



## Enhance data hiding capacity and reduce variability using image steganography for smart grid

Muzamil Lateef Wagay

[muzamillateef23@gmail.com](mailto:muzamillateef23@gmail.com)

Adesh Institute of Engineering and Technology, Faridkot,  
Punjab

Puneet Jain

[puneetjain988@gmail.com](mailto:puneetjain988@gmail.com)

Adesh Institute of Engineering and Technology, Faridkot,  
Punjab

### ABSTRACT

*In the Smart Grid (SG) network, the sensitive data is communicated over the network and it prone to attacks. In order to overcome these attacks, security algorithms like cryptography and steganography are used. Steganography algorithms provide imperceptibility by hiding the secret data in the cover image whereas cryptography algorithms scramble the data using a private key and scramble data gives attention to the attacker. In steganography, the Least Significant Bit (LSB) is the most preferred data hiding algorithm. In the LSB algorithm, the data is split into 1-bit chunks and hide in the cover image LSB bit. The LSB algorithm provides less variability with less embedding capacity. In this paper, we have designed an algorithm that provides better embedding capacity and lesser variability. Initially, the cover pixel read is read and its intermediate bits 5th and 6th are taken as a reference to hiding k-bits of data using the LSB algorithm. The benefit of taking the intermediate bits of the cover pixel as a reference is that no need to communicate reference bits information with the receiver. After that, the LSB bit of the stego image generated after data hiding is circularly rotated in order to reduce the variability. The experimental results were performed on the standard dataset images and various performance metrics calculated for it. Lastly, the proposed algorithm is compared with the existing algorithms and found that the proposed algorithm achieves randomness and better embedding capacity.*

**Keywords:** Data Hiding, Least Significant Bit, Smart Grid, Steganography.

### 1. INTRODUCTION

A smart grid is an electricity framework that may constitute the functions of all customers interconnected to smart grid-producers and users. Both of them do work proficiently deliver, cost, and protect electricity deliveries [1]. It recruits new and developed products and services with controlling, searching, informing, and self-remedy techniques to:

- Better smooth the interconnection and execute of producers of different sizes and techniques;
- Allow users to play a part in optimizing the operation of the system.
- Give users with greater information and choice of provision;
- Significantly decrease the surrounding effect of the provision of electricity system;
- Deliver increased levels of reliability and protection of provision.

#### 1.1 Attacks in the Smart Grid

In this section, we have explained the smart grid attacks which are presents in the literature [2].

- **Eavesdropping Attack:** Wireless signals are taken away in open place, and are open minded to eavesdropping through a conflicting. The confidential data may be noticed, and examined by a hack. Cheapest eavesdroppers present in the bazaar, to facility launch of these kinds of attacks. Information encryption is the best method towards securing confidential data from declaration to the conflicting, if a special kind of pattern is related through the transmitted information, an intelligent conflicting can be able to make out the message. For example, if a household is not occupied, the electricity application will attenuate. If the smart meter is performed to inform with the information concentrator when a special threshold of energy apply is crossed. If the length of data to be communicated is directly proportional to used energy, then a specimen of performance of the household may be made.
- **Data Injection and Replay Attacks:** the other type of malicious attacks is the data injection and replay attack. The wrong information injection attacks happen when wrong information is given into the surrounding noticed through the operator. These types of attacks make goals to the smart grid structure, mainly calculating and controlling the systems with the objective of handling meter and phasor calculates, to mislead the execution and monitor of the usage given.

- **Man-in-the-Middle Attack:** This kind of attack occurs when the conflicting in the network information and meter information from terminal units, frames component, and forwards the advanced kind to the monitor centre. In the modern power systems, there is absence of information warnings the adversary might received to advanced network and meter information such that they are relevant with the target.
- **Jamming Attack:** The objective is to stop the smart meters with the uses of given, by jamming of the wireless medium with noise signals. These types of attacks may be categorized into two different kinds: i) Proactive jamming, in which the jammer may produce noise signals to completely stop a wireless channel, and (ii) Reactive jamming, in which the jammer eavesdrops on the radio channel and embarked the attack when signals are realized on the channel. The outcomes of this attack, the laws smart meter may be influenced into two different kinds: (i) the channel will be marked busy for done through a law smart meter, (ii) the smart meter can be stopped from incoming information. It is non-trivial solution distinguished to the reactive jammer attacks that can be outcomes from routine communication signals.

### 1.2 Security Requirements in the Smart Grid

The National Institute of Standards and Technology (NIST) has stated three different types of basis needed to management the protection of data in the smart grid and held it secured, mainly secretly, integrity, and presence. The detailed of each basis is below [3].

- **Confidentiality:** Confidentiality protects official constrains on access as well as disclosure the data. The confidentiality criterion needs securing the privacy as well as possessive data from accessed or opened through non official entities, personals, or develops. Once an unofficial open of data happens, confidentiality is lost. For example, data like monitor of a meter, applicable of metering, and billing data that is sent between a user and different parties should be confidential as well as secured; otherwise, the user's data might be framed up, modified, or required for other various objectives.
- **Availability:** It is stated as make sure timely access and applies of data. It is assumed the necessity of protection criterion. Due to the loss of availability which means disruption of access to information in a smart grid. For example, loss of availability may unsettle the execution of the monitor system through blocking the data's flow via the network, hence disclaimed the data's availability to monitor the system.
- **Integrity:** It means securing opposite to improper correction as well as decimation of data. The loss of integrity is not authorized modification, or decimation of information in not detected method. For instance, power injection is an attack embarked through a conflicting that enhances the calculations and imparts them. Non-repudiation as well as reality of data is needed to managing the integrity. Non-repudiation states that personal entity as well as an organization is not able to execute an action and after that ignored it.

In order to achieve this security requirements, security algorithms are used. In the literature, cryptography and steganography algorithms are used. The cryptography algorithms scramble the secret data using a private key. On the other side, steganography hides the data in the cover image and gives imperceptibility to the attacker. In this paper, we have studied the steganography algorithms used for data hiding. In the literature, Least Significant Bit (LSB) is the most preferred data hiding algorithm in which cover image pixel, LSB bit is replaced with data bit. This algorithm provides lesser embedding capacity and variability [4]. In order to enhance the capacity, the k-bits LSB algorithm used but it increases the variability in the same proportion [5]. Further, in order to enhance the security, random bit position of the pixel data hiding is achieved whereas random bit position indexes need to communicate with the receiver [6]. In this paper, we have enhanced the embedding capacity and reduce the variability after data hiding. In order to achieve this goal, the cover image is read and its pixels manipulated for data hiding. The intermediate bit position of the pixel is taken as a reference to determine how many k-bits hide in that pixel. The whole process is repeated for other pixels for data hiding that gives the stego image in the output. Also, the benefit of this procedure is that the reference bit information no need to communicate with the receiver. After that, the LSB bit of stego image is read. The bits are randomly rotated and hide in the stego image and which rotation is gives minimum variability that rotation-based data hiding achieved. The experimental results show that the proposed algorithm provides lesser variability over the existing algorithms. The rest of the section as follows. Section 2 gives the overview of LSB and k-bits LSB algorithm. Section 3 illustrates the proposed algorithm. Section 4 shows the experimental results. Section 5 defines the conclusion and future scope.

## 2. RELATED WORK

In this section, we have studied the data hiding algorithms used for image steganography.

### 2.1 LSB Algorithm

In the LSB algorithm, the secret data bits are split into 1-bit chunks. After that, the cover image pixel read and its LSB bit is replaced with the data bit, as shown in Figure 1 [4].

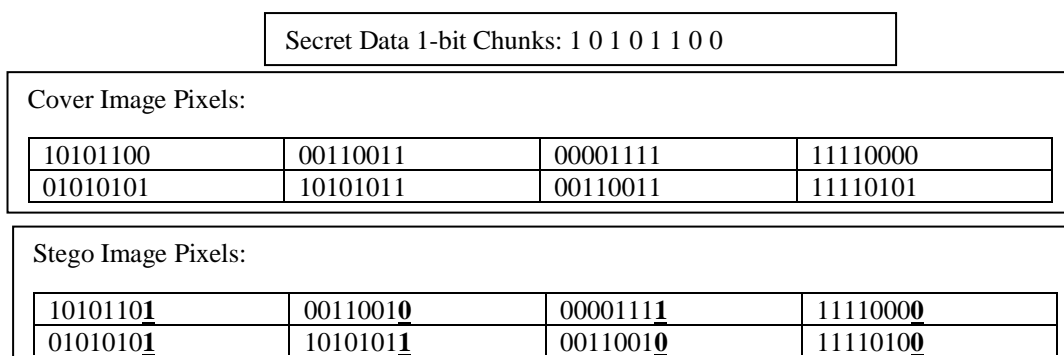


Fig. 1: LSB Algorithm

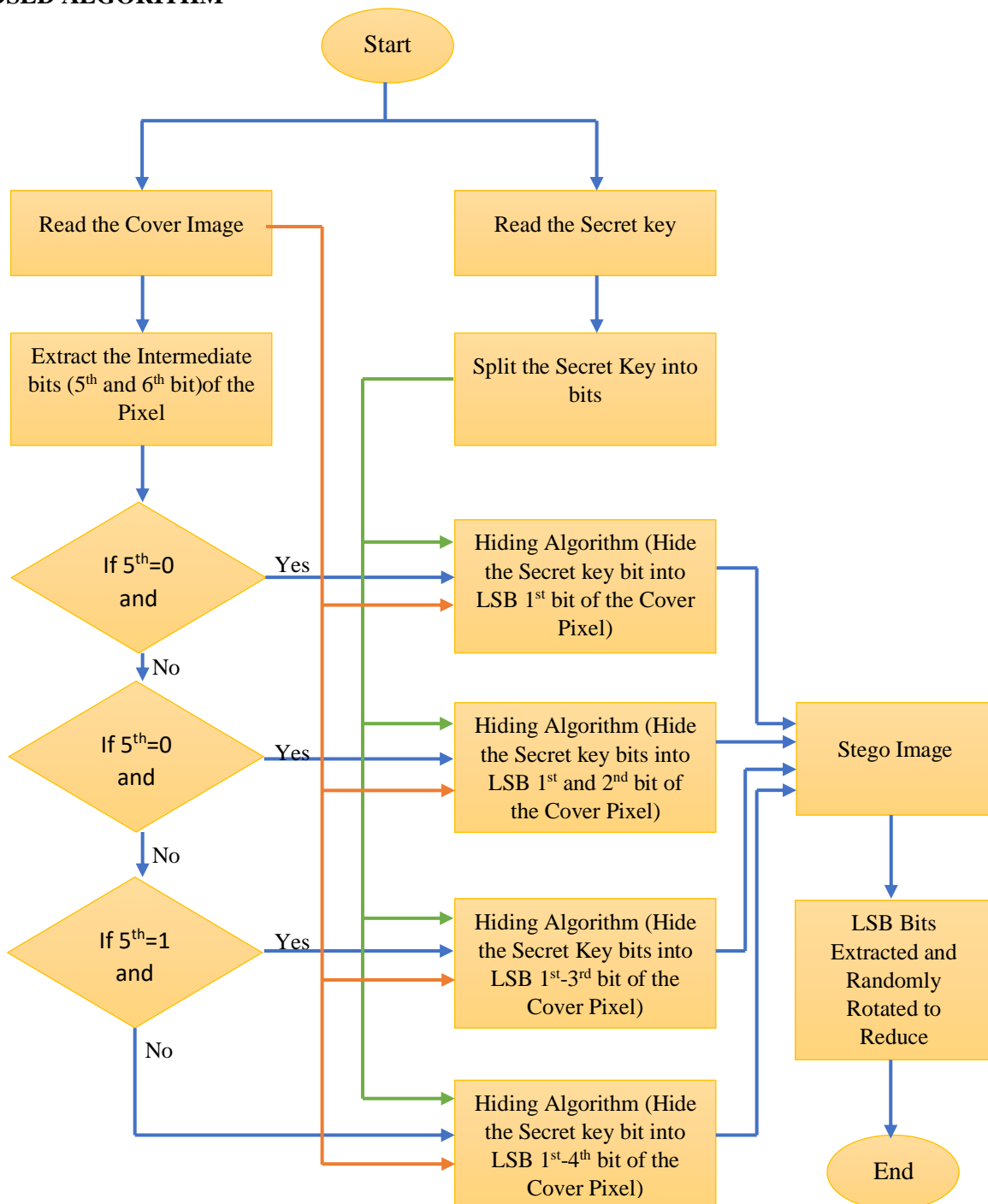
**2.2 K-bits LSB Algorithm**

In the K-bits LSB algorithm, the secret data is split into k-bits chunks. After that, the cover image pixel read and its LSB k-bits replaced with the data bits. Figure 2 shows the 2-bit LSB algorithm. The 2-bit LSB algorithm increases the secret data hiding capacity but also increases the variability [5].

Secret Data Chunks: 10 10 11 00 11 00 11 00			
Cover Image Pixels:			
10101100	00110011	00001111	11110000
01010101	10101011	00110011	11110101
Stego Image Pixels:			
101011 <b>10</b>	001100 <b>10</b>	000011 <b>11</b>	111100 <b>00</b>
010101 <b>11</b>	101010 <b>00</b>	001100 <b>11</b>	111101 <b>00</b>

**Fig. 2: 2-bit LSB Algorithm**

**3. PROPOSED ALGORITHM**



**Fig. 3: Flowchart of the Proposed Algorithm to Secure the Secret Data**

In this section, the proposed algorithm is designed to secure the secret data in the smart grid is explained. The flowchart of the proposed algorithm is shown in Figure 3. Initially, the cover image is read and its pixels intermediate bits (5<sup>th</sup> and 6<sup>th</sup>) are extracted and taken as a reference bit [5].

**Table 1: Bit Position for Key Bits Hiding**

6 <sup>th</sup>	5 <sup>th</sup>	Bit Position
0	0	1 <sup>st</sup>
0	1	1 <sup>st</sup> and 2 <sup>nd</sup>
1	0	1 <sup>st</sup> , 2 <sup>nd</sup> , 3 <sup>rd</sup>
1	1	1 <sup>st</sup> , 2 <sup>nd</sup> , 3 <sup>rd</sup> , 4 <sup>th</sup>

There is total four combinations possible of reference bits (00,01,10,11). According to the combination, 1-bit to 4-bit LSB data hiding is done and stego image generated in the output, as shown in Table 1. After that, in order to reduce variability, the LSB bit of the stego image is extracted and it is rotated and data hiding is done in the same position. The whole process is repeated 20 times and which rotation gives the minimum variability that combination used for data hiding. The benefit of the proposed algorithm is given below.

- The different combinations generated of reference bits for different cover images. Thus, data hiding in the two images are different.
- The rotation is random. Therefore, difficult to extract the original data without proper information of the rotation parameter.





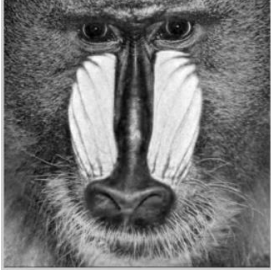
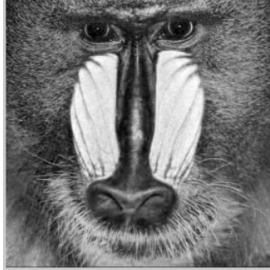


#### 4. EXPERIMENTAL RESULTS

In this section, the experimental results for the proposed algorithm are shown. The secret data is randomly generated. The algorithm is written and simulated in MATLAB 2013a. We have measured the various performance parameters for the proposed algorithm, as explained below.

##### 4.1 Visual Analysis

In the visual analysis, the cover image (original image) and stego image (generated after hiding the data bits) are compared and analysed how much the stego image is degraded after hiding the data bits. The results are shown in Table 2. The results show that both images look similar.

**Table 2: Visual Analysis between Cover and Stego Image**

Image Description (.jpg)	Cover Image	Stego Image
Lena		
Barbara		
Baboon		
Pepper		



**4.2 Mean Square Error (MSE)**

This parameter measures the variability generated in the cover image due to data hiding [7]. It is calculated using Eq. (1).

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

where AB denotes the row and columns of the cover image. CS denotes the cover and stego images. The results for the proposed algorithm are shown in Table 3. The results show that Lena image achieves lowest MSE and pepper image highest.

**Table 3: MSE for Different Cover Images**

Image	MSE
Lena	1.1972
Barbara	1.3535
Baboon	1.5016
Pepper	1.5568
Female	1.4779

**4.3 Peak Signal to Noise Ratio**

PSNR parameter measured the quality of stego image after data embedding [7]. It is calculated as (2)

$$PSNR = 10 \log_{10} \frac{P^2}{MSE} \text{ (dB)} \tag{2}$$

Here, P defined the maximum intensity and its value is 255 and MSE denotes the Mean Square Error. Table 4 shows the PSNR for different cover images. The results show that the Lena image achieves highest PSNR and Pepper image lowest PSNR.

**Table 4: Peak Signal to Noise Ratio for Different Cover Images**

Image	PSNR (in dB)
Lena	47.3491
Barbara	46.8161
Baboon	46.3653
Pepper	46.2085
Female	46.4344

**4.4 Embedding Capacity**

This parameter shows how many bits hide in the cover image [8]. The embedding capacity for the proposed algorithm is shown in Table 5. The results show that the pepper image achieves highest embedding capacity and Lena image least.

**Table 5: Embedding Capacity for Different Cover Images**

Image	Embedding Capacity (in bits)
Lena	91470
Barbara	103412
Baboon	103431
Pepper	112979
Female	111860

**4.5 Comparative Analysis with the Existing Algorithms**

**Table 6: Comparative Analysis with the Existing Algorithms based on PSNR**

Image	Shah et al. [6]		Data Hiding using Conventional K-bit LSB Algorithm		Proposed Algorithm (After Conventional K-bit LSB Algorithm and Circular Rotation)	
	PSNR (in dB)	EC (in Bits)	PSNR (in dB)	EC (in Bits)	PSNR (in dB)	EC (in Bits)
Lena	52.33	4096	46.5556	91470	47.3491	91470
Barbara	53.80	4096	45.9411	103412	46.8161	103412
Baboon	54.43	4096	45.5820	103431	46.3653	103431

Pepper	-	-	45.5011	112979	46.2085	112979
Female	-	-	45.7187	111860	46.4344	111860

In this section, we have compared the proposed algorithm with the existing algorithm in terms of PSNR and embedding capacity. There is an inverse relationship between PSNR and embedding capacity. The result shows that the Shah et al. [ref] achieves better PSNR with least embedding capacity. Further, the proposed algorithm result shows that the proposed algorithm achieves better embedding capacity as compared to the Shah, et al. [ref] and better PSNR as compared to the existing conventional k-bit LSB algorithm.

## 5. CONCLUSION AND FUTURE SCOPE

In this paper, initially, we have explained the overview of smart grid, attacks, and countermeasure algorithms. After that, steganography algorithm studied due to provide imperceptibility over cryptography algorithm. After, that, an algorithm is designed which provides better embedding capacity and PSNR. In the proposed algorithm, the intermediate bits of the cover image pixel are taken as reference and based on that data hiding is done using k-bit LSB algorithm. After that, the LSB bits of the stego image extracted and circular rotated in order to reduce the variability. The result shows that the proposed algorithm provides better results as compared to the existing algorithms.

## 6. REFERENCES

- [1] Vijayapriya, Tamilmaran, and DwarkadasPralhadas Kothari. "Smart grid: an overview." *Smart Grid and Renewable Energy* 2, no. 4 (2011): 305-311.
- [2] Baig, Z. A., & Amoudi, A. R. (2013). An analysis of smart grid attacks and countermeasures. *Journal of Communications*, 8(8), 473-479.
- [3] El Mrabet, Zakaria, Naima Kaabouch, Hassan El Ghazi, and Hamid El Ghazi. "Cyber-security in smart grid: Survey and challenges." *Computers & Electrical Engineering* 67 (2018): 469-482.
- [4] Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern recognition*, 37(3), 469-474.
- [5] Mstafa, R. J., & Elleithy, K. M. (2016). A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. *Multimedia Tools and Applications*, 75(17), 10311-10333.
- [6] 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.
- [7] 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.
- [8] Horng, J. H., Lin, J., Liu, Y., & Chang, C. C. (2020). 3D Multilayered Turtle Shell Models for Image Steganography. *Computer Modeling in Engineering & Sciences*, 125(2), 879-906.