IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Smart Grid Database Security Using Steganography Algorithm

[1*]Mandeep kaur Sidhu, [2]Anantdeep Kaur

[1]Department of Computer Engineering, Punjabi university, Patiala, India
[2]Department of Computer Engineering, Punjabi university, Patiala, India

Available online at: www.ijcseonline.org

Accepted: 24/Jul/2018, Published: 31/Jul/2018

Abstract **-** Smart Grids are the efficient network for manage and distribute the electricity in the power grids. The smart grid is provided the two-way communication between customers and distributors. In this paper, double layer security technique is designed using steganography spatial domain and cryptography AES algorithm for smart grid database security. In the proposed technique, one time padding initialization vector (IV) is generated based on the edges information of cover image, which resolved the replay attack. The encryption of secret data is done using AES_IV algorithm. Further, the data embedding is done in smooth reason of the image using 2-bit LSB technique. At the receiver end, based on the edges information IV is determined and data extraction is done. The avalanche effect, Peak-signal-to-noise ratio, embedding capacity parameters are measured for performance analysis. The experimental results show that for different images, different IV is generated and quality of output image not degraded.

Keywords-Steganography, Cryptography, Smart Grid, Avalanche Effect, Initialization Vector, One Time Padding.

I. INTRODUCTION

The smart grid is the advanced distributed and control system that automatically monitor, control, and protect the power grids. The smart grid is hybridization the power grid with information and communication system to achieve high efficiency and safety [1]. The model for the smart grid is shown in Fig. 1.

The Fig. 1 shows that the smart grid is provide two-way interaction between all units. In the smart grid, number of distributor and customers are involved and their data security and authentication is a requirement in smart grids for the effective communication [2] and impersonation-based on the smart grid network [3]. These are briefly explained below.

- **Key-based attacks**

In the smart gird, for authentication purposes secret key or certificate is used. There are two scenario, in the first scenario the attacker have the knowledge of the secret key. The cipher structure is determine by analyzing the secret key.

On the other hand, in second scenario, the attacker share the unknown key with the other adversary and based on the analysis of operation determine the key.

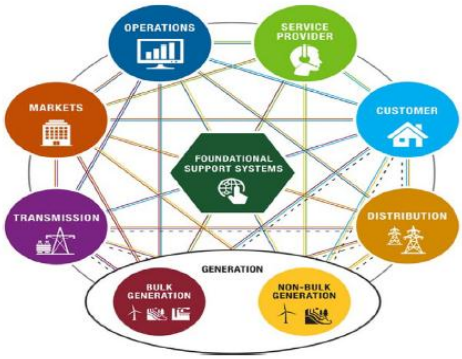

Fig.1 NIST Recommended Model for Smart Grid

- **Data-based attacks**

In the data-based attack, the attacker modify the electricity data and violate the integrity, confidentiality, repudiation.

- **Impersonation-based attacks**

In the attack, the attacker modify the data read by smart grid through the smart meters. There are number of attacks classify in this attacks. These are man-in-the-middle attack, replay attack, and eavesdropping attack.

The cryptography and steganography are the areas used for overcome these attacks. The cryptography encrypted the data and steganography hides the existence of data. The cryptography based on the key it is classified into symmetric

© 2018, IJCSE All Rights Reserved

and asymmetric ciphers. In the symmetric cipher, same key is employed for encryption-decryption. On the other side, different key used for encryption-decryption in the asymmetric ciphers [2]. The steganography is classified into spatial and frequency domain. In the spatial domain, pixels manipulated for data hiding and on the other side, frequency coefficient of pixels are determined and data hiding is done.

In this paper, we presented double layer security technique for resolving data based attack, replay and eavesdropping attacks for smart grid application. The data is encrypted using AES algorithm. In addition, one time padding is done in the encryption algorithm, which improve security and replay attack. The performance analysis parameters, which includes avalanche effect, PSNR, embedding capacity, are measured and compare with the existing work. The experimental results show that the double layer security technique is provide good security and visual quality.

The paper is as follows. The section II defined the related work has done in the field of smart gird for database security. The proposed technique is explained in section III. Section IV illustrated the results for the proposed technique and comparative analysis with existing technique. In the section V concluded the work.

II. RELATED WORK

In this section, a review on smart grid security algorithms are done.

Sunita, *et al.* [4], the cryptography and steganography algorithms hybridization improve security and provide efficient communication. Further, different
text steganography techniques are compared. They found that CASE approach is robust as compared to retyping and reformatting approach.

Jiang, *et al.* [5], designed real time covert VoIP communication using AES and audio steganography technique. The performance analysis is done on the basis of PESQ (which includes mean, variance) and compared the time domain and frequency domain samples. Their results is resistant to statistical attacks.

Abood, *et al.* [6], is done the comparative analysis between different cryptography algorithms such as AES, DES, TDES, RSA, and Blowfish based on effectiveness, key size, complexity. From the comparative study, they found that AES is better in terms of security for smart grids.

Abuadbba, *et al.* [7], hybridized the steganography algorithm with error detection and correction technique for cognitive smart grid security and robustness against the different attacks. In their proposed model, wavelet transform is used for data embedding and BCH algorithm is used for error detection and correction. In addition, number of random noise is applied on the proposed model to show robustness. To determine robustness BER, PRD, and RMS are measured for recover secret message.

Amir Hossein Ghane and Jalil Seifali Harsini [8], is proposed network based steganography approach for cognitive radio system. In their algorithm, the secret information is encoded using error correction codes such as BCH and Turbo channel encoding, DWT transform is taken for cover media, and data embedding is done.

Mouachi, *et al.* [9], in the smart grid cryptography algorithms are provided good security. Various cryptography symmetric and asymmetric algorithms are employed for data encryption and authentication purposes. In this paper, analyze various encryption algorithms and found that AES-128 is best encryption scheme for data security.

From the literature survey found that, cryptography and steganography, and error correction code fields are hybrid for security purposes in smart grids. The AES is the most suitable cryptography algorithm for data security. In this paper, AES and steganography spatial domain techniques are hybrid for

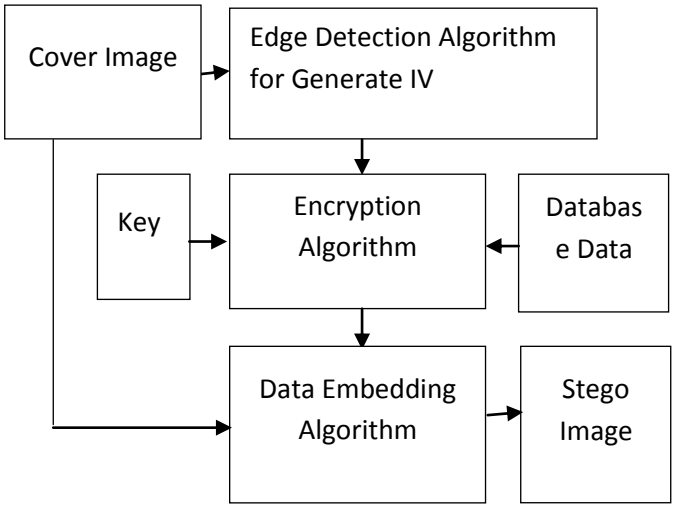

Fig. 2 Block Diagram for the Double Layer Security Technique (data security and capacity).

III. PROPOSED TECHNIQUE

In this section, the details of the proposed technique is explained. The block diagram is defined in the Fig. 2. The cover image is read and determine the edges of the cover image and random IV is generated for encryption algorithm. Next, read the secret data and data is encrypted using AES algorithm. The data is hidden in the cover image using 2-LSB technique [10]. In the last, the Avalanche effect, PSNR, and embedding capacity parameters are measured for performance analysis.

The proposed technique has three components and explained below.

© 2018, IJCSE All Rights Reserved

3.1 Edge Detection algorithm

In the proposed algorithm, the initialization vector is generated based on the information of edges of the cover image [11]. The advantage of determine IV on edges shows that for different images there are different IVs. In the proposed technique Sobel edge detection technique is used. The pseudocode for edge detection is explained in Table 1.

Table 1.Pseudocode for Edge Detection Algorithm

1. The Cover image is read and extract RGB planes.
2. The sobel edge detection algorithm is applied on red plane to determine edges.
3. The output of step 2 is binary image. Where, 0's represent the smooth pixel and 1's represents the edge pixel.
4. The edge pixels information is extracted and used for Initialization vector generation.

3.2 Encryption Algorithm:

In the proposed technique, AES encryption algorithm is used for data encryption. The AES encryption has 128-bit block size, 3 variant 128,192,256 bit key size. The algorithm is based on substitution and permutation network [12]. The AES_IV algorithm pseudocode is explained in Table 2.

Table 2. Pseudocode for AES_IV Algorithm

1. The 128 bit Plaintext, IV and key is read and xor operation is done.
2. The output of first step passed through 9 rounds and each round further contains four steps which includes s-box, shift row, mix-column, and add round key. In addition, in each round the key is updated.
3. In the last 10^{th} round, the round contains s-box, shift row and add round key operations is done and cipher is generated.
4. The Cipher is generated in the first block worked as IV for the next block.
5. The avalanche effect is measured for performance analysis.

3.3 Data Embedding algorithm

The proposed technique data embedding pseudocode is explained in Table 3. The data embedding is provided multi-layer security.

Table 3 . Pseudocode for Data Embedding

1. The cover image and encrypted secret message are read.
2. The secret message is divided into 2-bit chunks.
3. The cover image smooth region pixels least significant bits are replaced with secret data chunks to produce stego image.
4. The PSNR and Embedding Capacity is measured for the proposed technique.

In the next section, the proposed technique simulation and analysis is explained in detail.

IV. RESULTS

In this section, the proposed technique is simulated and compare with existing work. In the experimental setup, 5 standard dataset images are taken [13]. The visual analysis is done in the Table 4.

Table 4 Comparative Analysis between Cover and Stego Image based on Visual Analysis.

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

The following parameters are measured for the proposed technique.

- **Avalanche Effect**

  When a single bit changes in the plaintext, significantly change the cipher text bits known as avalanche effect [13]. In the Table 5 the avalanche effect the proposed technique is shown for one block. We have change 1 bit in the plaintext and approximate 47% bits are changed in the ciphertext.

© 2018, IJCSE All Rights Reserved

Table 5 Performance Analysis based on Avalanche Effect

Plaintext	Cipher Text	AES_IV
[84 111 125 134 86 123 141 139 95 123 141 142 114 127 144 152]	[33 192 55 165 254 90 42 5 4 159 147 203 43 126 62 11]	47%
[**83** 111 125 134 86 123 141 139 95 123 141 142 114 127 144 152]	[62 131 24 45 68 144 218 24 46 78 186 211 49 65 96 159]	

- **PSNR**

PSNR parameter measured the quality of stego image after data embedding [14]. It is calculated as (1)

$$\text{PSNR}=10\log_{10}\frac{A^2}{MSE}\ (\text{dB}) \quad (1)$$

Here, A defined the maximum intensity and MSE defined the square of different between cover and stego image and calculated as (2)

$$\text{MSE}=\frac{1}{KL}\sum_{i=1}^{K}\sum_{j=1}^{L}|M(i,j)-N(i,j)|^2 \quad (2)$$

Here, M and N represent the cover and stego image and KL resolution of the image.

- **Embedding Rate**

This parameter measured the number of bits is embedded in the cover image [14].

The performance analysis for the proposed technique is shown in Table 6. The Table shows that high PSNR and embedding capacity is achieved.

Table 6 Performance Analysis based on PSNR and Embedding Rate for the proposed technique.

Images (.jpg)	PSNR (dB)	Embedded Capacity
Lena	53.50	8020
Baboon	53.73	7896
Barbara	53.68	7534
Pepper	53.75	7748

For the comparative analysis the same dataset cover (Lena.jpg) and secret message is taken and applied on existing AES_LSB technique and proposed AES_IV_LSB technique and comparative shown in Table 7. The Table shows that proposed technique approximate same results as the existing AES. But, the proposed technique also provide authentication.

Table 7 Comparative Analysis with the existing technique

	Avalanche Effect	PSNR
AES_LSB	51%	53.44dB
AES_IV-LSB	47%	53.50db

V. CONCLUSION

In this paper, AES and steganography spatial domain technique is hybrid for data security. In addition, the Initialization Vector is generated based on the edges information of cover image to resolve replay attacks. The experimental results shows that the cover and stego image is looks similar and high avalanche effect, PSNR, is achieved. In last, comparative analysis is done with existing technique and found that approximate same results achieved with authentication provided by the proposed technique.

References

[1] Suleiman, H., Alqassem, I., Diabat, A., Arnautovic, E. and Svetinovic, D., 2015. Integrated smart grid systems security threat model. *Information Systems*, *53*, pp.147-160.

[2] Kumar, A. and Agarwal, A., 2016, November. Research issues related to cryptography algorithms and key generation for smart grid: A survey. In *Power Electronics (IICPE), 2016 7th India International Conference on* (pp. 1-5). IEEE.

[3] Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J. and Shu, L., 2018. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society*, *38*, pp.806-835.

[4] Chaudhary, S., Dave, M., Sanghi, A. and Manocha, J., 2016, March. An elucidation on steganography and cryptography. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (p. 43). ACM.

[5] Jiang, Y., Zhang, L., Tang, S. and Zhou, Z., 2013, August. Real-Time Covert VoIP Communications over Smart Grids by Using AES-Based Audio Steganography. In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing* (pp. 2102-2107). IEEE.

[6] Abood, O.G., Elsadd, M.A. and Guirguis, S.K.2017, December. Investigation of cryptography algorithms used for security and privacy

© 2018, IJCSE All Rights Reserved

protection in smart grid. In *Power Systems Conference (MEPCON), 2017 Nineteenth International Middle East* (pp. 644-649). IEEE.

[7] Abuadbba, A., Khalil, I., Ibaida, A. and Atiquzzaman, M., 2016. Resilient to shared spectrum noise scheme for protecting cognitive radio smart grid readings− BCH based steganographic approach. *Ad Hoc Networks*, *41*, pp.30-46.

[8] Ghane, A.H. and Harsini, J.S., 2018. A network steganographic approach to overlay cognitive radio systems utilizing systematic coding. *Physical Communication*, *27*, pp.63-73.

[9] Mouachi, R., Ait-Mlouk, A., Gharnati, F. and Raoufi, M., 2017. A Choice of Symmetric Cryptographic Algorithms based on Multi-Criteria Analysis Approach for Securing Smart Grid. *Indian Journal of Science and Technology*, *10*(39).

[10] Neeta, D., Snehal, K. and Jacobs, D., 2006, December. Implementation of LSB steganography and its evaluation for various bits. In *Digital Information Management, 2006 1st International Conference on* (pp. 173-178). IEEE.

[11] Vincent, O.R. and Folorunso, O., 2009, June. A descriptive algorithm for sobel image edge detection. In *Proceedings of Informing Science & IT Education Conference (InSITE)* (Vol. 40, pp. 97-107). California: Informing Science Institute.

[12] Heron, S., 2009. Advanced encryption standard (AES). *Network Security*, *2009*(12), pp.8-12.

[13] Bansod, G., Pisharoty, N. and Patil, A., 2016. PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing. *Defence Science Journal*, *66*(3).

[14] Chakraborty, S., Jalal, A.S. and Bhatnagar, C., 2017. LSB based non blind predictive edge adaptive image steganography. *Multimedia Tools and Applications*, *76*(6), pp.7973-7987.

© 2018, IJCSE All Rights Reserved