Zaidan, and A. W. Naji, ''Optimizing security and flexibility by designing a high security system for e-government servers,'' in *Proc. ICOCI*, 2009, pp. 1–5.

[38] B. Zaidan, A. Zaidan, F. Othman, R. Z. Raji, S. Mohammed, and M. Abdulrazzaq, ''Quality of image vs. quantity of data hidden in the image,'' in *Proc. IPCV*, vol. 6, 2009, pp. 343–350.

[39] B. B. Zaidan, A. A. Zaidan, A. Y. Taqa, and F. Othman, ''An empirical study for impact of the increment the size of hidden data on the image texture,'' in *Proc. ICFCC*, 2009.

[40] H. Alanazi, A. A. Zaidan, B. B. Zaidan, H. A. Jalab, and Z. K. Al-Ani, ''New classification methods for hiding information into two parts: Multimedia files and non multimedia files,'' *J. Comput.*, vol. 2, no. 3, pp. 144–151, 2010.

[41] M. Tang, W. Song, X. Chen, and J. Hu, ''An image information hiding using adaptation and radix,'' *Optik*, vol. 126, no. 23, pp. 4136–4141, 2015.

[42] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, S. A. B. Ariffin, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, and M. Hashim, ''Real-time medical systems based on human biometric steganography: A systematic review,'' *J. Med. Syst.*, vol. 42, no. 12, p. 245, 2018.

[43] A. W. Naji, A. A. Zaidan, B. B. Zaidan, S. A. Hameed, and O. O. Khalifa, ''Novel approach for secure cover file of hidden data in the unused area within exe file using computation between cryptography and steganography,'' *J. Comput. Sci.*, vol. 9, no. 5, pp. 294–300, 2009.

[44] A. A. Zaidan, F. Othman, B. B. Zaidan, R. Z. Raji, A. K. Hasan, and A. W. Naji, ''Securing cover-file without limitation of hidden data size using computation between cryptography and steganography,'' in *Proc. World Congr. Eng.*, vol. 1, 2009, pp. 1–7.

[45] B. B. Zaidan, A. A. Zaidan, A. K. Al-Frajatand, and H. A. Jalab, ''On the differences between hiding information and cryptography techniques: An overview,'' *J. Appl. Sci.*, vol. 10, no. 15, pp. 1650–1655, 2010.

[46] A. Majeed, L. M. Kiah, H. T. Madhloom, B. B. Zaidan, and A. A. Zaidan, ''Novel approach for high secure and high rate data hidden in the image using image texture analysis,'' *Int. J. Eng. Technol.*, vol. 1, no. 2, pp. 63–69, 2009.

[47] A. A. Zaidan, B. B. Zaidan, M. M. Abdulrazzaq, R. Z. Raji, and S. M. Mohammed, ''Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography,'' in *Proc. Int. Assoc. Comput. Sci. Inf. Technol.*, vol. 19, 2009, pp. 482–489.

[48] M. E. Eltahir, L. M. Kiah, B. B. Zaidan, and A. A. Zaidan, ''High rate video streaming steganography,'' in *Proc. Int. Conf. Inf. Manage. Eng.*, Apr. 2009, pp. 550–553.

[49] S. H. Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan, and G. M. Alam, ''Securing peer-to-peer mobile communications using public key cryptography: New security strategy,'' *Int. J. Phys. Sci.*, vol. 6, no. 4, pp. 930–938, 2011.

[50] F. Othman, L. Maktom, A. Y. Taqa, B. B. Zaidan, and A. A. Zaidan, ''An extensive empirical study for the impact of increasing data hidden on the images texture,'' in *Proc. Int. Conf. Future Comput. Commun.*, Apr. 2009, pp. 477–481.

[51] Z. K. Al-Ani, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Overview: Main fundamentals for steganography," 2010, *arXiv:1003.4086*. [Online]. Available: https://arxiv.org/abs/1003.4086

[52] P. M. S. Raja and E. Baburaj, "An efficient data embedding scheme for digital images based on particle swarm optimization with LSBMR," in *Proc. 3rd Int. Conf. Comput. Intell. Inf. Technol. (CIIT)*, 2013, pp. 17–24.

[53] A. W. Naji, S. A. Hameed, M. R. Islam, B. B. Zaidan, T. S. Gunawan, and A. A. Zaidan, "'Stego-analysis chain, session two' novel approach of stego-analysis system for image file," in *Proc. Int. Assoc. Comput. Sci. Inf. Technol.-Spring Conf.*, Apr. 2009, pp. 410–413.

[54] M. A. Ahmed, M. L. M. Kiah, B. B. Zaidan, and A. A. Zaidan, "A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm," *J. Appl. Sci.*, vol. 10, no. 1, pp. 59–64, 2010.

[55] R. Islam, A. W. Naji, A. A. Zaidan, and B. B. Zaidan, "New system for secure cover file of hidden data in the image page within executable file using statistical steganography techniques," *Int. J. Comput. Sci. Inf. Secur.*, vol. 7, no. 1, pp. 273–279, 2009.

[56] A. A. Zaidan, B. Zaidan, and F. Othman, "New technique of hidden data in PE-file with in unused area one," *Int. J. Comput. Elect. Eng.*, vol. 1, no. 5, pp. 642–650, 2009.

[57] H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation," *J. Comput.*, vol. 1, no. 1, pp. 108–113, Dec. 2009.

[58] M. Abomhara, O. O. Khalifa, A. A. Zaidan, B. B. Zaidan, O. Zakaria, and A. Gani, "An experiment of scalable video security solution using H.264/AVC and advanced encryption standard (AES): Selective cryptography," *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 4053–4063, 2011.

[59] H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "New design for information hiding with in steganography using distortion techniques," *Int. J. Eng. Technol.*, vol. 2, no. 1, p. 72, 2010.

[60] M. Elnajjar, A. A. Zaidan, B. B. Zaidan, M. E. M. Sharif, and H. Alanazi, "Optimization digital image watermarking technique for patent protection," *J. Comput.*, vol. 2, no. 3, pp. 142–148, 2010.

[61] A.-N. Yahya, A. A. Zaidan, B. B. Zaidan, H. A. Jalab, and H. O. Alanazi, "A new system for hidden data within header space for EXE-file using object oriented technique," in *Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol.*, vol. 7, 2010, pp. 9–13.

[62] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[63] A. K. Al-Frajat, H. A. Jalab, Z. M. Kasirun, A. A. Zaidan, and B. B. Zaidan, "Hiding data in video file: An overview," *J. Appl. Sci.*, vol. 10, no. 15, pp. 1644–1649, 2010.

[64] A. A. Zaidan, B. B. Zaidan, O. Hamdan Alanazi, A. Gani, O. Zakaria, and G. M. Alam, "Novel approach for high (secure and rate) data hidden within triplex space for executable file," *Sci. Res. Essays*, vol. 5, no. 15, pp. 1965–1977, 1965.

[65] M. Abomhara, O. O. Khalifa, O. Zakaria, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Suitability of using symmetric key to secure multimedia data: An overview," *J. Appl. Sci.*, vol. 10, no. 15, pp. 1656–1661, 2010.

[66] A. K. Hmood, H. A. Jalab, Z. M. Kasirun, B. B. Zaidan, and A. A. Zaidan, "On the capacity and security of steganography approaches: An overview," *J. Appl. Sci.*, vol. 10, no. 16, pp. 1825–1833, 2010.

[67] A. H. Ali, L. E. George, A. A. Zaidan, and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 31487–31516, Jun. 2018.

[68] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed, "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Comput. Standard Interfaces*, vol. 66, Oct. 2019, Art. no. 103343.

[69] S. U. Maheswari and D. J. Hemanth, "Performance enhanced image steganography systems using transforms and optimization techniques," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 415–436, 2017.

[70] A. W. Naji, A. A. Zaidan, B. B. Zaidan, and I. A. S. Muhamadi, "Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard," *Proc. World Acad. Sci. Eng. Technol.*, vol. 56, no. 5, pp. 498–502, 2010.

[71] B. B. Zaidan, A. A. Zaidan, A. Taqa, G. M. Alam, M. L. M. Kiah, and A. H. Jalab, "StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem," *Int. J. Phys. Sci.*, vol. 5, no. 11, pp. 1796–1806, 2010.

[72] A. A. Zaidan, B. B. Zaidan, Y. A. Taqa, M. K. Sami, G. M. Alam, and A. H. Jalab, "Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem," *Int. J. Phys. Sci.*, vol. 5, no. 11, pp. 1776–1786, 2010.

[73] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Comput. Standard Interfaces*, vol. 64, pp. 41–60, May 2019.

[74] M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, A. M. Ahmed, and S. H. Al-bakri, "A review of audio based steganography and digital watermarking," *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 3837–3850, 2011.

[75] Y. Salem, M. Abomhara, O. O. Khalifa, A. A. Zaidan, and B. B. Zaidan, "A review on multimedia communications cryptography," *Res. J. Inf. Technol.*, vol. 3, no. 3, pp. 146–152, 2011.

[76] S. A. Hameed, B. B. Zaidan, A. A. Zaidan, A. W. Naji, and O. Faroq, "Novel simulation framework of three-dimensional skull bio-metric measurement," *Int. J. Comput. Sci. Eng.*, vol. 1, no. 3, pp. 269–274, 2009.

[77] S. A. Hameed, B. B. Zaidan, A. A. Zaidan, A. W. Naji, and O. F. Tawfiq, "An accurate method to obtain bio-metric measurements for three dimensional skull," *J. Appl. Sci.*, vol. 10, no. 2, pp. 145–150, 2010.

[78] A. K. Hmood, B. B. Zaidan, A. A. Zaidan, and H. A. Jalab, "An overview on hiding information technique in images," *J. Appl. Sci.*, vol. 10, no. 18, pp. 2094–2100, Dec. 2010.

[79] A. Hamdan, H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "New frame work of hidden data with in non multimedia file," *Int. J. Comput. Netw. Secur.*, vol. 2, no. 1, pp. 46–54, 2010.

[80] A. H. Shihab, B. B. Zaidan, A. A. Zaidan, A. W. Naji, and F. Omar, "Accurate method to measure three dimensional skull bio-metric," *J. Appl. Sci.*, vol. 10, no. 2, pp. 145–150, 2010.

[81] A. A. Zaidan, B. B. Zaidan, A. K. Al-Frajat, and H. A. Jalab, "Investigate the capability of applying hidden data in text file: An overview," *J. Appl. Sci.*, vol. 10, no. 17, pp. 1916–1922, 2010.

[82] A. K. Sahu and G. Swain, "Information hiding using group of bits substitution," *Int. J. Commun. Antenna Propag.*, vol. 7, no. 2, pp. 2–8, 2017.

[83] B. B. Zaidan, A. A. Zaidan, H. Abdul Karim, and N. N. Ahmad, "A new digital watermarking evaluation and benchmarking methodology using an external group of evaluators and multi-criteria analysis based on 'large-scale data,"' *Softw., Pract. Exper.*, vol. 47, no. 10, pp. 1365–1392, Oct. 2017.

[84] B. B. Zaidan and A. A. Zaidan, "Software and hardware FPGA-based digital watermarking and steganography approaches: Toward new methodology for evaluation and benchmarking using multi-criteria decision-making techniques," *J. Circuits, Syst. Comput.*, vol. 26, no. 7, Jul. 2017, Art. no. 1750116.

[85] B. B. Zaidan, A. A. Zaidan, H. A. Karim, and N. N. Ahmad, "A new approach based on multi-dimensional evaluation and benchmarking for data hiding techniques," *Int. J. Inf. Technol. Decis. Making*, vol. 16, pp. 1–42, 2017.

[86] B. B. Zaidan and A. A. Zaidan, "Comparative study on the evaluation and benchmarking information hiding approaches based multi-measurement analysis using TOPSIS method with different normalisation, separation and context techniques," *Measurement*, vol. 117, pp. 277–294, May 2018.

[87] A. H. Mohsin, "Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: A multi-layer systematic review," *J. Med. Syst.*, vol. 42, no. 12, p. 238, 2018.

[88] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, 2014.

[89] M. Najjarzadeh and A. Ayatollahi, "A comparison between genetic algorithm and PSO for linear phase FIR digital filter design," in *Proc. Int. Conf. Signal Process. (ICSP)*, Oct. 2008, pp. 2134–2137.

[90] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri, A. S. Albahri, M. Alaa, F. M. Jumaah, M. Talal, K. L. Tan, W. L. Shir, and C. K. Lim, "A survey on communication components for IoT-based technologies in smart homes," *Telecommun. Syst.*, vol. 69, no. 1, pp. 1–25, 2018.

[91] A. A. Zaidan, "A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: Coherent taxonomy, open issues and recommendation pathway solution," *Health Technol.*, vol. 8, no. 4, pp. 223–238, Sep. 2018.

[92] O. S. Albahri, A. S. Albahri, K. I. Mohammed, A. A. Zaidan, B. B. Zaidan, M. Hashim, and O. H. Salman, "Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations," *J. Med. Syst.*, vol. 42, no. 5, p. 80, 2018.

[93] A. A. Zaidan and B. B. Zaidan, "A review on intelligent process for smart home applications based on IoT: Coherent taxonomy, motivation, open challenges, and recommendations," *Artif. Intell. Rev.*, vol. 51, pp. 1–25, 2018.

[94] M. A. Alsalem, A. A. Zaidan, B. B. Zaidan, M. Hashim, O. S. Albahri, A. S. Albahri, A. Hadi, and K. I. Mohammed, "Systematic review of an automated multiclass detection and classification system for acute Leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects," *J. Med. Syst.*, vol. 42, no. 11, p. 204, 2018.

[95] M. A. Alsalem, A. A. Zaidan, B. B. Zaidan, M. Hashim, H. T. Madhloom, N. D. Azeez, and S. Alsyisuf, "A review of the automated detection and classification of acute leukaemia: Coherent taxonomy, datasets, validation and performance measurements, motivation, open challenges and recommendations," *Comput. Methods Programs Biomed.*, vol. 158, pp. 93–112, May 2018.

[96] A. S. Albahri, A. A. Zaidan, O. S. Albahri, B. B. Zaidan, and M. A. Alsalem, "Real-time fault-tolerant mHealth system: Comprehensive review of healthcare services, opens issues, challenges and methodological aspects," *J. Med. Syst.*, vol. 42, no. 8, p. 137, 2018.

[97] O. S. Albahri, A. A. Zaidan, B. B. Zaidan, M. Hashim, A. S. Albahri, and M. A. Alsalem, "Real-time remote health-monitoring systems in a medical centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects," *J. Med. Syst.*, vol. 42, no. 9, p. 164, 2018.

[98] O. Zughoul, F. Momani, O. H. Almasri, A. A. Zaidan, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, A. S. Albahri, and M. Hashim, "Comprehensive insights into the criteria of student performance in various educational domains," *IEEE Access*, vol. 6, pp. 73245–73264, 2018.

[99] M. Khatari, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, and M. A. Alsalem, "Multi-criteria evaluation and benchmarking for active queue management methods: Open issues, challenges and recommended pathway solutions," *Int. J. Inf. Technol. Decision Making*, vol. 18, no. 4, pp. 1187–1242, Apr. 2019.

[100] M. Talal, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, A. S. Albahri, A. H. Alamoodi, M. L. M. Kiah, F. M. Jumaah, and M. Alaa, "Comprehensive review and analysis of anti-malware apps for smartphones," *Telecommun. Syst.*, vol. 72, no. 2, pp. 285–337, 2019.

[101] N. M. Napi, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, and A. S. Albahri, "Medical emergency triage and patient prioritisation in a telemedicine environment: A systematic review," *Health Technol.*, pp. 1–22, 2019.

[102] M. L. Shuwandy, B. B. Zaidan, A. A. Zaidan, and A. S. Albahri, "Sensor-based mhealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review," *J. Med. Syst.*, vol. 43, no. 2, p. 33, Aug. 2019.

[103] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem, C. K. Lim, K. L. Tan, W. L. Shir, and K. I. Mohammed, "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *J. Med. Syst.*, vol. 43, no. 3, p. 42, Mar. 2019.

[104] E. M. Almahdi, A. A. Zaidan, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, and A. S. Albahri, "Mobile patient monitoring systems from a benchmarking aspect: Challenges, open issues and recommended solutions," *J. Med. Syst.*, vol. 43, no. 7, p. 207, 2019.

[105] K. Mohammed, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, A. S. Albahri, A. Hadi, and M. Hashim, "Real-time remote-health monitoring systems: A review on patients prioritisation for multiple-chronic diseases, taxonomy analysis, concerns and solution procedure," *J. Med. Syst.*, vol. 43, no. 7, p. 223, 2019.

[106] Y. Prasad, K. K. Biswas, and M. Hanmandlu, "A recursive PSO scheme for gene selection in microarray data," *Appl. Soft Comput.*, vol. 71, pp. 213–225, Oct. 2018.

[107] H. A. AlSattar, A. A. Zaidan, B. B. Zaidan, M. R. A. Bakar, R. T. Mohammed, O. S. Albahri, M. A. Alsalem, and A. S. Albahri, "MOGSABAT: A metaheuristic hybrid algorithm for solving multi-objective optimisation problems," *Neural Comput. Appl.*, vol. 30, pp. 1–15, Oct. 2018.

[108] H. A. Alsattar, A. A. Zaidan, and B. B. Zaidan, "Novel meta-heuristic bald eagle search optimisation algorithm," *Artif. Intell. Rev.*, Jul. 2019.

[109] F. O. Sameer, M. R. Abu Bakar, A. A. Zaidan, and B. B. Zaidan, "A new algorithm of modified binary particle swarm optimization based on the Gustafson-Kessel for credit risk assessment," *Neural Comput. Appl.*, vol. 31, no. 2, pp. 337–346, Jul. 2017.

[110] A. A. Zaidan, B. Atiya, M. R. A. Bakar, and B. B. Zaidan, "A new hybrid algorithm of simulated annealing and simplex downhill for solving multiple-objective aggregate production planning on fuzzy environment," *Neural Comput. Appl.*, vol. 31, no. 6, pp. 1823–1834, Jul. 2017.

[111] A. M. Nickfarjam, H. Ebrahimpour-Komleh, and A. P. Najafabadi, "Image hiding using neighborhood similarity," in *Proc. 6th Conf. Inf. Knowl. Technol. (IKT)*, May 2014, pp. 79–82.

[112] P. Bedi, R. Bansal, and P. Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance," *Comput. Elect. Eng.*, vol. 39, no. 2, pp. 640–654, 2013.

[113] Y. E. A. Al-Salhi, L. Songfeng, A. A. G. Al-Hamodi, A. H. Al-Mter, and Z. Zhangv, "New Qubits steganography algorithm to conceal a secret file in compressed edge detection operators based on optimized adaptive neural networks," in *Proc. Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 167–176.

[114] N. N. El-Emam, "New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization," *Comput. Secur.*, vol. 55, pp. 21–45, Nov. 2015.

[115] P. Rajeswari, P. Shwetha, and S. Purushothaman, "Application of wavelet and particle swarm optimization in steganography," in *Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)*, Mar. 2017, pp. 129–132.

[116] S. I. Nipanikar, V. H. Deepthi, and N. Kulkarni, "A sparse representation based image steganography using particle swarm optimization and wavelet transform," *Alexandria Eng. J.*, vol. 57, no. 4, pp. 2343–2356, 2017.

[117] S. Sajasi and A. M. E. Moghadam, "An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method," *Appl. Soft Comput.*, vol. 30, pp. 375–389, May 2015.

[118] Z. Li and Y. He, "Steganography with pixel-value differencing and modulus function based on PSO," *J. Inf. Secur. Appl.*, vol. 43, pp. 47–52, Dec. 2018.

[119] D. J. Hemanth, S. Umamaheswari, D. E. Popescu, and A. Naaji, "Application of genetic algorithm and particle swarm optimization techniques for improved image steganography systems," *Open Phys.*, vol. 14, no. 1, pp. 452–462, 2016.

[120] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, Mar. 2004.

[121] A. Thamallah, A. Sakly, and F. M'Sahli, "A new constrained PSO for fuzzy predictive control of quadruple-tank process," *Measurement*, vol. 136, pp. 93–104, Mar. 2019.

[122] J. Matos, R. P. V. Faria, I. B. R. Nogueira, J. M. Loureiro, and A. M. Ribeiro, "Optimization strategies for chiral separation by true moving bed chromatography using particles swarm optimization (PSO) and new parallel PSO variant," *Comput. Chem. Eng.*, vol. 123, pp. 344–356, Apr. 2019.

[123] L. Hongbo and A. Abraham, "Fuzzy adaptive turbulent particle swarm optimization," in *Proc. 5th Int. Conf. Hybrid Intell. Syst. (HIS)*, Nov. 2005, pp. 445–450.

[124] Y. Sun and F. Liu, "Selecting cover for image steganography by correlation coefficient," in *Proc. 2nd Int. Work. Educ. Technol. Comput. Sci. (ETCS)*, vol. 2, Mar. 2010, pp. 159–162.

[125] A. K. Sahu and G. Swain, "An improved data hiding technique using bit differencing and LSB matching," *Internetworking Indonesia J.*, vol. 10, no. 1, pp. 17–21, 2018.

[126] A. K. Sahu and G. Swain, "An optimal information hiding approach based on pixel value differencing and modulus function," *Wireless Pers. Commun.*, vol. 108, no. 1, pp. 159–174, 2019.

[127] A. K. Sahu and G. Swain, "A novel n-rightmost bit replacement image steganography technique," *3D Res.*, vol. 10, no. 1, pp. 1–2, 2019.

[128] A. K. Sahu, G. Swain, and E. S. Babu, "Digital image steganography using bit flipping," *Cybern. Inf. Technol.*, vol. 18, no. 1, pp. 69–80, 2018.

[129] A. K. Sahu and G. Swain, "Pixel overlapping image steganography using PVD and modulus function," *3D Res.*, vol. 9, no. 3, p. 40, 2018.

[130] S. Saini, B. A. Rambli, D. Rohaya, M. N. B. Zakaria, and S. B. Sulaiman, "A review on particle swarm optimization algorithm and its variants to human motion tracking," *Math. Problems Eng.*, vol. 2014, pp. 13–15, Nov. 2014.

[131] M. S. Sohail, M. O. B. Saeed, S. Z. Rizvi, M. Shoaib, and A. U. H. Sheikh, "Low-complexity particle swarm optimization for time-critical applications," pp. 1–24, 2014, *arXiv:1401.0546*. [Online]. Available: https://arxiv.org/abs/1401.0546

[132] C. W. Wook, J. An, and J.-C. Yoo, "Estimation of particle swarm distribution algorithms: Combining the benefits of PSO and EDAs," *Inf. Sci.*, vol. 192, pp. 109–119, Jun. 2012.

[133] S. Wang, F. Zheng, and L. Xu, "Comparison between particle swarm optimization and genetic algorithm in artificial neural network for life prediction of NC tools," *J. Adv. Manuf. Syst.*, vol. 7, no. 1, pp. 1–7, 2008.

A. H. MOHSIN received the B.Sc. degree in software engineering from Al-Sadiq University, Baghdad, Iraq, in 2008, and the M.Sc. degree in software engineering from Hamdard University, New Delhi, India, in 2013. He is currently pursuing the Ph.D. degree with Universiti Pendidikan Sultan Idris (UPSI), Tanjung Malim, Malaysia. He is currently working as a Manger Assistance with the Presidency of Ministries, Establishment of Martyrs, Baghdad. He led or was a member of many funded research projects. He has published more than ten articles in various international prestige journals. His research areas include data security, software engineering, and medical informatics.

A. A. ZAIDAN received the B.Eng. degree (Hons.) in computer engineering from the University of Technology, Baghdad, Iraq, in 2004, the M.Sc. degree in data communications and computer network from the University of Malaya, Malaysia, in 2009, and the Ph.D. degree in artificial intelligence from Multimedia University, Malaysia, in 2013. He led or was a member of many funded research projects. He is currently a Senior Lecturer with the Department of Computing, University Pendidikan Sultan Idris. He has published more than 150 articles in various international conferences and journals. His research areas include artificial intelligence, decision theory, data communication and networks, AI applications on telemedicine, and e-health.

B. B. ZAIDAN received the B.Sc. degree in applied mathematics from Al-Nahrain University, Baghdad, Iraq, in 2004, and the M.Sc. degree in data communications and information security from the University of Malaya, Malaysia, in 2009. He led or was a member of many funded research projects. He is currently a Senior Lecturer with the Department of Computing, University Pendidikan Sultan Idris. He has published more than 150 articles in various international conferences and journals. His research areas include artificial intelligence, decision theory, information security and networks, and multicriteria evaluation and benchmarking.

O. S. ALBAHRI received the B.Sc. degree in computer science from Al Turath University College, Baghdad, Iraq, in 2011, the M.Sc. degree in computer science and communication from Arts, Sciences and Technology University in Lebanon, Beirut, Lebanon, in 2014, and the Ph.D. degree in artificial intelligence from Universiti Pendidikan Sultan Idris (UPSI), Tanjung Malim, Malaysia, in 2019. He is currently working as a Senior Lecturer with the Department of Computing, University Pendidikan Sultan Idris. He led or was a member for many funded research projects. He has published more than 33 articles at various international ISI/WOS journals. His research areas are decision theory, artificial intelligent, and medical informatics. He is also a member and a Reviewer in lots of prestige Clarivate Analytics Journals.

A. S. ALBAHRI received the M.Sc. degree in ICT from Arts, Sciences and Technology University in Lebanon, Beirut, Lebanon, in 2014, and the Ph.D. degree in artificial intelligence from Universiti Pendidikan Sultan Idris (UPSI), Malaysia. He is a specialist in medical informatics and health sciences. He is currently working as a Lecturer with the University of Information Technology and Communications (UOITC) and the Iraqi Commission for Computers and Informatics (ICCI). His research interests are AI applications on telemedicine, disaster management, e-health, m-health, machine learning, multicriteria decision-making (MCDM), the IoT, big data, and student evaluation. He has published many articles in WoS (ISI) databases under affiliation A.S. Albahri. He is also a member and a Reviewer in lots of prestige journals by Clarivate Analytics.

M. A. ALSALEM received the B.Sc. and M.Sc. degrees in computer science from the University of Mosul, Iraq, in 2010 and 2014, respectively. He is currently pursuing the Ph.D. degree with Universiti Pendidikan Sultan Idris (UPSI), Tanjung Malim, Malaysia. He is currently working as a Lecturer with the University of Mosul. He led or was a member for many funded research projects. He has published more than 25 articles at various international journals. His research areas are machine learning, telemedicine, and multicriteria decision making.

K. I. MOHAMMED received the M.Sc. degree in computer Science from Anbar University, Iraq, in 2014, and the Ph.D. degree in artificial intelligence from Universiti Pendidikan Sultan Idris (UPSI), Malaysia. He is a specialist in medical informatics and health sciences. He is currently working as a Lecturer with Sunni Endowment Diwan. His research interests are AI applications on telemedicine, disaster management, e-health, m-health, machine learning, multicriteria decision-making (MCDM), the IoT, bigdata, and student evaluation. He has published many articles in WoS (ISI) databases under affiliation K. I. Mohammed. He is also a member and a Reviewer in lots of prestige journals by Clarivate Analytics.

SHAHAD NIDHAL received the B.Sc. degree in electrical and electronics engineering from the University of Technology, Iraq, in 1999, and the M.Sc. degree in electrical engineering and the Ph.D. degree from UKM University, Malaysia, in 2005 and 2012, respectively. He is working as a Lecturer with MSU University. He led or was a member for many funded research projects. He has published more than seven articles at various international conferences and journals. His research areas are pattern recognition, digital signal processing, signal processing, biomedical signal processing, and renewable energy.

NAWAR. S. JALOOD received the B.Sc. degree in software engineering from the University of Imam Ja'afar Al-Sadiq, Baghdad, Iraq, in 2013, and the M.Sc. degree in computer science/information technology from Upsi University, Malaysia, in 2018. He is also graduated from Universiti Pendidikan Sultan Idris (Upsi), Tanjung Malim, Malaysia. He is currently working as a Senior Engineer with the Ministry of Education, Iraq. His research areas are education application, decision making, artificial intelligent, and medical informatics.

ALI NAJM JASIM received the B.Sc. degree in software engineering from the University of Imam Ja'afar Al-Sadiq, Baghdad, Iraq, in 2012, and the M.Sc. degree in computer science/information technology from Upsi University, Malaysia, in 2018. He is also graduated from Universiti Pendidikan Sultan Idris (Upsi), Tanjung Malim, Malaysia. He is currently working as an Engineer with the Foundation of Alshuhda, Iraq. His research areas are education application, decision making, artificial intelligent, and medical informatics.

ALI. H. SHAREEF received the B.Sc. degree in software engineering from the University of Imam Ja'afar Al-Sadiq, Baghdad, Iraq, in 2013, and the M.Sc. degree in computer science/information technology from Upsi University, Malaysia, in 2018. He is also graduated from Universiti Pendidikan Sultan Idris (Upsi), Tanjung Malim, Malaysia. He is currently working as a Lecturer with the University of Thi-Qar, Iraq. His research areas are education application, decision making, artificial intelligent, and medical informatics.