

Data Encryption and Key Wrapping for the Smart Grid Security

Manroop Kaur, Puneet Jain, Ravinder Kumar

Abstract— In the Smart Grid (SG), smart meters are used to communicate user information periodically to the grid. Thus, sensitive information of the user and their electricity consumption is communicated to the grid which is prone to number of attacks such as eavesdropping, modification attack. To overcome these attacks, various symmetric and asymmetric cryptography algorithms such as DES, AES, and Homomorphic encryption is used which provide better security but consumes larger resources. On the other hand, the symmetric algorithms are fast as compared to asymmetric for data encryption but required to communicate the key to the receiver. Therefore, key is also prone to key based attacks. Hence, while taking care of all issues, in this paper lightweight encryption is done using PICO algorithm as well as key wrapping algorithm is designed using histogram reversible technique. The performance analysis of the proposed technique is done based on the qualitative and quantitative parameters such as PSNR, Normalized Cross Correlation, avalanche effect, and Image Fidelity.

Index Terms— Smart Grid, PICO, Histogram Reversible Technique, PSNR.

I. INTRODUCTION

Smart Grid is advanced power grid which provides several features such as efficiency, reliability, and flexibility [1]. Also, the integration of renewable resources in the smart grid will make grid sustainable and eco-friendly. In the smart grid, advanced metering infrastructure plays an important role which includes smart meter, data concentrator gateway, trusted authority, and others. The AMI manages the real time electricity. To achieve this goal, the smart meter periodically measures the user consumption and communicates to the utility company through the gateway. The servers in the utility company measure the electricity consumption and based on that generate the dynamic pricing and billing. On the other side, sensitive communication is communicated between smart meter and utility company. Thus, prone to various attacks.

1.1 Smart Grid Attacks

Smart Grid is susceptible to the various attacks. The attacks are explained below in detail [2].

Eavesdropping Attack: In the eavesdropping, attacker intercepts the communication between smart meter and grid.

Traffic Analysis: In traffic analysis attack, attacker tries to analyze the message or its pattern of communication.

Replay Attack: In replay attack, attacker based on the old communication between authenticated parties attacks the authenticated user in the network.

Man-in-the-Middle Attack: In the man-in-the-middle attack, attacker tries to modify the message or delete the content of message before delivered to the receiver.

Denial-of-service Attack: In this attack, the attacker floods the resources or bandwidth of the target system. Therefore, authenticated users are not accessing the devices and resources on the network.

Malware attack: In this attack, attacker adds a malicious program such as worms, viruses, trojan horses in the device which perform malicious operations such as stealing, deleting, altering, and encrypting the sensitive information. We will resolve eavesdropping, traffic analysis, and key based attack in this paper.

1.2 Security Field for the Smart Grid

To overcome these attacks, various cryptography and steganography algorithms are used in the smart grid [3,4]. In the cryptography algorithm, the secret message is encrypted such a way only authenticated user which has private key can decrypt the secret data. The private key is needed to communicate on the network. Therefore, prone to key based attack. Thus, to secure the key on the network steganography algorithm is used. Steganography algorithm hides the existence of the secret data and only authenticated users extract the private key for decryption.

In this paper, lightweight PICO cipher is used for data encryption which consumes less resources and histogram reversible shifting algorithm is used for key wrapping. The experimental analysis is done on the basis of various performance parameters such as avalanche effect, PSNR, Normalized Cross Correlation, and Image Fidelity. In the last, comparative analysis is done with the existing techniques.

The rest of the paper as follows. Section II defines the related work. Section III highlights the proposed technique. Section IV shows the experimental results and performance analysis. In section V draw the conclusion.

II. RELATED WORK

In this section, the Smart Grid attacks and its security solution techniques are defined.

Zhang, et al. [5], Smart Grid (SG) is a brand new architecture for the next generation's power grid system. Delivering control, monitoring and management data to grid elements firmly in the network is a basic requirement for SG. This paper proposes 256-bit Advanced Encryption Standard (AES) as a safety answer for SG system terminals. A couple of prototyping nodes is also implemented via Altera's DE2 boards' Nios II architecture. The two-node scheme works

Manroop Kaur, Dept. of Electrical Engineering Adesh Institute of Engineering and Technology, Faridkot (MRSPTU) Faridkot, India

Puneet Jain, dept of Electrical Engineering, AIET (PTU) Adesh Institute Of Engg. And Tech. (PTU, Jalandhar)

Ravinder Kumar, dept of Electrical Engineering, AIET (PTU) Adesh Institute Of Engg. And Tech. (PTU, Jalandhar)

correctly with AES encryption/decryption function. It suggests a probable solution for SG security.

Amjad Iqbal, Tariq Iqbal [6], Modern trend, towards renewable energy sources has complex our power systems' network with the dispersed generation and its organization. The main confront of this system is to put into practice a little cost, safe and genuine communication system between Supervisory Control and Data Acquisition (SCADA) unit and Remote End Devices (RED). This paper addresses the issues of safety and genuineness for wireless communication for SCADA system. Algorithm of Advanced Encryption Standard (AES) has been implemented on ESP32 with LoRa unit to safe the wireless communication for micro-grids and validity has been achieved by generating sole Message Authentication Code (MAC). A point to point communication group has been built-up with diversity above 10km and cost less than \$40 with power expenditure of 5mW.

Abood, et al. [7], in this paper, a comparison of various cryptography algorithms such as AES, DES, 3DES, RSA and Bllowfish is done. The comparison is set between to find the effectiveness, key size, complexity and time required between those algorithms. The performance evaluation of these algorithms is evaluated using MATLAB.

Fouda, et al. [8], Smart grid (SG) communication has just received important attentions to make easy intelligent and dispersed electric power transmission systems. However, communication faith and safety issues still there sensible concerns to the use of SG. In this paper, to deal with these difficult concerns, we recommend a lightweight message validation format features as a decisive yet crucial component for safe SG communication skeleton. Particularly, in the planned scheme, the smart meters which are dispersed at different hierarchical networks of the SG can first attain joint authentication and set up the joint session key with Diffie-Hellman exchange protocol. Then, with the joint session key between smart meters and hash-based authentication code technique, the following messages can be authenticated in a lightweight way. Complete safety analysis shows that the planned scheme can gratify the enviable security desires of SG communications. In addition, widespread simulations have also been conducted to show the effectiveness of the planned scheme in terms of low latency and a small number of signal message exchanges

Lv, et al. [9], Cyber security is believed as a major issue which must be checked early during the transfer from the current aging electric power grid into the supposed Smart Grid. Key management is the basic following cryptographic technologies for Smart Grid cyber security. This paper basis on remote key invention and division for Smart Grid, specially computation-saving mechanisms for meters. Specifically, we concentrate asymmetric key-wrapping to the Smart Grid application scenario, and further advocate an instantiation of remotely generating and distributing keys for Smart Grid, which is an issue raised by National Institute of Standards and Technology. In this way, we attain a key-wrapping adapter, retrofitting an encryption system to work with an mismatched key-management building and seamlessly following different options of cryptosystems for smart meters. The planned scheme has low calculus cost at fragile smart meters, because of the weaker safety statement of the wrapping algorithm and the transport of computational cost from meters to servers.

Rao, et al. [10], Authenticated Encryption (AE) is a symmetric key cryptographic system that aims to give both confidentially and data integrity. This project presents a narrative approach a (key sharing) for secret message communication amid a group (g) using wrapping technique. In order to boost security to share out secret message (key) and a produce a key to share out we initiate a wrapping technique in sponge (where as even absorbing and squeezing function are also used). In this project functioning of secret key sharing is to be done in a group of server-client technology using sponge function. In this process a sponge tool batch file installed in the server. The server will share out or converse the secret message to client based on one to one or one too many mapping. With the assist of the sponge tool a message has been encrypted and distributed amongst respective clients .In the client side the decryption batch file to be installed to be confirmation of secret message authentication. We determine the time complexity and space complexity for message cryptosystem and produce one time password for key communication which gives more safety and can stop hackers form hacking the data.

The literature survey shows that in the literature various conventional encryption [5-7] as well as key wrapping algorithm [9-10] is used which consumes huge resources and complex in nature. Therefore, in this paper, lightweight encryption and key wrapping algorithm is proposed. The proposed consume less resources as compared to conventional encryption technique, and key wrapping technique use logical operators to wrap the key.

III. PROPOSED TECHNIQUE

In the proposed technique, the sensitive data is encrypted using lightweight cryptography algorithm PICO which consumes less resources as compared to the existing cryptography algorithms. Next, the key is wrapped using histogram reversible data hiding algorithm which generate the key as well as original cover image in the receiver side. The block diagram of the proposed technique is shown in Fig. 2.

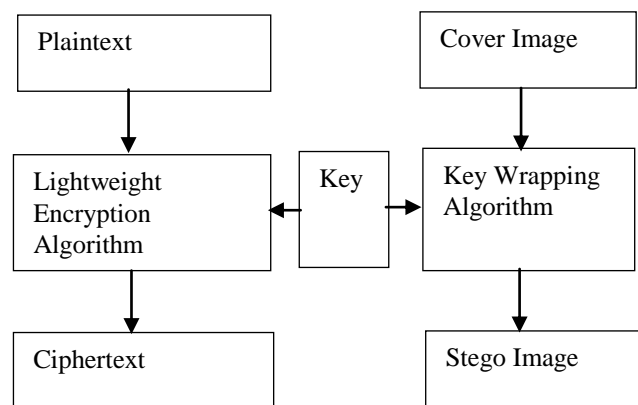


Fig. 2 Block Diagram of the Proposed Technique

Initially, the secret data, key is read and given to PICO algorithm which generate the ciphertext. On the other side, the cover image is read and key is hide in the cover image using histogram reversible algorithm which generate the stego image in the transmitter side. The ciphertext and stego image is communicated from the transmitter. In the receiver side, extraction algorithm is applied on the stego image and original key is recovered. Next, the key and ciphertext is

given to the decryption module which generate the original data.

The detail description of PICO algorithm and Histogram Reversible technique is given below.

3.1 PICO Algorithm [11]

PICO is a lightweight algorithm which is based on substitution permutation network as shown in Fig. 3. In the PICO cipher, the plaintext and key XOR operation is performed and given to s-box. The s-box is an bijective mapping look up table which transform the input to output bit form as shown in Fig. 4. Next, the permutation layer which is basically bit shuffle layer, shuffle the bits as shown in Fig. 5. Also, in each round key is updated using key scheduling and new key generation for the next round as shown Table 1

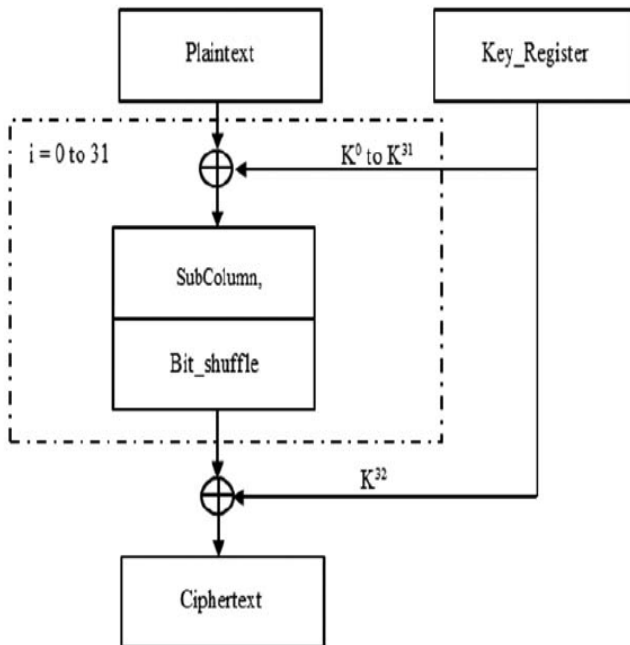


Fig. 3 Block Diagram of PICO Algorithm

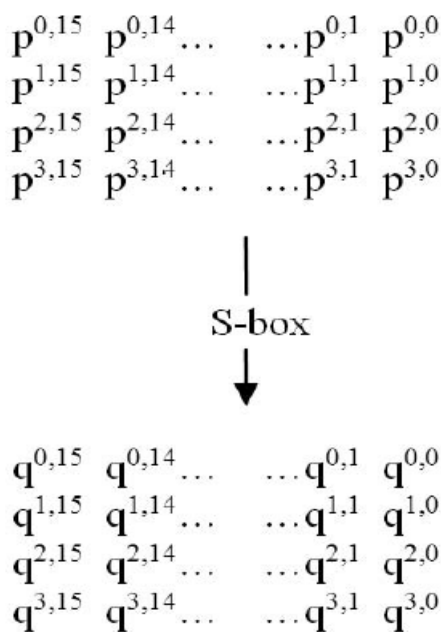


Fig. 4 S-Box

| | | | | | | | | | | | | | | | | |
|-------|------|-----|------|------|------|------|------|------|------|------|------|------|------|-----|-----|------|
| j \ i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 0.10 | 1.5 | 1.12 | 2.6 | 2.12 | 3.0 | 3.11 | 0.1 | 3.3 | 0.15 | 2.9 | 0.2 | 3.12 | 2.2 | 1.8 | 1.4 |
| 1 | 3.8 | 0.6 | 1.1 | 1.15 | 2.4 | 3.5 | 0.12 | 2.14 | 1.14 | 3.4 | 0.11 | 0.4 | 1.7 | 2.3 | 2.8 | 3.15 |
| 2 | 0.8 | 2.7 | 0.3 | 2.11 | 3.9 | 3.1 | 1.0 | 1.9 | 2.5 | 2.10 | 3.13 | 3.2 | 0.0 | 0.9 | 1.2 | 1.10 |
| 3 | 3.10 | 3.7 | 0.7 | 1.3 | 1.13 | 0.14 | 2.15 | 2.0 | 2.1 | 0.5 | 3.14 | 2.13 | 0.13 | 3.6 | 1.6 | 1.11 |

Fig. 5 Permutation Layer of PICO Cipher

Table 1 Key Scheduling

| |
|---|
| $K^0 = K^{63}, K^{62}, \dots, \dots, \dots, \dots, K^0$ $L^1 = K^{127}, K^{126}, \dots, \dots, \dots, \dots, K^{64}$ For $j=0$ to 31 rounds $L^2 = (K^j \text{ XOR } (RCSL^1, 3)) \text{ XOR } L^1$ $K^{j+1} = (L^2 \text{ XOR } (LCSK^j, 7)) \text{ XOR } J$ $L^1 = L^2$ Where RCS is Right Circular Shift and LCS is Left Circular Shift. |
|---|

Fig. 6 Key Scheduling

3.2 Key Wrapping using Histogram Reversible Technique

The histogram reversible shifting algorithm provide authentication [12]. In which, cover grey image is read and histogram bins are drawn. In the grey scale images, each pixel is represented in the 8-bit. Thus, the grey level is varied from 0 to 255. The level “0” and “255” represents the black color and white color. The grey values range between 0 to 255, and this range represents the different shades of grey color from low contrast to high contrast. Next, the peak value and zero value bin the histogram is determined. The bins between peak and zero value bin is shifted by 1-bit which makes the adjacent bin of the peak is zero. Further, the key bits are embedded in the peak bin value. After data embedding, there is the maximum 1-bit probability of change in the pixel value. Thus, the embedding capacity in the histogram reversible data embedding technique depends on the peak value in the image. Conversely, in the receiver side, the secret data was extracted from the peak value and its adjacent histogram value. After which, the histogram was adjusted to recover the original image.


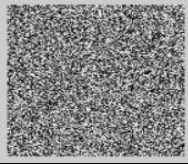

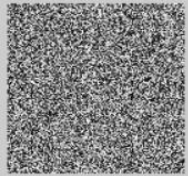

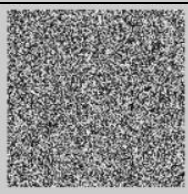

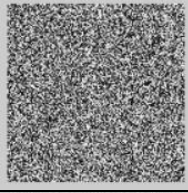

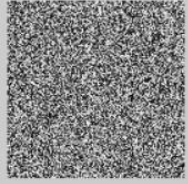

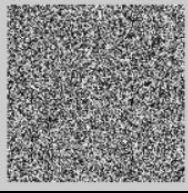

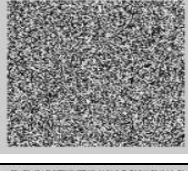

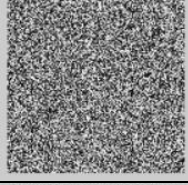
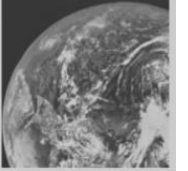
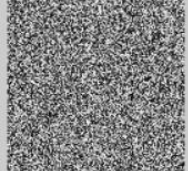

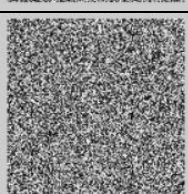
IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

In this section, proposed technique is tested in the MATLAB 2013a. In our work, 10 standard dataset grey images are taken to check the effectiveness of the proposed technique [13]. The resolution of the images is 128x128 and format .jpg. The simulation results for divided into two types

4.1 Simulation Results and Performance Analysis of Encrypted Image

In this section, qualitative means visual comparison between original and encrypted image is done as shown in Table 2. The results show that encrypted image is completely changed after encryption.

Table 2 Qualitative Analysis of Original and Encrypted Image

| Image Name | Original Image | Encrypted Image |
|------------|---|---|
| Lena |  |  |
| Brabara |  |  |
| Baboon |  |  |
| Pepper |  |  |
| Female |  |  |
| Couple |  |  |
| Aeroplane |  |  |
| Lake |  |  |
| Earth |  |  |
| Tree |  |  |

4.2 Performance Analysis of PICO and Key Wrapping Algorithm

The performance analysis of the proposed technique is done on the basis of various parameters. These parameters are

- Peak Signal to Noise Ratio

This parameter is used to measure the distortion in the encrypted image. In the ideal case, low value of PSNR gives better for the encrypted image and calculated using Equation (1-2) and measured in decibel [14].

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{MSE} \quad (1)$$

Here,

$$MSE = \frac{1}{J \times K} \sum_{m=1}^J \sum_{n=1}^K (X_{m,n} - Y_{m,n})^2 \quad (2)$$

Here, J, and K defines as the row and column of the

Table 3 PSNR value for the Encrypted Images

| Image | PSNR (in dB) |
|-----------|--------------|
| Lena | 12.35 |
| Brabara | 13.71 |
| Baboon | 12.56 |
| Pepper | 12.77 |
| Female | 19.52 |
| Couple | 24.33 |
| Aeroplane | 8.57 |
| Lake | 11.27 |
| Earth | 13.48 |
| Tree | 10.92 |

image. The X and Y represent the original and encrypted frame. In the Table 3, PSNR for the encrypted image is shown.

- Normalized Cross-Correlation (NCC)

This parameter is used to measure the similarity between original and encrypted image. In the ideal case, 0 value is required in the cryptography which show that no similarity between original and encrypted image. The value of NCC is varies between -1 to 1. It is measured using equation (3). Table 4 shows that NCC between original and encrypted image is approximate 0.

$$NCC = \frac{\sum_{j=1}^M \sum_{k=1}^N C(j,k) \times S(j,k)}{\sum_{j=1}^M \sum_{k=1}^N C(j,k)^2} \quad (3)$$

Table 4 Normalized Cross Correlation for the Encrypted Images

| Image | Normalized Cross Correlation |
|-----------|------------------------------|
| Lena | -0.0018 |
| Brabara | 0.0069 |
| Baboon | 0.0030 |
| Pepper | -0.00009 |
| Female | 0.0050 |
| Couple | 0.0103 |
| Aeroplane | 0.0032 |
| Lake | -0.0113 |
| Earth | -0.0134 |
| Tree | 0.0026 |

- Avalanche Effect

When a single bit change in the input significantly change the output, bits is known avalanche effect. In the ideal case, 50% bits change in the cipher text required if one-bit change in the

input. If this property achieved then algorithm resist to number of attacks. The avalanche effect for the PICO cipher is shown in Table 5. The result show that PICO achieves high avalanche effect.

Table 5 Avalanche Effect

| | | |
|-----------|--|-------------------|
| Plaintext | [0000 0000 0000 0000] | Avalanche Effect% |
| Key | [00000000000000000000 000000000000] | |
| Cipher1 | fda7e7de58c913f4 | |
| Key | [08000000000000000000 000000000000] | |
| Cipher2 | 72f4081fae46ef5d | 62% |

• Comparative Analysis with the Existing Techniques





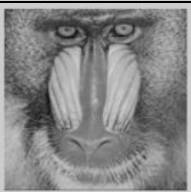
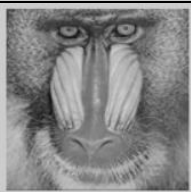


In this section, the PICO algorithm compared with the existing algorithms were studied in the literature in the Table 6. The result show that PICO consume less area and better avalanche effect as compared to AES.

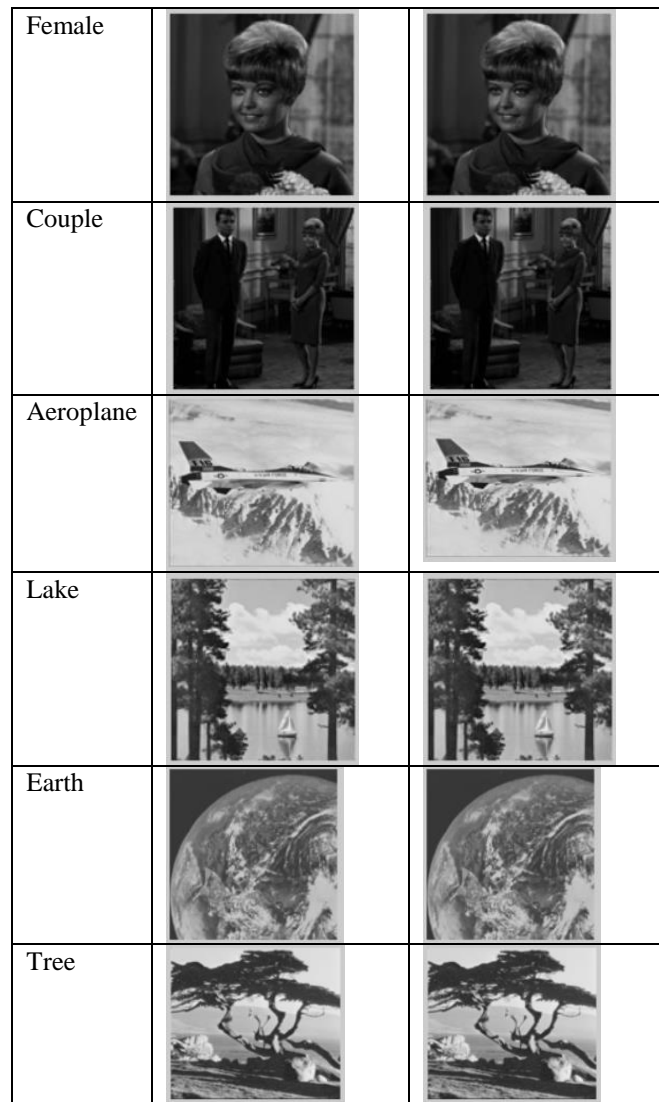
Table 6 Comparative Analysis with the Existing Technique

| Algorithm | Memory Usage for S-Box | Avalanche Effect |
|-----------|------------------------|------------------|
| AES | $2^8=256$ byte | 51% |
| PICO | $2^4=16$ Nibble | 62% |

Next, the performance analysis of key wrapping algorithm is done. The qualitative analysis between cover and stego image is done after hiding the key bit in the cover image as shown in Table 6.

Table 6 Qualitative Analysis between Cover and Stego Image

| Image Name | Cover Image | Stego Image |
|------------|---|---|
| Lena |  |  |
| Brabara |  |  |
| Baboon |  |  |
| Pepper |  |  |



The peak signal to noise ration between cover and stego image is calculated using Eq. (1-2) as defined earlier but in the steganography, high PSNR is required for cover and stego image. For the different images Key wrapping algorithm PSNR is shown in Table 7. The results show that proposed technique achieve better PSNR.

Table 7 PSNR for the Key Wrapping Algorithm

| Image | PSNR |
|-----------|-------|
| Lena | 51.91 |
| Brabara | 50.13 |
| Baboon | 45.65 |
| Pepper | 50.81 |
| Female | 53.24 |
| Couple | 59.76 |
| Aeroplane | 51.23 |
| Lake | 51.22 |
| Earth | 60.85 |
| Tree | 51.77 |

Next, the Normalized Cross Correlation between cover and stego image is calculated using Eq. (3). In the steganography, cover and stego image is approximate looks equal. Therefore, in the ideal case NCC 1 is required. The NCC for the different image is shown in Table 8. The results show that proposed technique achieve approximate 1 NCC.

Table 8 Normalized Cross Correlation for the Key Wrapping Algorithm

| Image | Normalized Cross Correlation |
|-----------|------------------------------|
| Lena | 0.9997 |
| Brabara | 0.9995 |
| Baboon | 0.998 |
| Pepper | 0.9997 |
| Female | 0.9996 |
| Couple | 0.9997 |
| Aeroplane | 0.9997 |
| Lake | 0.9999 |
| Earth | 0.9999 |
| Tree | 0.9998 |

• Image Fidelity

This parameter is measured the perceptual quality between using cover and stego image. It is calculated using Eq. (4).

$$\text{Image Fidelity} = 1 - \text{MSE} \quad (4)$$

Table 9 Image Fidelity for the Key Wrapping Algorithm

| Image | Image Fidelity |
|-----------|----------------|
| Lena | 0.58 |
| Brabara | 0.37 |
| Baboon | -0.76 |
| Pepper | 0.46 |
| Female | 0.69 |
| Couple | 0.89 |
| Aeroplane | 0.51 |
| Lake | 0.51 |
| Earth | 0.94 |
| Tree | 0.57 |

V. CONCLUSION

In this paper, lightweight encryption as well as key wrapping algorithm is proposed using PICO and Histogram Reversible algorithm. The experimental analysis is done on the standard dataset images and various visual and performance analysis parameter is measured such as PSNR, NCC, Image Fidelity, and Avalanche Effect. The result show that proposed technique achieves better results as compared to existing techniques.

REFERENCES

[1]Braeken, A., Kumar, P., & Martin, A. (2018). Efficient and privacy-preserving data aggregation and dynamic billing in smart grid metering networks. *Energies*, 11(8), 2085.

[2]Goel, S., & Hong, Y. (2015). Security challenges in smart grid implementation. In *Smart Grid Security* (pp. 1-39). Springer, London.

[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]Asghar, M. R., Dán, G., Miorandi, D., &Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communications Surveys & Tutorials*, 19(4), 2820-2835.

[5]Zhang, P., Elkeelany, O., &Mcdaniel, L. (2010, March). An implementation of secured Smart Grid Ethernet communications using AES. In *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)* (pp. 394-397). IEEE.

[6] Iqbal, A., & Iqbal, T. (2018, October). Low-cost and Secure Communication System for Remote Micro-grids using AES

Cryptography on ESP32 with LoRa Module. In *2018 IEEE Electrical Power and Energy Conference (EPEC)* (pp. 1-5). IEEE.

[7] 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.

[8] Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., & Shen, X. S. (2011). A lightweight message authentication scheme for smart grid communications. *IEEE Transactions on Smart Grid*, 2(4), 675-685.

[9] Lv, X., Mu, Y., & Li, H. (2015). Key management for Smart Grid based on asymmetric key-wrapping. *International Journal of Computer Mathematics*, 92(3), 498-512.

[10] Rao, K. V., Rao, M. S., &Vasavi, P. (2018). An implementation of key wrapping for a user in a group using sponge function based on PKCS. *International Journal of Current Research in Life Sciences*, 7(02), 1088-1092.

[11] Bansod, G., Pisharoty, N., & Patil, A. (2016). PICO: an ultra lightweight and low power encryption design for ubiquitous computing. *Defence Science Journal*, 66(3), 259-265.

[12]Shie, S. C., & Jiang, J. H. (2012). Reversible and high-payload image steganographic scheme based on side-match vector quantization. *Signal Processing*, 92(9), 2332-2338.

[13] <http://sipi.usc.edu/database/>

[14]Kamil, Samar, MasriAyob, Siti Norul Huda Sheikh Abdullah, and Zulkifli Ahmad. "Challenges in Multi-Layer Data Security for Video Steganography Revisited." *Asia-Pacific Journal of Information Technology and Multimedia* 7, no. 2-2 (2019).