IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 6 - V7I6-1292)
Available online at: https://www.ijariit.com

Optimized data hiding based steganography approach to secure the confidential information in smart grid

Angrej Singh
erangrejs@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

Puneet Jain
puneetjain988@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

ABSTRACT

The standard electrical power grid is integrated with information and communication technologies in a smart grid (ICT). Such integration empowers electrical utilities providers and consumers, increases the efficiency and availability of the power system, and allows customers' needs to be continually monitored, controlled, and managed. A smart grid is a massive, complicated network made up of millions of linked objects and organisations. With such a large network comes a slew of security problems and flaws. Cryptography and steganography algorithms have been applied to give security in SG. Steganography algorithm hides the important data in the cover media to provide imperceptibility to the attacker. Image is the most essential cover media in the steganography. Least significant bit (LSB) method is used to hide the confidential information in the cover image. The hiding process provides variability in the cover image. In this paper, an optimized data hiding method is proposed to reduce the variability. The proposed method has two phases. In the first phase, the confidential information bits are matched with LSB bits of cover image pixel. For matching purposes, original or complemented form of confidential information bits is matched with cover image pixel and if match found then index is determined. In the second phase, the indexs are hided in the cover image in optimal way using the JAYA optimization algorithm. The optimization algorithm searches the optimal starting point in the cover image for index hiding. After searching the optimal starting pixel, hide the index using k-bits LSB method. The proposed method is simulated in MATLAB and performance analysis is done using various parameters. The simulation outcomes represent that the presented method is better than existing methods.

Keywords: *Confidential Information, JAYA Algorithm, Least Significant Bit, Smart Grid, Steganography.*

1. INTRODUCTION

The SG is a cutting-edge infrastructure in power systems that offers a slew of advantages, including the effective integration of RESs. However, because a vast quantity of data must be shared to successfully manage such a complex system, the SG is heavily reliant on improved communication [1]. As a result, cyber-attacks on the smart grid have increased. Next, we have discussed the most prominent attacks in the smart grid [2].

- Traffic Analysis Attack: In this attack, the attacker is monitor the communication line. In the smart grid, the smart meter periodically communicate the data to the smart grid. The data contain information of electricity usage and area. Further, this information is processed to predict electricity demand in the future. Thus, any vulnerabilities in the data negatively impact the smart grid network.
- Man-in-the-Middle Attack: The MITM attack is a sort of monitor in which the attacker attempts to establish separate connections with dangerous communication at both ends and transmits data in the middle. Furthermore, authorised users at endpoints believe in communicating directly with one another via their personal connection.
- False data injection attack: This kind of attack as a well-crafted sort of integrity attack, can have an influence on the execution as well as management of SGs through passing bad data detection systems. To disrupt the state variables, the attacker might insert bad data into a randomly picked vector. The latter is a more significant assault since the attacker has a good understanding of the network structure and can make pre-programmed modifications to state variables. When important meters are hacked, detecting harmful data assaults becomes increasingly difficult. False data injection attacks may be mitigated using several traditional strategies that safeguard specific vital sensors in the power system. The sort of attacked meters might vary, for

example, in load alteration as well as load relocation assaults, the quantity of the load meter is changed to launch a cyber attack on the SG.

- Jamming attack: is a sort of DoS attack that may be used to disrupt real-time communications. As a result of the jamming, state estimate and online checking may fail to reveal the genuine operational status of the system, and the associated power price will be determined incorrectly. The primary objective for launching the attack is to manipulate the electricity market's prices. When there is a jamming, the pricing mechanism is based on state estimates from sensors that are unavailable to the control centre.

To overcome these attacks, security algorithms are deployed in the smart grid. Cryptography and steganography is the most preferred fields [3-5]. The steganography approaches hide the confidential information in the media of cover as well as gives no special attention to the attacker [5]. Therefore, in this paper, we have find out the steganography approaches. In the literature, LSB is the most essential information hiding approach. This algorithm replace the cover image LSB bit with confidential data bit. However, data hiding process generate variability. To reduce the variability, various methods are proposed. Pratik D. Shah and R.S. Bichkar [1], match the secret data bits with the cover image pixel bits. If matched found then index is determined else data is hided using LSB method. After that, hide the indexes in the cover image using genetic algorithm. However, this method provides lesser embedding capacity. Further, Kamil et al. [2], matches the original or complemented form of secret data bits with LSB bits of the cover image pixels. After that, hides the matched index in the cover image using 2-bit LSB method. The advantage of the their method is original or complemented form of secret data bits is always matched with cover image pixel bits. However, 2-bit LSB based index hiding generates variability. These challenges are taken under consideration and designed a method that lesser variability over existing methods.

The main contribution of this paper is to secure the confidential data of smart grid using steganography. To obtain this aim, the confidential information bits are hided in the cover image in the optimal way. There are two phases of the proposed method. In the first phase, confidential data bits are matched with cover image pixels and matched index is determined. In the second phase, the matched index are hidden in the cover image in the optimal way using the JAYA algorithm. The simulation results show that the proposed method provides superior results in terms of PSNR as compared to other methods.

The other sections of the proposed article is as follows. Section 2 shows the related work. Section 3 illustrates the presented technique. Section 4 shows the simulation results. Conclusion, as well as future scope, is defined in Section 5.

2. RELATED WORK

In this section, we have reviewed the articles are published in steganography for data hiding.

Kamil et al. [6], The use of an optimal cover media match was shown to be beneficial in concealing data accurately and increasing the visual quality of steganography approaches. Several improved steganography algorithms have recently been created to protect cloud data from dangerous assaults. Although these approaches may find the best bits matches in the media of cover to hide the confidential information exactly and with less fluctuation, they take longer to compute. As a result, this research suggested a steganography approach with almost zero variability and a short processing time. Video steganography was used to accomplish and optimise the data concealment of confidential information bits in either complemented or non-complemented forms. In addition, in the covered frame, the indices for the complemented as well as non-complemented forms were obscured. When extracting the secret messages, this allowed information to be sent effectively to the receiver. Various criteria such as PSNR, normalised crosscorrelation, as well as normalised absolute error were used to evaluate the suggested algorithm's performance. The created method has been proven to be extremely successful in the management of video data security in cloud computing.

Sahil Garg and Naresh Kumar Garg [7], Steganography algorithms used to secure sensitive data on the Internet. It hides the hidden information in the cover image and provides imperceptibility to the attacker. The LSB is the most essential method in the steganography. In this method, the least significant bit of the picture of cover pixel replaced with data bits. In the literature, the data hiding achieved without considering the HVS characteristics that degrade the visual quality of the image. In this paper, the optimized data hiding has done. The colour picture contains three planes known as the red–green–blue plane. The green plane is the most sensitive, and blue is less sensitive to the human eyes. In the optimized method, the hidden information bits match with the cover image bits. If the bits match, then the corresponding optimal index determines, else data hiding done in the LSB bits of the cover pixel. After that, the optimal indexes hide in the cover image using a 2-bit LSB technique. In the proposed technique, image smooth and edge region characteristics explored before data hiding. There is a high correlation between the consecutive pixels in the smooth region and the minimum correlation on the edges. Thus, we have matched the secret data bits with the cover pixel bits in the smooth as well as hide the optimal indexes on the edges. The experimental results performed on the standard dataset images downloaded from the USC-SIPI image database.

Shah et al. [8], Covert communication is accomplished through the use of steganography. In picture steganography, the hide data is hidden in the cover image in such a manner that the cover image changes very little. Although there has been a lot of study into picture steganography, only a few studies have looked at the idea of picking a cover image for steganography that is more compatible with the hidden data. We provide a GA-based approach for picking a cover picture from a database of photographs in this work. The chosen cover picture is the best suitable with the secret info provided.

Pratik D. Shah and R.S. Bichkar [9], Many data security challenges have arisen as a result of the significant increase in data flow through the Internet. Steganography is a technique for concealing the existence of classified information. As a result, it is often utilised to address data security concerns. A safe and lossless spatial domain picture steganography approach is proposed in this study. By selecting acceptable sites to hide 2 bits of hide information, a stream of secret data is hidden in a quarter of the picture, resulting in the creation of corresponding to the location of match. LSB replacement steganography is used to hide these coefficients in the rest of the picture. The suggested approach is exceedingly safe and practically hard to extract secret data from since a genetic algorithm is utilised to identify the best feasible spot to hide these coefficients in the image. The suggested technique's results are compared to LSB replacement steganography, which uses the same amount of secret data. When compared to LSB steganography, the suggested approach is shown to be far better. It improves MSE and PSNR values while also minimising histogram deterioration and so avoiding histogram attack.

Sahu et al. [10], The bit flipping approach is proposed in this article as a way to hide hidden information in the original picture. Here, a block is made up of two pixels, with one or two LSBs being flipped to secret hidden data. There are two versions of it. Both Variant-1 and Variant-2 hide the secret data in the 7th and 8th bits of a pixel. Variant-1 hides 3 bits per pixel pair, whereas Variant-2 hides 4 bits per pixel pair. When compared to existing bit flipping methods, our suggested approach significantly increases the capacity and the number of bits per pixel. The suggested approaches' picture steganographic properties were compared to the findings of an existing bit flipping method as well as various state-of-the-art articles.

3. PROPOSED METHOD

The proposed method hides the smart grid secret information in the picture of cover in the optimal way to reduce variability. The flowchart of the proposed method is represented in Figure 1. Initially, cover image is read as well as split into two halves. The first half of the cover image and confidential data is given to the matched algorithm. The matching algorithm matches the confidential data bits with LSB bits of the picture of cover. In the this algorithm, to match the bits, the confidential data bits are split into 2-bits chunks. After that, confidential data bits, original or its complemented form is matched with cover image pixels. Next, which form is matched according to that index is determined along with first half of the stego image.

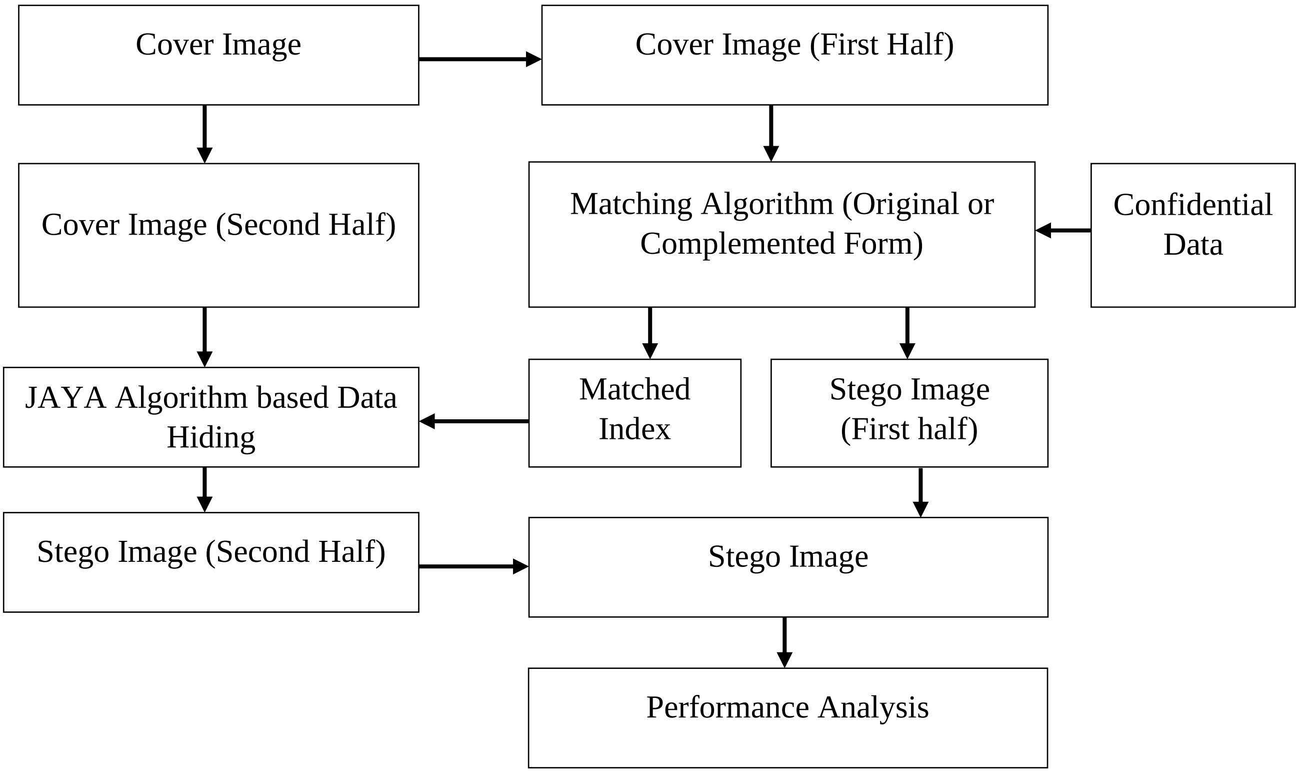

Cover Image
Cover Image (First Half)
Cover Image (Second Half)
Matching Algorithm (Original or Complemented Form)
Confidential Data
JAYA Algorithm based Data Hiding
Matched Index
Stego Image (First half)
Stego Image (Second Half)
Stego Image
Performance Analysis

Figure 1 Flowchart of the Proposed Method

The second half is used to secret the matched index in the picture of cover in the optimal way using the JAYA algorithm. Therefore, second half of the cover image and matched index is given to the JAYA algorithm. The JAYA algorithm searches the optimal starting pixel in the picture of cover to reduce the variability that generated due to index hiding. After determing the optimal starting pixels, the index hides in the picture of cover using 2-bit LSB bit method. In the last, the performance analysis of the proposed method is done using qualitative and quantitative analysis.

A detailed description of the JAYA algorithm is given below.

- Basic Concepts of JAYA Algorithm: Rao [11] proposed the JAYA algorithm, a population-based metaheuristic algorithm. This section introduces and evaluates the JAYA algorithm from several optimization angles. Initially, the JAYA algorithm inspiration is described. The JAYA algorithm's procedural steps are then presented.
- Inspiration of JAYA Algorithm: The JAYA method was created to solve optimization functions that were both limited and unconstrained. The title JAYA comes from Sanskrit and signifies "victory." This algorithm is a population-based metaheuristic that combines evolutionary and Swarm-based intelligence properties. It is based on the "survival of the fittest" principle's natural behaviour. This means that in the JAYA population, solutions are drawn to the best global solutions while the worst ideas are ignored. To put it another way, the JAYA algorithm's search process strives to come closer to success by reaching the global best solutions, and tries to avoid failure by avoiding the worst options. The JAYA algorithm offers various advantages over other

population-based algorithms, including ease of implementation and independence from method-specific parameters (i.e., the population size, and maximum number of iterations)

- JAYA Algorithm Steps: In this section, the basic flowchart and algorithm are shown in Figure 2 and Table 1 [12].

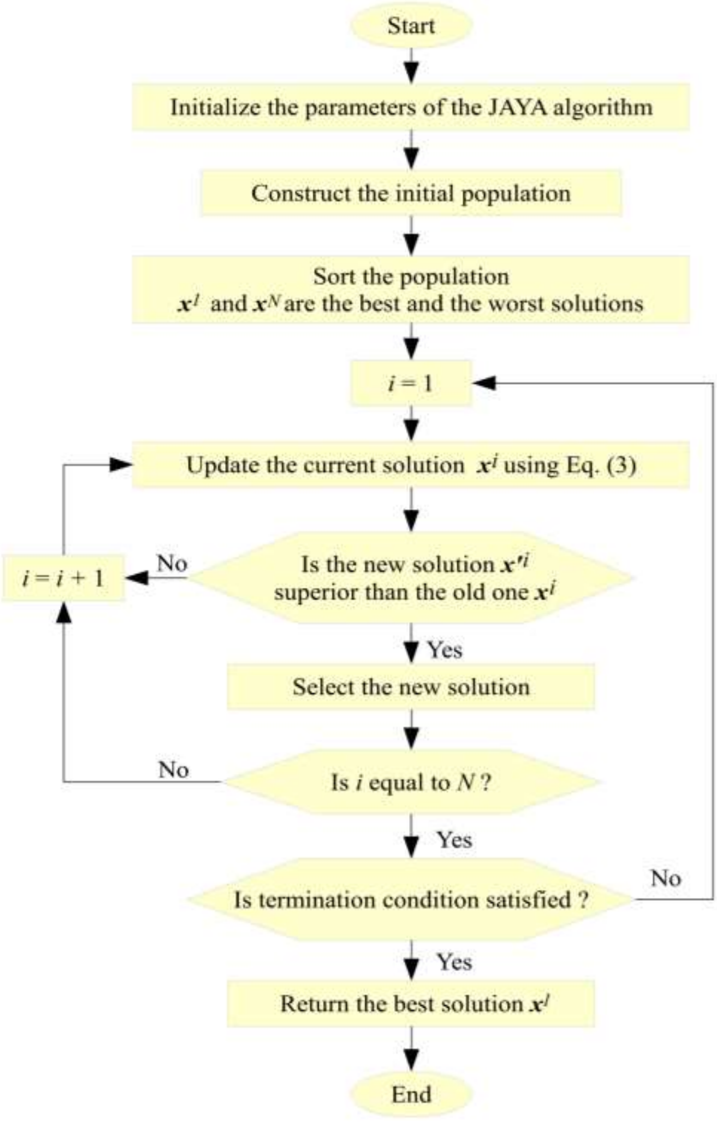
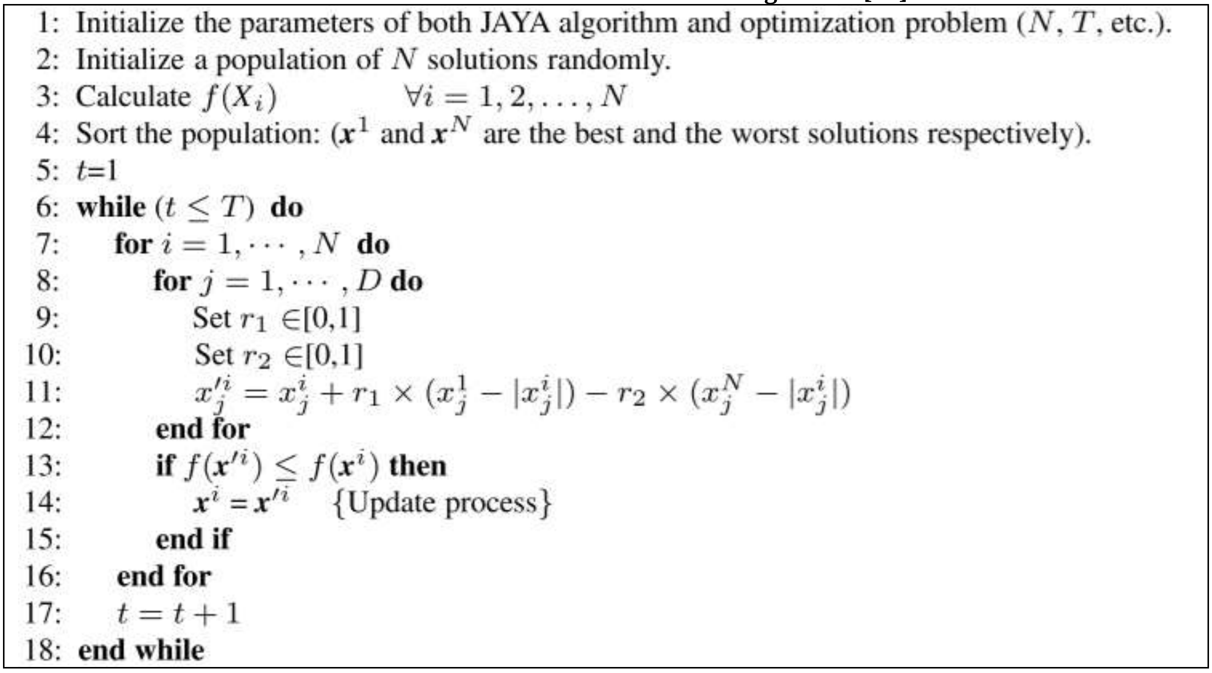

Start
Initialize the parameters of the JAYA algorithm
Construct the initial population
Sort the population
x^1 and x^N are the best and the worst solutions
$i = 1$
Update the current solution x^i using Eq. (3)
Is the new solution x'^i superior than the old one x^i
No
$i = i + 1$
Yes
Select the new solution
Is i equal to N ?
No
Yes
Is termination condition satisfied ?
No
Yes
Return the best solution x^1
End

Figure 2 Flowchart of JAYA Algorithm [12]

Table 1 Pseudocode of JAYA Algorithm [12]



```
Initialize the parameters of both JAYA algorithm and optimization problem ($N$, $T$, etc.).
Initialize a population of $N$ solutions randomly.
Calculate $f(X_i)$        $\forall i = 1, 2, \ldots, N$
Sort the population: ($x^1$ and $x^N$ are the best and the worst solutions respectively).
$t$=1
while ($t \leq T$) do
    for $i = 1, \cdots, N$ do
        for $j = 1, \cdots, D$ do
            Set $r_1 \in$[0,1]
            Set $r_2 \in$[0,1]
            $x'^i_j = x^i_j + r_1 \times (x^1_j - |x^i_j|) - r_2 \times (x^N_j - |x^i_j|)$
        end for
        if $f(x'^i) \leq f(x^i)$ then
            $x^i = x'^i$     {Update process}
        end if
    end for
    $t = t + 1$
end while
```

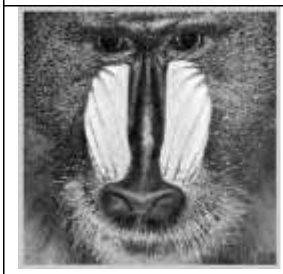
4. SIMULATION RESULTS

In this section, the simulation results of the proposed method is presented. The algorithm is simulated in MATLAB.

4.1 Qualitative Analysis

In this analysis, the pictures of cover, as well as stego, are compared based on the visual variability. Table 2 shows the qualitative analysis of the proposed method.

Table 2 Qualitative Analysis

Cover Image	Stego Image
 Lena	
 Baboon	
 Barbara	
 Pepper	
 Female	

4.2 Quantaitive Analysis

In this analysis, the most prominent paramters, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are calculated for the proposed method.

4.2.1 Mean Square Error (MSE): This parameter calculates the variability in the picture of cover as a result of data concealing [13]. It's worked out using Eq (1).

$$MSE = \frac{1}{AB}\sum_{i=1}^{A}\sum_{j=1}^{B}(C_{ij} - S_{ij})^2 \qquad (1)$$

where AB denotes the cover image's row as well as columns. The cover and stego pictures are denoted by the letters CS. Table 3 shows the outcomes of the suggested method. The result shows that the proposed method MSE is on average is 0.6179.

Table 3 MSE for the Proposed Method

Images	MSE
Lena	0.6226
Baboon	0.6196
Barbara	0.6202
Pepper	0.6153
Female	0.6120
Average	0.6179

4.2.2 Peak Signal to Noise Ratio (PSNR): PSNR parameter calculated the quality of picture of stego after information embedding [13]. PSNR is stated as eq (2)

$$\mathrm{PSNR}=10\log_{10}\frac{P^2}{MSE}\,(\mathrm{dB}) \qquad (2)$$

Here, P defined the maximum intensity and its value is 255. Table 4 represented the PSNR for the various picture of cover. The result shows that the proposed method MSE is on average is 50.2214dB.

Table 4 PSNR for the Proposed Method

Images	PSNR (in dB)
Lena	50.1886
Baboon	50.2099
Barbara	50.2052
Pepper	50.2403
Female	50.2629
Average	50.2214

4.3 Comparative Analysis

The presented method is compared with other methods which are based on the PSNR parameter in Table 4.4 with the same cover and secret data size. The outcomes show that the presented method is better than other methods.

Table 5 Comparative Analysis with the Existing Methods

Methods	Pratik D. Shah and R.S. Bichkar [9]	Kamil et al. [6]	Proposed Method
PSNR (in dB)	52.12	53.14	53.28

5. CONCLUSION AND FUTURE WORK

In the presented article, we have designed an optimized data hiding method to reduce variability. To achieve this goal, the original or complemented form of the confidential data is matched with LSB bits of the cover image as well as matched index is determined. After that, the matched index is hide in the cover image in the optimal way using the JAYA algorithm. The JAYA algorithm searches the optimal starting pixel for index hiding. Next, hide the index using k-bit LSB method from the optimal starting pixel. The result shows that the presented technique gives better PSNR than other methods. In the future, the proposed method is enhanced by deploying the data compression method. The deployment of data compression method before data hiding enhancing the embedding capacity.

6. REFERENCES

[1] Mohammadi, F. (2021). Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies*, *14*(5), 1380.

[2] Pour, M. M., Anzalchi, A., & Sarwat, A. (2017, March). A review on cyber security issues and mitigation methods in smart grid systems. In *SoutheastCon 2017* (pp. 1-4). IEEE.

[3] Abood, O. G., Elsadd, M. A., & Guirguis, S. K. (2017, December). Investigation of cryptography algorithms used for security and privacy protection in smart grid. In *2017 Nineteenth International Middle East Power Systems Conference (MEPCON)* (pp. 644-649). IEEE.

[4] Abuadbba, A., & Khalil, I. (2015). Wavelet based steganographic technique to protect household confidential information and seal the transmitted smart grid readings. *Information Systems*, *53*, 224-236.

[5] Kumar, A., & Raghava, N. S. (2019). Chaos-based steganography technique to secure information and integrity preservation of smart grid readings using wavelet. *International Journal of Computers and Applications*, 1-7.

[6] Kamil, S., Ayob, M., Abdullah, S. N. H. S., & Ahmad, Z. (2018, November). Optimized data hiding in complemented or non-complemented form in video steganography. In *2018 Cyber Resilience Conference (CRC)* (pp. 1-4). IEEE.

[7] Gupta, S., & Garg, N. K. (2021). Optimized Data Hiding for the Image Steganography Using HVS Characteristics. In *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020* (pp. 275-285). Springer Singapore.

[8] Shah, P. D., & Bichkar, R. S. (2020, June). Genetic Algorithm based Approach to Select Suitable Cover Image for Image Steganography. In *2020 International Conference for Emerging Technology (INCET)* (pp. 1-5). IEEE.

[9] 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.

[10] Sahu, A. K., Swain, G., & Babu, E. S. (2018). Digital image steganography using bit flipping. *Cybernetics and Information Technologies*, *18*(1), 69-80.

[11] Rao, R., 2016. Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. *International Journal of Industrial Engineering Computations*, *7*(1), pp.19-34.

[12] Zitar, R.A., Al-Betar, M.A., Awadallah, M.A., Doush, I.A. and Assaleh, K., 2021. An Intensive and Comprehensive Overview of JAYA Algorithm, its Versions and Applications. *Archives of Computational Methods in Engineering*, pp.1-30.

[13] Alia, A. S., Al-Tamimib, M. S. H., & Ahmed, A. (2020). Secure Image Steganography Through Multilevel Security. *Image*, *11*(1).