International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 6 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195659

Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography

Musa. M. Yahaya, Aminat Ajibola
Department of Computer Science, University of Abuja, Abuja, Nigeria
Corresponding Author's Email: mmyahaya05@gmail.com

ABSTRACT

Recently, the rate of data transfer over the internet globally has increased and this called for more data security as security of data is of great concern for individuals as well as business owners. Cryptography and steganography are two major key players for data security technique. Cryptography is use to perform encryption on the secrete message while steganography hides the secrete message in digital media, image in this regards. This paper employed these two techniques using Advanced Encryption Standard (AES) for the cryptography and Least Significant Bit (LSB) for the steganography. Combining the two algorithms ensured data integrity, data security, and flexibility. The changes in the secrete message carrier (Stego) is insignificant and is often not noticeable by the nicked eyes, thus this make the interception of the message often difficult by intruder.

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

I. INTRODUCTION

In the new era, with a fast-growing of internet usage across the globe and new trend in information technology, this make information security more demanding in data transmission data storage. Therefore, the security of vital information or data from an intruder or unauthorized access is important. Cryptography and steganography are key players in the field of information security.

The need for data security has become daily concern for government, individuals and business owners, thus, the high demand for data privacy. Cryptography, which entails encryption and decryption, is one of the popular methods for accomplished data security. Encryption converts plain text in to cipher text, while decryption converts cipher text back into the original format (plain text). Ciphers are known to be mathematical functions or cryptography algorithms used for data encryption and decryption [1].

In earlier days, only textual format was commonly used as data format, but recently different file formats such as audio, image and video can seamlessly be transmitted over the internet with the help of computer networks that grows rapidly. The huge amount and frequency of data being transfer often make the data prone to attack or low data privacy. Image security is an application layer technology to protect the transmitted information against modification and unwanted disclosure while in transit. [2]. This ranging from copyright, confidentiality, protection, authentication and access control.

II. LITERATURE REVIEW

As technology evolved, digital commination is also evolving speedily which leads to increase in

information dissemination. In addition, the secret information is often being transferred using public or open channels which make the data more prone to attack.

In the recent decades, the number of data security threats has been gradually increased and this has always been area of great concern for security experts across the globe. To circumvent this challenge, cryptography and steganography have key role to play. The two techniques can be used together to achieve higher security level compare to when they are used separately.

In [3], the authors presented an improved secure data transfer scheme using smart Internet of Things (IoT) environment. Their proposed technique employed an integrated approach of steganography and cryptography during transfer data between IoT device & and home server and cloud server. The data sensed from IoT device is encrypted and embedded in the cover image along with message digest of data sensed and send to the home server for authentication purpose. At the home server the embedded message digests and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is repeated between home server and cloud server.

In [4], the authors proposed an integration of RSA cryptography and audio steganography in which the secret message is converted to ciphertext using the RSA algorithm alongside LSB audio technique where the converted ciphertext is hidden. The authors ascertained that the combination of the two techniques resulted in higher level of data security.

In [5], the authors presented a hybrid-based approach for securing image transfer which provides reliable and quality encryption. The encryption of the image was done using blowfish algorithm to produce the cipher image. Furthermore, the encrypted image is embedded using LSB technique in the cover image. Blowfish algorithm is lossless and highly secured encryption technique, added by the authors.

In [6], the authors proposed a method that increases the security of data transfer by combining cryptography and steganography. Mp3 file is taken as the cover media and AES was adopted to encrypt the secret message by using MD5 has function processed key.

In [7], authors in this research came up with space domain steganography where secret image and carrier image are taken of same size. Pseudo random noise sequence of both image is generated which is dependent on key. A single plane (R or G or B) is selected from both the images. The career image plane is divided into a set of 16 pixels, and the selection of these pixels is achieved in a manner in which they appeared. Also, the given plane of secret image (SI) is sliced into a set of 16 pixels based upon column select sequence and row select sequence sequences. Then selected pixel was ciphered using second key and farther embedded into the carrier image.

The authors in [8] proposed techniques using AES algorithm for securing ecommerce and m-commerce. This algorithm was combined with LSB technique to ensure the model is more secure and reliable. Block size of 16 bytes with 128-bit keys was adopted, the authors ascertained that this is the best combination for operation based on the memory limitation and speed of the devices used. The authors concluded that high level of data security and invisible communication was obtained in their model by combining steganography and cryptography.

III. CRYPTOGRAPHY AND STEGANOGRAPHY

A. Cryptography

Cryptography is commonly known as the art of secret (crypto) writing (graphy). This is also referred to as the science or art of combining the methods and principles of transforming an intelligible data into an unintelligible one, and then decrypting or transforming the message back to its original form [9].

According to [10], cryptography is described as a "method of storing and transmitting data in a form that only those it is intended for can read and process it".

Encryption and decryption operations are structured and controlled by one or more keys. Private key cryptography method uses the same secrete key for both encryption and decryption, while public key cryptography uses different keys for encryption and Fig. 1 depicts the cryptography model.

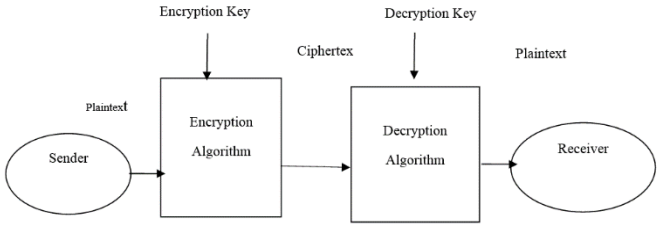

Fig. 1. Cryptography Model

B. Steganography

Steganography is generally known as the method of hiding the secret messages or its existence so that it remains unidentified or undetected. One of the major advantages of steganography over cryptography is that its conceals the presence of the secrete message, also the potential secret message does not attract attention to itself as an object of security. Steganography today, however, is significantly more sophisticated, allowing a user to hide large amounts of information within an image, audio, and video files. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is the encryption of the secrete message and then hidden, so that an adversary has to first find the information (an often difficult task in and of itself) and then decrypt it as shown in fig. 2.

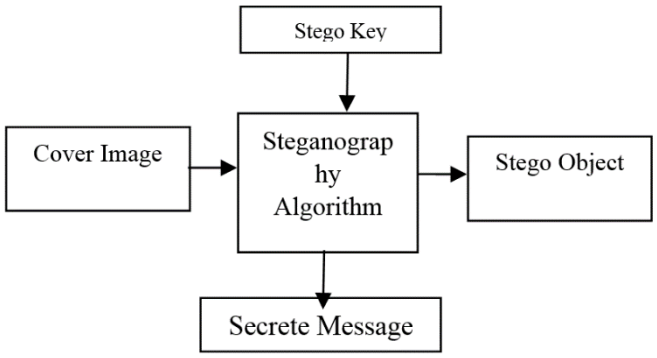

Fig. 2. Steganography Model

AES Algorithm

Advanced Encryption Standard, AES is cryptography algorithm which is a block cipher with a block length of 128 bits. Its allows three different key lengths which are 128, 192, or 256 bits. This research focused on 128 bits' key length with respect to using another key length other than 128 bits, in which the major thing that changes in AES is the key scheduling is generation from the key.

The Encryption process consists of 10 rounds for processing 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. All rounds are identical with the exception of the last round.

Each processing round includes one single-byte based substitution step, a column-wise mixing step, a row-wise permutation step, and the addition of the round key. The order in which these steps are executed completely differs for encryption and decryption.

Before any round-based processing for encryption can be initiated, the input state array is XORed with the first four words of the key schedule. The same process take place during the decryption except from that fact that the ciphertext state array will be XORed with the last four words of the key schedule.

The Advance Encryption Standard (AES) can be categorized in to four phases as follows:

- ✓ Byte Substitution
- ✓ Shift Rows
- ✓ Mix Column
- ✓ Add Round Key

The input block is first arranged into a 4x4 byte of array and is XOR with the128-bit before any of these phases begins [6].

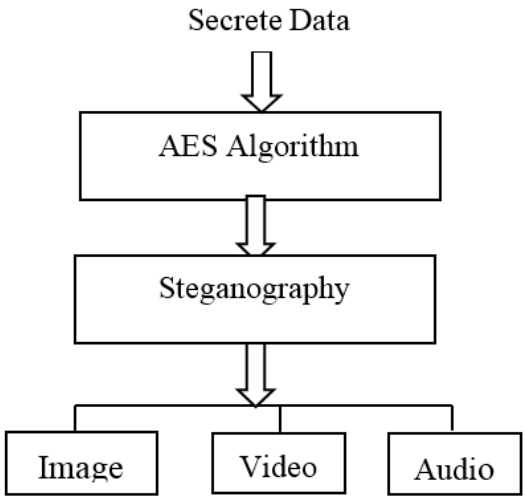

Fig. 3. AES and Steganography Algorithm

LSB Encryption Algorithm: First the secrete message (file in fig. 4 and Text in fig. 5) is chosen or inputted as shown in Fig. 4 and 5 respectively, and the cover image is selected. Afterwards, the secrete message has to be converted into ciphertex or binary format. The binary conversion is performed by taking the American Standard Code of Information Interchange (ASCII) equivalent values of the character and convert them into binary format after which stream of bits are generated. The Bytes in the cover image representing the pixels are taken in an array which leads to generation of byte stream.

Bits of message are taken orderly and are further placed in LSB bit of image byte. Same procedure is taken until all the message bits are all placed in the image bytes. The image produced is referred as '*Stego-Image*' as depicted in the Fig. 4 and 5 respectively.

LSB Algorithm for Hidden the Secret Data in Career Image

Step 1: Read the career image and the secret message which is to be embedded in to the career image.
Step 2: Compress the secret message.
Step 3: The compressed secret message is converted into ciphertext using the secret key
Step 4: Convert the compressed encrypted secrete message into binary form.
Step 5: Find LSBs of each pixels of the career image.
Step 6: Embed the bits of the secret message into bits of LSB of pixels of the career image.
Step 7: Continue the procedure until the secret message is fully embedded into career image.

The LSB Decryption Algorithm: This is the revert of the encryption process in which the 'Stego-Image' is first chosen to generate single array of bytes. The total number of bits of encrypted secret message and the bytes representing the pixels of stego-image are taken. The counter is set to 1, and this gives an index number of the pixel byte where secret message bit is available in LSB. This process is continued until the final count of the secret message bit is reached. Follow this process is the generation of the bit stream of the message

Algorithm for Decrypting the Secret Message
Step 1: Select the stego image.
Step 2: Get the LSBs of each pixel of the stego image.
Step 3: Find and retrieve the LSBs of each pixel of the stego image.
Step 4: Continue the process until the secrete message is extracted from stego image.
Step 5: Decompress the secret message
extracted in step 4.
Step 6: Decrypt the secret message using the secrete key used for encryption.

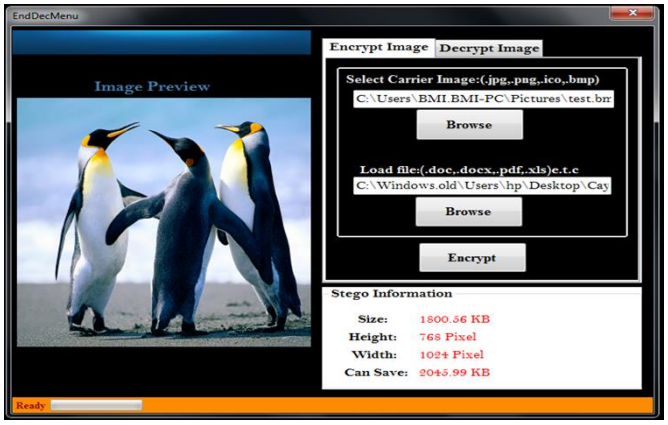

Fig. 4 Sample Implementation of File Encryption and Decryption

Fig. 4 shows the encryption and decryption module where user can encrypt or decrypt different file formats.

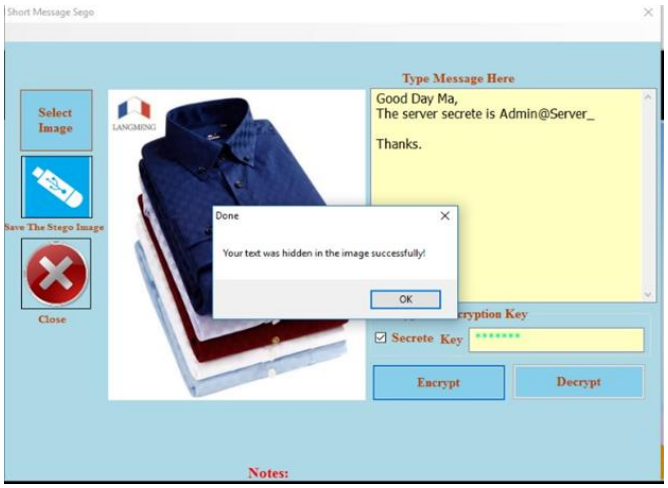

Fig. 5. Sample Implementation of Text Encryption and Decryption

Fig. 5 depicts a user define message where user input the secret message and chose a desire password to encrypt the secret message.

IV. CONCLUSION

An attempt has been made in this paper to identify the key elements or requirements for data security technique in which secure data transmission can take place over open channels without the fear of data breach or interference by third party. Steganography technique is mostly used for data hiding. This technique come under the general believe that if the future is visible, then the chances is high, thus, the primary goal in steganography is try as much as possible to obscure the existence of the embedded secrete data. Using steganography alone or cryptography alone is not a good solution that can be used to circumvent data breach. On the other hand, combining the two techniques provides more data security. Combining these two techniques produced double layers of protection as encrypted message is also embedded using steganography method which reduced the chance of the embedded message being detected. The secrete message is embedded into an image in such a way that the degradation in the stego image quality if often not noticeable.

Compliance with Ethical Standards

This article was neither founded by cooperate body nor individual.

Conflict of Interest:

There is no conflict of interest among the authors.

V. REFERENCES

[1]. Slain T., Deon S. (2004). Symmetric Key Encryption using Rijndael and C#.

[2]. Narendra K Pareek (2012). Design and analysis of a novel digital Image encryption) scheme. International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2.

[3]. Ria Das, Indrajit Das (2016). Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques. IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN).

[4]. Ankit Gambhir and Sibaram Khara (2016). Integrating RSA Cryptography & Audio Steganography. IEEE ICCCA.

[5]. Moresh Mukhedkar, Prajkta Powar and Peter Gaikwad (2015.). Secure non real time image encryption algorithm development using

cryptography & Steganography. IEEE INDICON.

[6]. Irfan Pratama (2016). Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function". International Conference on Science and Technology-Computer. (ICST), IEEE.

[7]. Nikhil Patel, ShwetaMeena (2016). LSB Based Image Steganography Using Dynamic Key Cryptography. International Conference on Emerging Trends in Communication Technologies (ETCT).

[8]. S. H. Gawanda and P. Y. Pawar, (2012). M-Commerce Security Using random LSB Steganography and Cryptography." International Journal od Machine Learning and Computing, vol. 2(4).

[9]. Amogh Mahapatra, Rajballav Dash (2007), Data encryption and decryption by using hill cipher technique and self-repetitive matrix", International Conference on Intelligent Computing, Computer Science & Information Systems.

[10]. Himanshi Sharma, Kamal Kumar Sharma and Sharad Chauhan (2015). Steganography Techniques Using Cryptography-A Review", Paper. International Journal of Recent Research Aspects, Special Issue: Engineering Research Aspects ISSN: 2349-7688.

Cite this article as :

Musa. M. Yahaya, Aminat Ajibola , "Cryptosystem for Secure Data Transmission using Advance Encryption Standard (AES) and Steganography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 6, pp. 317-322, November-December 2019. Available at doi : https://doi.org/10.32628/CSEIT195659

Journal URL : http://ijsrcseit.com/CSEIT195659