International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, 2020 pp.652-662

Improving Security in Mechanical Robots through Steganography Using a Hybrid Method Based on Meta-heuristic Algorithms

Ladan Riazi[1], Alireza Pourebrahimi[2*], Mahmood Alborzi[3], Reza Radfar[4]

[1]*Department of Information Technology Management, Science and Research Branch, Islamic Azad University, Tehran, Iran.*

[2]*Department of Industrial Management, Karaj Branch, Islamic Azad University, Karaj, Iran.*

[3]*Department of Information Technology Management, Science and Research Branch, Islamic Azad University, Tehran, Iran.*

[4]*Department of Technology Management, Science and Research Branch, Islamic Azad University, Tehran, Iran.*

Abstract:

In this paper, a method is proposed to improve the security of gathered information by mechanical robot sensors through Steganography Using a Hybrid Method Based on Meta-heuristic Algorithms. In this method, the desired information is first encoded into pre-stored images and then the image containing the information, stored or sent to the control center. When needed, information is extracted from the image. This way, using steganography, secret information are embedded into the image, and the security of the information collected by the robot is maintained. It is very important to maintain image quality after steganography. Combined method based on meta-heuristic algorithms contains firefly, bee and cuckoo search algorithms is used for steganography. According to the results, after the steganography with the mentioned method, the average PSNR which is used as the image quality assessment index has improved 39.58% compared to the simple LSB method, which is a significant percentage.

Keywords: *Mechanical robot, security, steganography, meta-heuristic algorithms.*

1. Introduction

Nowadays, robots are widely used in various fields of industry, space, medicine, military, education, home, etc. and play a vital role in human life. For example, they are used to obtain environmental information in locations with difficult or restricted accessibility and to send the collected information to the control center.

The information collected by robots is often secret (confidential) and sensitive, and protecting the security of the information sent by the robot is crucial. For example, robots are used to search and detect critical locations in military operations. In particular, for robots that are controlled online via a remote Internet connection, it is possible that unauthorized individuals may access the information collected by the robot. Therefore, it is necessary to provide some security solutions to protect the information.

Various sensors are employed to detect the environment depending on the type of information the robot requires including distance, color, light, sound, motion, and vibration (piezoelectric), temperature, smoke, etc. Sensors provide the information required by the robot and convert the desired physical or chemical quantities into electrical signals. This information is sent to the robot control center (RCC) after processing. This paper presents a method to safeguard the information collected by robot sensors.

Image steganography is one of the most common methods currently used to protect information security.

ISSN: 2233-7857 IJFGCN

Steganographic techniques are applied to embed and send secret messages through a digital medium so that no suspicion arises that the information is in the host medium. The main purpose here is to conceal the existence of secret information. Steganographic algorithms make some small changes to embed secret information into host data so that it is invisible to the naked eye. Since the human eye shows less sensitivity to changes in images, in image steganography, images are considered to be a suitable coverage medium for embedding secret information.

This paper presents a method for enhancing security in sending robot sensor information using hybrid steganography based upon metaheuristic algorithms.

In this method, first, the information is hidden in pre-stored images. Then, the stego image is saved or sent to the control center. The required information is extracted from the image as needed.

Thus, security and sensitive information are embedded inside the image and the security of the collected information is maintained by the robot using the image steganography technique. One of the benefits of the proposed method is that people cannot see the message and the intruder is not aware of the information embedded inside the image.

Obviously, the image quality and consequently the transparency of steganography is reduced by an increase in the data embedded inside the image. Hence, the security of the hidden message is compromised [1]. Therefore, a method with the least impact on quality should be used.

This study uses the hybrid steganography technique based on metaheuristic algorithms [2], a combination of firefly (FF), artificial bee colony (ABC), and cuckoo search (CS) algorithms to hide sensor information inside the image.

One of the well-known methods in image steganography is the Least Significant Bit (LSB) substitution method. Digital images generally consist of a 2D array of pixels each containing eight bits (in black and white images) and 24 bits (in color images). The LSB hides the information in the right-most bit in each pixel. The effect of the LSB method on image quality depends on the number of bits used for steganography. If a suitable substitution matrix is used, the information hiding quality is increased in LSB-Steganography [3]. This n*n matrix is aimed at converting some colors to other colors to reduce the detrimental effect of the LSB method on image quality (n equals 2r and r is the number of bits used per pixel to replace). The quality of the stego images is evaluated using the PSNR value (described in Section 2.1). Thus, the aim here is to select a suitable substitution matrix so that the PSNR value is maximized after applying the matrix. As the number of bits used for substitution increases, the search space for creating a suitable substitution matrix increases significantly. Hence, metaheuristic algorithms can be used as one of the solutions to this problem [18].

Until now, a number of studies have been carried out on the use of metaheuristic algorithms, including the genetic algorithm (GA) [4] and cat swarm optimization (CSO) [5], to obtain a suitable substitution matrix. Moreover, in another study [6], the combination of two metaheuristic algorithms, namely particle motion and simulated annealing, to obtain the substitution matrix improved the quality of steganography. In [7], the particle swarm optimization (PSO) algorithm is used to obtain the substitution matrix yielding better results compared to the GA. In [8], a method is proposed by combining genetic metaheuristic algorithms and PSO as well as applying chaos theory. In this study, the message is encrypted by one of the chaotic functions before embedding it into the image. The author claims that the proposed method improves implementation speed and security.

In [9], the ant colony optimization (ACO) metaheuristic algorithm is used to find suitable substitution pixels. According to the results, the proposed method improves the PSNR value compared to the simple LSB method and DCT-M3 [10]. ACO algorithm has also been used in [1] to create an optimal substitution matrix.

ISSN: 2233-7857 IJFGCN

In [11], the CS algorithm was used to select appropriate pixels in image steganography. Levy flight is used to move randomly between pixels. Evaluation of the results showed that this study was able to significantly improve the PSNR value compared to the GA and simple LSB. In [12], a combination of data mapping methods and GAs has been used for image steganography. Two bits of the "secret message" is stored in each image pixel. There are eight different locations to place two bits of the "secret message" in each pixel using the gray image. Mapping coefficients are generated based on where both message bits stored per pixel; for example, 0 for 010001 **, 1 for 01000**0, 2 for 0100**00, etc. The secret message is stored in one-quarter of the image using this method and the rest of the image pixels are used to store the mapping coefficients. The GA is used to embed the coefficients in the appropriate pixels in the remainder of the image. According to the results of this study, this method has managed to contribute to 1.7% (on average) improvement in the PSNR value of the stego image compared to the simple LSB method.

This study aims to increase the quality of the stego image (reduced degradation) and subsequently to increase the transparency of steganography using the hybrid metaheuristic method to obtain the optimal substitution matrix in the LSB method. In steganography, three factors, namely capacity, resistance, and transparency are usually investigated and it is attempted to observe each of these factors as needed given the applications, premises, and other conditions.

Capacity: Hiding capacity (payload) is the amount of information that can be stored according to the type of coverage medium. The higher this capacity, the smaller the coverage medium available for a fixed-size message, so the required bandwidth is reduced.

Resistance: The resistance of an information steganographic system means that the hidden message resistant enough to unwanted and unintentional changes made during the transmission path (e.g., noise) or intentional changes by the active attacker to modify or destroy the message. Common attacks include linear or nonlinear filtering, noise addition, blurring or sharpening, image resizing, and lossy compression.

Transparency (imperceptibility or indiscernibility): This determines the ability of the steganographic algorithm to hide data in the coverage medium so as not to attract the attention of others. In other words, hiding must be done so as to maintain the original quality of the coverage medium as much as possible. Maintaining the original quality of the coverage medium makes the hidden data less observable and there is no comprehensible difference for human senses. The transparency of the system states that there should be no noticeable difference in the coverage medium before and after message embedding because the purpose here is to convey the message in an indiscernible way. The security of a steganographic system depends on transparency.

In image steganography, the greater the similarity between the original image and the image containing the secret message, the higher the security because it will make the steganography less discernable, thereby reducing any suspicion of the message being present inside the image.

This study aims to enhance the security in sending robot sensor information by hiding the information contained within pre-stored images (i.e., unrealistic and misleading images for intruders) so that image transparency is maintained as much as possible after steganography.

2. Methodology

This study uses a hybrid method based on metaheuristic algorithms to maintain the quality of the stego image to hide the information received from robot sensors [2]. This method uses a combination of three algorithms, i.e., FF, ABC, and CS to develop an optimal substitution matrix for image steganography using the LSB method. Indeed, the optimal response of an algorithm is considered as the primary input of another algorithm. Below is a full description of the method above.

2.1. Fitness Function Used in This Study

ISSN: 2233-7857 IJFGCN

Since parameters PSNR and MSE are used to evaluate image quality in image processing problems, this study also uses the PSNR value as the fitness function to evaluate the stego image quality [13], [14], and [15]. PSNR is a metric criterion for evaluating the image reconstruction quality associated with perceptual quality calculated in dB based on the following formula:

$$PSNR = 10 * \log_{10}({}^{255^2}/_{MSE}) \quad (1)$$

$$MSE = \frac{1}{W*H} \sum_{i=1}^{W} \sum_{j=1}^{H} (s_{ij} - c_{ij})^2 \quad (2)$$

Where i and j are the image coordinates, c_{ij} and s_{ij} are pixel $_{ij}$ intensities in the original image and the image obtained, respectively. W and H are the number of pixels in length and width of the primary image (i.e., image dimensions). The greater the difference between the original and obtained images, the MSE increases and the PSNR decreases. Moreover, the lower the MSE value and thus the higher the PSNR value, the closer the quality of the stego image is to that of the original one. Therefore, a higher PSNR means less noise and higher quality of the image obtained.

2.2. Images Used

Standard color images in the field of image processing with a rich color spectrum (i.e., RGB) have been used to evaluate the method. A standard test image is a digital image file used by various institutions to perform image processing tests and image compression algorithms. Various researchers and laboratories can compare results, both visually and quantitatively, using the same standard test images. USC-SIPI standard test images have been used with respect to the necessity of comparing and evaluating the methodology of this study with that of other similar studies in image steganography. Therefore, the samples were selected based on a literature review from the standard images used inside the image steganography literature including references [16], [17], and numerous other studies.

2.3. Application of the Firefly Algorithm

The firefly (FF) algorithm works by modeling the behavior of a set of fireflies and assigning a value corresponding to the location of each firefly. In this algorithm, the amount of luciferin is modeled. Updating the firefly position is examined in successive iterations to obtain the optimal solution in this algorithm. This algorithm has two main phases: the luciferin update phase and the firefly movement phase. Fireflies move toward other fireflies in their neighborhood with a luciferin higher than their own. Thus, the set tends to a better response during successive iterations.

The firefly attractiveness level is determined by its brightness that depends on the objective function. As firefly attractiveness is proportional to the light intensity seen by adjacent fireflies, attractiveness β_0 of firefly can be defined as follows:

β (r)= β_0e-yr2 (3)

where β_0, y, and r are the predefined attractiveness level, the optical absorption coefficient, and the distance between firefly i and firefly j, respectively. The distance between firefly i and firefly j in X_i and X_j can be shown as follows:

$$r_{ij} = \left\| x_i + x_j \right\| = \sqrt{\sum_{k=1}^{d} \left(x_{i,k} - x_{j,k}\right)^2} \quad (4)$$

where X_{ik} is the K_{th} part of the spatial coordinates (X_i) of firefly i. r_{ij} is displayed in a 2D mode as follows:

$$r_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \quad (5)$$

ISSN: 2233-7857 IJFGCN

The movement of firefly i and its attraction to the brighter firefly j is determined as follows:

$$x_i = x_i + \beta_0 e^{-\gamma r_{ij}^2}(x_j - x_i) + \alpha\left(rand - \frac{1}{2}\right) \quad (6)$$

rand is a random number generator in the interval [0,1].

The steps to apply the firefly algorithm to the image steganography problem are:

Step 1: Randomly initialize n fireflies.

Step 2: For each firefly i among the population of fireflies:

Embed the text into the image.

Calculate the fitness function PSNR for each image and initialize the fitness function associated with each firefly.

Step 3: Update the location of each firefly using the fitness function.

Step 4: Repeat the second and third steps until you reach the maximum number of repetitions.

Table 1 shows the values of the parameters used to apply the firefly algorithm in this study.

Table 1. Parameters used in the firefly algorithm

Parameter	Description	Value
n	Population Size	100
MaxIt	Maximum No. of Loops	50
α	Randomization Parameter	0.5
β	Attractiveness Level	0.2
r_{ij}	Distance Between Firefly i and Firefly j	Based on the Formula
y	Optical Absorption Coefficient	1

2.4. Application of the Bee Colony Optimization Algorithm

In image steganography, the bee colony optimization (BCO) algorithm first initializes the population generated by the random number generator within the specified range. The main loop of the BCO algorithm, i.e., performing the reproduction process, is generated to produce new solutions by worker bees, onlooker bees, and scout bees. Then, it is evaluated by the fitness function. This process continues until the algorithm termination (stopping) criterion is satisfied. The optimal parameters are obtained after running is complete. The solution for the best fitness function of the final generation is used to embed the information. The objective function is used to check the fitness of each candidate solution in terms of image quality and attack resistance.

First, the food sources or initial responses to the problem are initialized randomly.

$$X_{ij} = x_{min.j} + rand(0.1) * \left(x_{max.j} - x_{min.1}\right) \quad (7)$$

The fitness function is calculated for all initial responses.

Worker bees move toward food sources. Food sources are the same as the location of the bees in the problem space. Each worker bee randomly selects a neighbor and moves toward it by the following equation:

$$y_{i.j} = x_{i.j} + \varphi_{i.j} * (x_{i.j} - x_{k.j}) \quad (8)$$

ISSN: 2233-7857 IJFGCN

where $j \in \{1.2 \ldots . D\}$ and $k \in \{1.2 \ldots . SN\}$ are selected at random so that index K differs from index i. $\varphi_{i.j}$ is a random parameter between -1 and 1 that produces new solutions in the neighborhood $x_{i.j}$.

The fitness function of the new position is calculated. The bee stays in the new location if the new position is of better quality; otherwise, it returns to its former location and a unit is added to the bee trial index. This index calculates the number of consecutive bee movements with no improvement. If the bee trial index value exceeds a certain limit, the food zone shall be free of any nectar and therefore must be abandoned.

The onlooker bee chooses another food source near the received stored data and replaces the previous value with that value if the fitness function is better. The choice of a food source is calculated based on the probability of Pi as follows:

$$P_i = \frac{fit_i}{\sum_{i=1}^{SN} fit_i} \tag{9}$$

Where fit_i is the fitness function of the ith solution in the problem space. SN is the number of solutions or the number of worker bees, calculated as follows:

$$fit_i = \begin{cases} \frac{1}{f(X_i)} & if\ f(X_i) \geq 0 \\ 1 + abs\big(f(X_i)\big) & elsewhere \end{cases} \tag{10}$$

Where f(Xi) is the objective function measured in the ith food position.

Scout bees leave those areas identified as undesirable with regard to nectar and select other areas randomly. If a better food source is not found after the trial index reaches a certain limit, a new food source will be initialized randomly by the scout bees using the following equation:

$$X_{ij} = x_{min.j} + rand(0.1) * (x_{max.j} - x_{min.1}) \tag{11}$$

The algorithm is repeated until it reaches a certain value and the best response obtained from the algorithm is considered as the optimal substitution matrix. In this study, the parameters of this algorithm are set according to Table 2.

Table 2. Parameters used in the BCO algorithm

Parameter	Description	Value
n	No. of Scout Bees	20
m	No. of locations selected for local search	10
e	No. of randomly chosen locations from m locations	5
nep	No. of fresh bees for selected locations	6
t	No. of bees to be sent elsewhere	4
loop	No. of repetitions	50

2.5. Application of the Cuckoo Search Algorithm

The cuckoo optimization algorithm (COA) was first introduced in 2009 by investigating cuckoo hatchlings and how some birds and flies would fly. One of the characteristics of cuckoos is that they never make a nest for themselves and instead they lay their eggs in the nests of other birds. There are two possibilities: either the host bird becomes aware of the alien eggs or they do not. If an alien egg is discovered, it will be thrown away out of the nest or the host bird simply abandons its nest and builds a whole new nest elsewhere. Hence, cuckoos carefully choose the color and pattern of host bird eggs so that the likelihood of detecting their eggs is reduced. In the COA, each egg in the nest represents a potential solution. The reproduction process in the cuckoo search algorithm works under three assumptions:

ISSN: 2233-7857 IJFGCN

- Each cuckoo lays one egg at a time and places it in a random nest.
- The solution to the problem is the best nest with the best eggs that will continue into the next generation.
- The number of available host nests is fixed and a host can identify an alien egg with a probability *pa*. If this happens, the host can throw the alien eggs out of the nest or leave the nest.

In this study, the following steps are considered to use the cuckoo search algorithm:

- Initialize the parameters.
- Create an initial population of the host nests randomly.
- Calculate the fitness function of each nest and select the best nest.
- Produce new nests based on the Levy flight algorithm.
- Evaluate the value of the fitness function for each new nest and select the best nest.
- Compare selected nests and keep the best solution.
- Optimize the best solution.

The parameters used in the cuckoo search optimization algorithm are set according to Table 3.

Table 3. Parameters used in the cuckoo search optimization algorithm

Parameter	Description	Value
Pa	Probability of detecting cuckoo eggs	1
a	Movement of the nest to a new place	0.25
n	No. of nests	75
β	Size of random steps	1.5
loop	No. of repetitions	50

2.6. Application of the Hybrid Algorithm

As mentioned earlier, this study uses a hybrid approach based on metaheuristic algorithms and combines three algorithms, i.e., firefly algorithm, bee colony optimization algorithm, and cuckoo search algorithm to create an optimal substitution matrix for image steganography using the LSB method. Indeed, the optimal response of an algorithm is considered as the primary input of another algorithm. Figure 1 shows the steps of the hybrid algorithm used. Moreover, Figure 2 provides an overview of the image steganography process using the hybrid method. First, the collected information is introduced to the software by robot sensors as a secret message, as well as a pre-stored image and a hybrid metaheuristic algorithm to hide the text inside the image. Then, the stego image is stored or sent to the control center.

ISSN: 2233-7857 IJFGCN

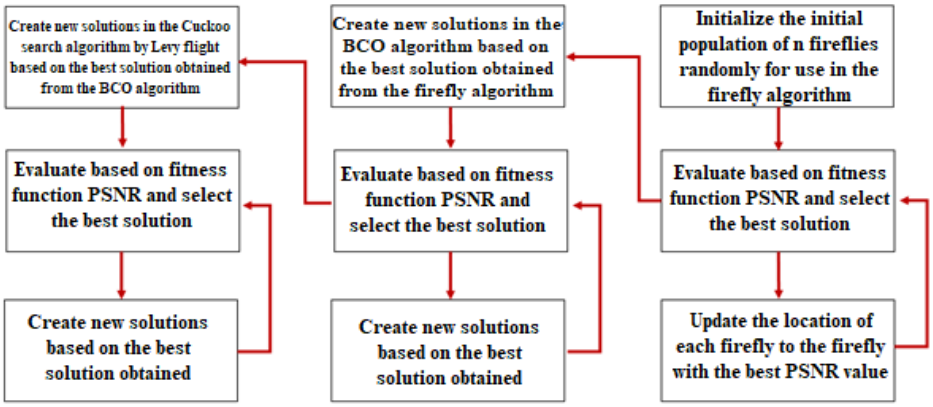

Figure 1. The algorithm used in this study to create an appropriate substitution matrix

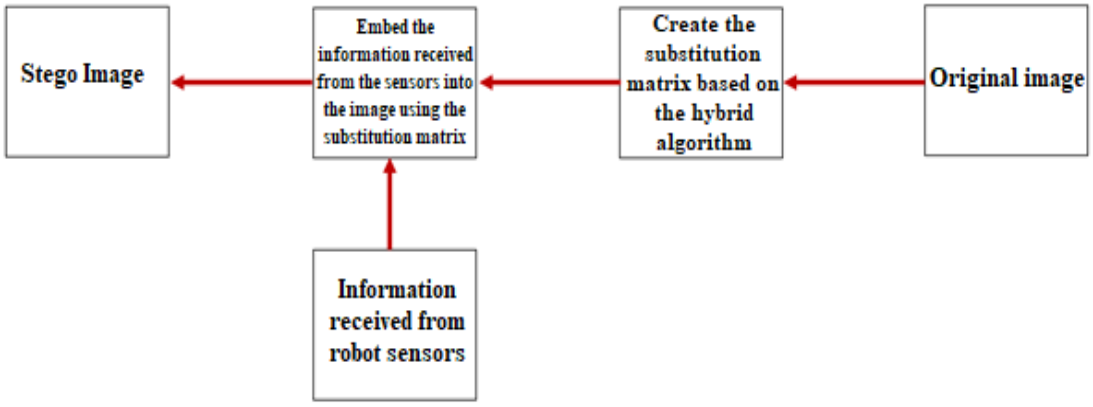

Figure 2. The steganography process before sending or storing information received by the sensors

2.7. Simulation

Depending on the type of problem, software simulation is considered as an appropriate method for evaluating different policies and proposed algorithms. MATLAB version 9.0 is used to evaluate the algorithm. The simulations are run in an environment with Intel® Core ™ i7 @ 2.3 GHz CPU and 6 GB of RAM. The operating system used is Windows 7 Ultimate 64Bit. All steps are simulated in the software and the results are evaluated based on the software output.

3. Results and Discussion

This study aims to improve the security in sending robot sensor information by hiding information inside the image so that image quality is maintained as much as possible after steganography. Table 4 presents improvements in PSNR value after applying the hybrid algorithm used in this study compared to the LSB method.

Table 4. Improvements in PSNR value after applying the hybrid algorithm using standard test images

ISSN: 2233-7857 IJFGCN

Image Name	Hybrid Algorithm Used	Improvements Over LSB (%)
Lena	57.12	41.21
Baboon	53.04	37.95
Pepper	54.52	39.45
Average	54.89	39.58

Table 5 compares the results of the proposed method with those obtained from other studies using metaheuristic algorithms in image steganography. Improvements in PSNR value after applying different methods are presented for each method compared to the simple LSB method. It compares the results of the proposed method with those of the following studies:

The PSO-SA method in [6] which uses a combination of PSO and SA algorithms.

The GA-PR method in [3] has added the path-relinking method to the GA to create a substitution matrix.

In [11], the CS method together with Levy flight has used the cuckoo search algorithm to select the appropriate pixels of the image for substitution and Levy flight to move randomly between the pixels.

The combined data mapping method and the GA has been used in [12] in which two bits of the secret message is stored in each pixel of the image. Mapping coefficients are generated based on the storage of two bits of the message in each pixel. The secret message is stored in one-quarter of the image using the mapping and the rest of the image pixels are used to store the mapping coefficients. The GA is used to embed the coefficients in the appropriate pixels in the remainder of the image.

The combination of symmetric encryption and firefly algorithm have been used in [11], which is based on symmetric encryption to encrypt text information prior to embedding and on the firefly algorithm to hide encrypted information in digital images.

Table 5. A Comparison between improvements in PSNR value in the proposed method and those obtained in other studies

No.	Algorithm	Improvements Over Simple LSB(%)
1	PSO-SA	12.63
2	GA-PR	5.41
3	CS-Levy	28.40
4	GA-Data mapping	1.70
5	Symmetric Image Steganography Firefly	11
6	Algorithm Used	39.58

Based on the results presented in the table, the proposed method has achieved a comparable improvement in PSNR value compared to other methods.

Next, the proposed algorithm was applied to 10 experimental images to hide the sensor information. Table 6 presents the results of the mean PSNR value.

Table 6. Improvements in PSNR value after applying the hybrid algorithm on a set of 10 experimental images

ISSN: 2233-7857 IJFGCN

	Application of the Hybrid Algorithm Used	Application of the LSB Method	Improvements over LSB(%)
Mean PSNR Value	55.30	39.24	40.73

4. Conclusion

Steganographic algorithms apply small changes to the host data based on the message signal to embed message signal information into the host data. Obviously, the image quality (transparency) will change with an increase in the data embedded in an image and the likelihood of being suspected of having a hidden message inside the image, thereby jeopardizing the security of the hidden message. It is very important to choose an algorithm that will preserve the original cover image quality as much as possible after steganography, as it will make the hidden data less observable, make no discernible difference to the human senses in the coverage medium, and make the message indiscernible.

This study proposed a method to enhance the security in sending robot sensor information using hybrid steganography based on metaheuristic algorithms.

In the method above, first, the information is hidden inside the pre-stored images and then the stego image is stored or sent to the control center. The required information is extracted from the image as needed.

Thus, security and sensitive information are embedded inside the image using the steganographic technique and the security of the collected information is maintained by the robot. One of the benefits of the proposed method is that the message cannot be seen by individuals and the intruder is unaware of the information embedded inside the image.

It is very important to maintain image quality after steganography. For this purpose, the hybrid metaheuristic method [2] has been used to obtain the optimal substitution matrix in the LSB method, resulting in a decrease in image quality degradation and thus an increase in the transparency of steganography compared to the conventional methods by combining firefly, bee colony optimization, and cuckoo search algorithms.

According to the results presented in Table 4, a 39.58% improvement was achieved in the mean PSNR value of the combination used compared to the simple LSB method, which is a significant percentage.

Based on the results presented in Table 5, the proposed algorithms in other studies including PSO-SA, GA-PR, CS-Levy flight, GA-Data mapping, and firefly symmetric encryption obtained a 12.63, 5.41, 28.40, 1.70, and 11% improvement in PSNR value, respectively. However, improvements in PSNR value after applying the hybrid method used in this study was 39.58%, which is higher than all values mentioned compared to the simple LSB method.

References

[1] Lakzaie, M. Khodaie, S.M. (2010). *LSB Steganography Optimization Using ACO Algorithm.* Paper presented at the 13th Iranian student's conference on electrical engineering (ISCEE), Tehran, Iran. [in Persian]

[2] Riazi, L. (2019). *Presenting a combination model to improve Steganography in images using meta-hueristic algorithms.* (Unpublished doctoral dissertation*). Islamic Azad University, Science and Research Branch,* Tehran, Iran.

[3] Brazil, A. L., Sanchez, A., Conci, A., & Behlilovic, N. (2011, September). Hybridizing genetic algorithms and path relinking for steganography. In *Proceedings ELMAR-2011* (pp. 285-288). IEEE.

ISSN: 2233-7857 IJFGCN

[4] Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern recognition*, *34*(3), 671-683.

[5] Wang, Z. H., Chang, C. C., & Li, M. C. (2012). Optimizing least-significant-bit substitution using cat swarm optimization strategy. *Information Sciences*, *192*, 98-108.

[6] Sadeghi, F., Rafsanjani, M. K., & Kermani, F. Z. (2013). Hiding Information in Image by Compound Meta-Heuristic Algorithm PSO-SA. *International Journal of Computer Science and Artificial Intelligence*, *3*(4), 125.

[7] De Carvalho, R. L., Da Silva, W. G., & de Morais, A. H. O. (2017). Optimizing image steganography using particle swarm optimization algorithm. *International Journal of Computer Applications*, *164*(7).

[8] Asgari, S., Shabani, D., Fadavi, A.M. (2018). *Hiding Information Using Combined Genetic Algorithm and Particle Swarm Using Chaos Theory*. Paper presented at the 4th National Conference on Distributed Computing and Big Data Processing, Tabriz, Iran. [in Persian]

[9] Sadeghi, F., ZARISFI, K. F., & KUCHAKI, R. M. (2015). Optimizing Image Steganography by Combining the GA and ICA. *The ISC Int'l Journal of Information Security*, *7*(1).

[10] Attaby, A. A., Ahmed, M. F. M., & Alsammak, A. K. (2017). Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. *Ain Shams Engineering Journal*.

[11] Abbas, S. A., El Arif, T. I., Ghaleb, F. F., & Khamis, S. M. (2015, December). Optimized video steganography using Cuckoo Search algorithm. In *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)* (pp. 572-577). IEEE.

[12] Shah, P. D., & Bichkar, R. S. (2018). A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator. In *International Conference on Intelligent Computing and Applications* (pp. 119-129). Springer, Singapore.

[13] Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, *81*(1), 150-158.

[14] Hussain, M., Wahab, A. W. A., Ho, A. T., Javed, N., & Jung, K. H. (2017). A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. *Signal Processing: Image Communication*, *50*, 44-57.

[15] Li, Z., & He, Y. (2018). Steganography with pixel-value differencing and modulus function based on PSO. *Journal of information security and applications*, *43*, 47-52.

[16] Suraj, A. A., Francis, M., Kavya, T. S., & Nirmal, T. M. (2014). Discrete wavelet transform based image fusion and de-noising in FPGA. *Journal of Electrical Systems and Information Technology*, *1*(1), 72-81.

[17] Hemalatha, S., Acharya, U. D., & Renuka, A. (2015). Wavelet transform based steganography technique to hide audio signals in image. *Procedia Computer Science*, *47*, 272-281.

[18] Mohammadi, F. G., & Sajedi, H. (2017). Region based image steganalysis using artificial bee colony. *Journal of Visual Communication and Image Representation*, *44*, 214-226.

ISSN: 2233-7857 IJFGCN