International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-7, Issue-6, June 2021
ISSN: 2395-3470
www.ijseas.com

Advanced Encryption Standard and Least Significant Bit Combined Techniques: An application to Data and Information Security

1st* Christine Bukola Asaju

Department . of Computer Science, The Federal Polytechnic, Idah, Nigeria,, Chrisamaju02@gmail.com

2nd Florence Funke Abiola

Department of Computer Science,The Federal Polytechnic, ,Idah, Kogi State, Nigeria,chrisamaju0202@gmail.com

Abstract

In this paper, we combine steganographic and cryptographic techniques using Advanced Encryption Standard (AES) with Least Significant Bit (LSB) methods that add up more complexity for the enrichment of data and information security over the network. The proposed scheme embeds the decryption key in the encrypted message using the AES algorithm. The LSB algorithm then shuffles the sequence of message content and disperses bits of the key within the encrypted message in a spatial domain that makes an attack more difficult. We evaluate the performance of the proposed approach by comparing the encryption and decryption time of each technique to the combined method, AES-LSB. The result shows each technique (AES and LSB) took less time to encrypt the message whiles our combined technique used more process time to decrypt a message, confirming improved data security with a Mean Squared Error (MSE) of 0.0049 and a PSNR value of 40 dB.

Keywords—Cryptography,Steganography,Advanced Encryption Standard (AES), Least Significant Bit (LSB)

I. INTRODUCTION

The desire to keep data and information confidentiality, integrity and privacy has been a primary concern to users of communication networks, publishing and broadcasting technology. With the upsurge number of data and information exchanged over the internet, securing data to prevent unauthorized access and users is imperative. It is, however, necessary to have a reliable means for encoding messages or information such that only authorized parties can access it. We can achieve this reliability through steganography or cryptography. Steganography security mechanism hides sensitive information among the bits of a cover file such as an image, text, an audio or a video file in such a way that only sender and receiver could identify the concealed message inside the cover file. Existing communication methods implement this technique to hide the exchange of information and avoid drawing suspicion to the transmission of hidden data. Steganography model involves a carrier or cover-object, message and password. The cover-object embeds the message by hiding its presence in a way that alterations made to the image are perceptually indiscernible. Common among steganography techniques include Least significant bit insertion (LSB), Masking and Filtering, and the transform techniques.

Cryptography, on the other hand, includes encryption and decryption process of a message. According to [1] Cryptography protects sensitive information by encrypting it into an unreadable format called cipher text. The main aim in steganography is to hide the very existence of a message in a cover medium while the goal of cryptography is to make data unreadable by a third party.

While many techniques for securing data have used either cryptography or steganography, many counter techniques expose data based on these approaches posing a challenge to securing data.

Though challenging to decipher encrypted data, it is relatively easy to detect [2]. Encryption only conceals the meaning of messages and not its existence. Using cryptography alone attracts suspicion from the attacker and as such expose the secrecy of the file to threat. Our proposed work provides a reliable means of achieving high data security through to control unauthorized access to confidential and secret messages through creating complexity in the process of unravelling or hacking secret data by making such secret message unsuspicious. Our work provides multi-layers, high Peak Signal to Noise Ratio (PSNR) value, low Mean Square Error (MSE) value, good imperceptibility and robustness of a secret message.

II. RELATED LITERATURE

Hiding data means embedding information into digital content without creating perceptual depravity. In data hiding, three well-known methods can be used. They are watermarking, steganography and cryptography. We define steganography in Greek as covered writing. Steganography includes any process that deals with data or information within other data.

Reference [3] noted that steganography is hiding the existence of a message by hiding information into various carriers. The primary intent is to prevent the detection of hidden information. Research in steganography technique dates back in ancient Greek were during that time the ancient Greek practice of tattooing a secret message on the shaved head of a messenger, and

letting his hair grow back before sending him through enemy territory where the latency of this communications system was measured in months [4].

Reference [5] opined that the reason for this growing interest in steganography is due to the combined use of the techniques to achieving higher levels of security. Reference [6] proposed an encrypting system, combining cryptography and steganography techniques with data hiding. Instead of using a single layer security system scholars have been proposing multi-layer security systems that combine both cryptography and steganography techniques. Reference [7] proposed a method of encrypting a message by a substitution cypher then it will be embedded using LSB insertion. Reference [8] proposed a higher level security approach for data communication system based on AES cryptography and DWT steganography, [9] also presented a dual image steganography technique: countermeasure and analysis which combines LSB embedding based steganographic image technique and AES algorithm to secure the image data from outside intruders and attackers. Also, [10] presented a Dual Steganography Technique Using Status LSB and DWT Algorithms, one that combines two steganography algorithms.

Reference [11] proposed a novel scheme based on steganography and cryptography to embed data in colour images. Reference [12] proposed a system that compresses the secret message encrypts it by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm.

A study by [13] proposed a combined approach of Secure Medical Image, by using encryption and steganography; the image is embedded using lossless LSB data hiding method with patient information, and then the embedded image is encrypted using two share method. Reference [14] demonstrated that a new secure communication protocol could combine steganography and cryptography techniques based on the LSB matching method. Reference [15] used examples of combining steganography and visual cryptography techniques as evidence. In the proposed method, secret data are embedded using a Matrix embedding technique using Hamming codes and shares are generated from this stego image using the Random Grids method. Similarly, [16] presented a new system for the combination of cryptography and Steganography using four keys which, as at then was proved to be a highly secure method for data communication soon.

Reference [17] designed and implemented a secured algorithm using genetic algorithm along with visual cryptography to ensure improved security and reliability. Bansod et al. (2012) suggested algorithm based on hybrid cryptographic techniques built on DES (Data Encryption Standard) and RSA (Rivest Shamir Adleman) algorithms; the combination of both techniques provides superior security control. The suggested algorithm is modified BPCS (Bit-Plane Complexity Segmentation) steganography technique that can replace all the "noise-like" regions in all the bit-planes of the cover image with secret data without deteriorating the image quality.

III. METHODOLOGY

This section describes the proposed technique to achieve better information confidentiality over open communication channels. Our technique uses AES cryptography combined with LSB steganography techniques in the Java programming language. Figure 1 shows a pictorial representation of the proposed framework adopted for the study.

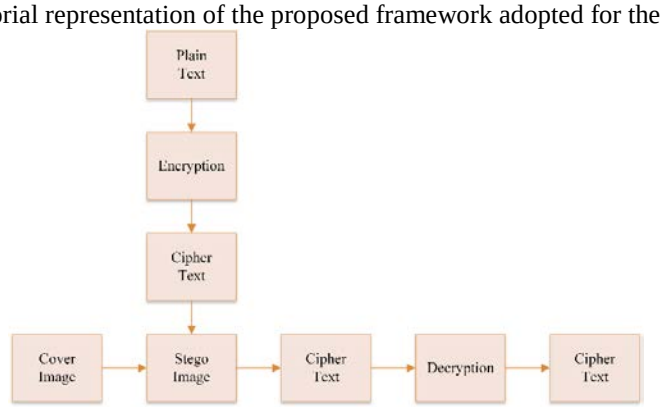

Fig. 1. Proposed Framework

In the proposed scheme, the plain text is converted into a cipher text using the AES encryption algorithm with a key length of 128-bits for this purpose. A cypher key (the same as the one used for encryption) is supplied to decrypt the encrypted message in order to get the original message. We then embed information in the stego image using the LSB (Least Significant Bit) algorithm by replacing the least significant bit of each sampling points with a binary message. After this, the encoded file is cipher text is decoded first and then decrypted by the public key that is known only by the authorized receivers or users of the proposed system.

Figure 2 shows the use case diagrams for the encrypting and decrypting processes of the proposed scheme.

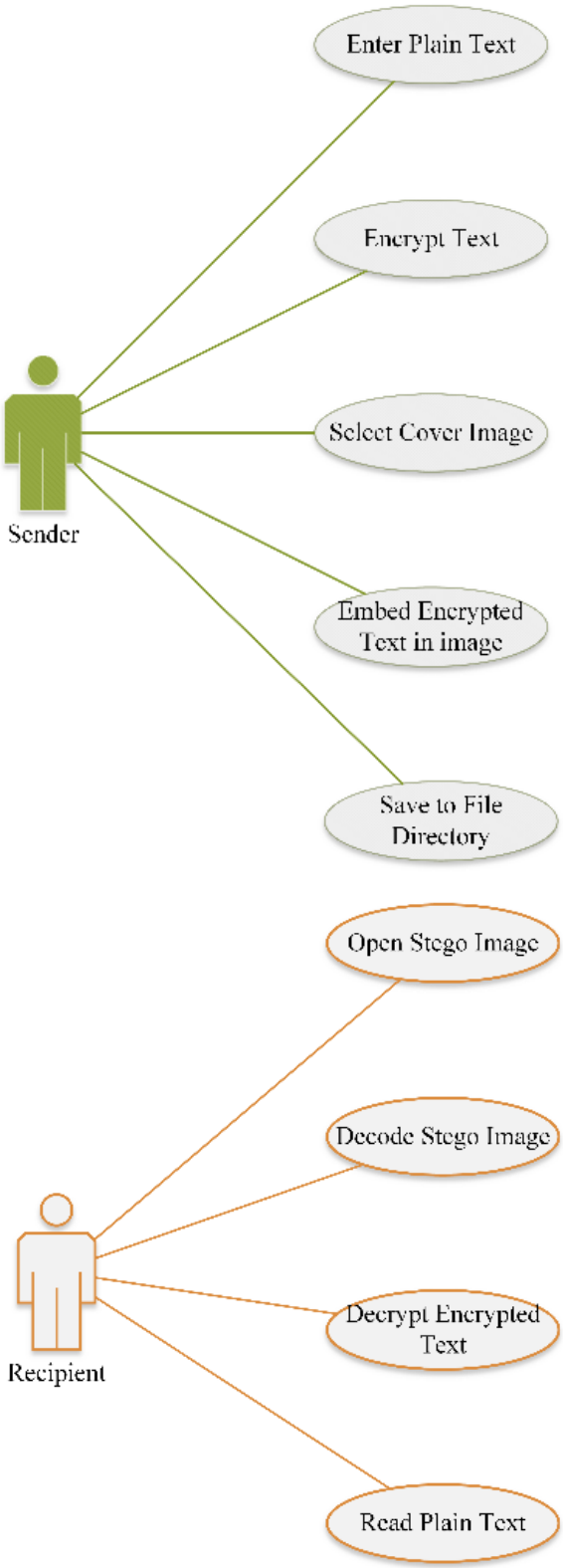

Fig. 2. Sender's and Recipient's Use Case Diagram

IV RESULTS

An application was developed in Java Programming Language to implement the proposed combined algorithm. The application involved two main modules; sender and receiver, respectively. We examine the performance of our proposed approach and quality of stego-file using MSE and PSNR.

Table 1: Testing Result of Stego Image Using MSE and PSNR with their Execution Times

Cover Image	MSE	PSNR	Execution Time
Yung6ix	0.004892	0.412123	4.812003
Casie	0.004900	0.397212	4.112233
Tomatoes	0.004901	0.401310	3.812003
Average	0.004898	0.403548	4.245413

From table 1, we observed that the average value for MSE and PSNR were 0.004898 and 40.35dB respectively, with an average execution time of 4.25. The higher the PSNR value, the less the the image distortion. We could then explain that it is less likely to have a variety of visual attacks by the human eyes (HSV) if the value of PSNE is large. Figure 3 and 4 show the comparison of cover images and stego images.

Fig. 3. Original Images (Cover Images)

Fig. 4. Stego Images

V. CONCLUSION

This research presented a new secure communication model that combines cryptography and steganography methods to provide two-layer security to hide the existence of a secret message. We test the encryption scheme using three images with dimensions of 280 by 280. Firstly, the secret message is encrypted using the AES cryptographic technique, and then the encrypted data is hidden or embedded in the cover image using LSB steganography. With this combination, the secret message can be transmitted over an open channel because not only does the cipher text look meaningless, but its presence is concealed by using steganography to hide its existence in an image.

Our experimental results showed that our proposed approach outperforms the original AES and LSB obtaining a PSNR value of 40dB from the stego image. In practice, it becomes challenging to see the differences between the cover image and the stego-image for PSNR greater than 40 dB. The higher the PSNR value, the less the distortion of the image will be.
Future work, the proposed encryption scheme will be applied to an audio and video data whiles focusing on obtaining higher PSNR value.

REFERENCES

1. Guru A, Ambhikar A. A Study of Cryptography to Protect Data from Cyber-crimes. Research Journal of Engineering and Technology. 2020 Apr 1;11(2):45-8.

2. Vrijsen JH, Rubens M, Junkers T. Simple and secure data encryption via molecular weight distribution fingerprints. Polymer Chemistry. 2020;11(40):6463-70.

3. Lou, D. C., Wu, N. I., Wang, C. M., Lin, Z. H., & Tsai, C. S., “A novel adaptive steganography based on local complexity and human vision sensitivity”. Journal of Systems and Software, vol. 83(7), 2010 1236-1248.

4. Arya, Manish Kumar. "Implementation and Analysis of Steganography Methods." National Institute of Technolgy,Kurukshetra (2018).

5. AlKhodaidi T, Gutub A. Refining image steganography distribution for higher security multimedia counting-based secret-sharing. Multimedia Tools and Applications. 2021 Jan;80(1):1143-73.

6. Usha, S., Kumar G. A. S and Boopathybagan, A Secure Triple Level Encryption Method using Cryptography and Steganography. International Conference in Computer Science and Network Technology (ICCSNT) IEEE, 2(11), 2011, pp. 1017-1020.

7. Laskar, S. A., & Hemachandran, K., "High capacity data hiding using LSB steganography and encryption". International Journal of Database Management Systems, vol. 4(6), 2012, pp. 57-96.

8. Saja, M.S.and Aser, M.M., "Higher level security approach for data communication system based on AES cryptography and DWT stenography." Jordanian Journal of Computer and Information Technology, vol. 2 (3), 2016, pp.6-20.

9. Deepak, K. P., Srinivasa, D. R. and Sriram, G., "Dual image steganography technique: countermeasure and analysis". IOSR Journal of Computer Engineering (IOSR- JCE),vol. 18(6), 2016, pp. 92-100.

10. Manisha and Deepkiran M., "Dual steganography techniques using status LSB and DWT algorithms". International Journal of Innovative Research in Computer and Communication Engineering, vol. 4(6), 2016, pp. 121-130.

11. Li Q, Wang X, Wang X, Ma B, Wang C, Xian Y, Shi Y. A Novel Grayscale Image Steganography Scheme Based on Chaos Encryption and Generative Adversarial Networks. IEEE Access. 2020 Sep 2;8:168166-76.

12. Umamaheswari, M., S. Sivasubramanian and S. Pandiarajan., "Analysis of different steganographic algorithms for secured data hiding, ijcsns international journal of computer science and network security", vol. 10(8), 2010, pp. 154-160.

13. Pandey and Shrivastava, . Secure medical image transmission using combined approach of data hiding, encryption and steganography. International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2(12), 2012, pp. 54-57.

14. Sharma K, Aggarwal A, Singhania T, Gupta D, Khanna A. Hiding Data in Images Using Cryptography and Deep Neural Network. arXiv preprint arXiv:1912.10413. 2019 Dec 22.

15. Wu X, Yang CN. Partial reversible AMBTC-based secret image sharing with steganography. Digital Signal Processing. 2019 Oct 1;93:22-33.

16. Prema, G. and S. Natarajan,. "Steganography using genetic algorithm along with visual cryptography for wireless network application". In Information Communication and Embedded Systems (ICICES),International Conference, IEEE, 2013, pp: 727-730.