IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10512

SECURED INFORMATION IN DIGITAL IMAGE WITH ADVANCE ENCRYPTION SYSTEM (AES) AND LEAST SIGNIFICANT BIT (LSB)

Bolaji-Adetoro[1], D.F., Isiaka, O.S[2] & Abdulkareem Q.B [3]

Department of Computer Science, Institute of Information and Communication Technology,
Kwara State Polytechnic, Ilorin[1,2,3]

Abstract: With the ever increasing amount and variety of data to be stored and transmitted in various mediums, the specification of security which has to be established at various levels of medium access and the accompanying issues of authentication and authorization has become a critical factor. Various steganographic, watermarking and data-embedding algorithms have usually manipulated the actual data in order to either hide any coveted information or to provide some level of access control over the medium. The mediums are usually images, video, audio etc., wherein specific portions or the overall space is usually 'corrupted' with 'significant' data. We attempt to bring out the significance of the steganographic techniques that are employed in information processing algorithms for data security. It deals with the problem of data security, focusing mainly on images, and tries to state the various properties and characteristics that the steganographic algorithms should possess. We also highlight the technique of masking used in the conventional steganographic LSB algorithms and in its variants.

Keywords: Steganography, LSB Algorithm, AES Algorithm, ASCII codes.

I. INTRODUCTION

Steganography is a study of techniques that embed secret information imperceptibly into a cover medium for the purpose of security, protection or covert communication [7]. Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually unencrypt the data. A solution to this problem is steganography.

The inability to detect the hidden data, perceptually or by computer analysis, is paramount for surreptitious operation [3]. Steganographic messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stego-text. For example, the letter size, spacing, typeface, or other characteristics of a cover-text can be manipulated to carry the hidden message; only the recipient, who must know the technique used, can recover the message and then decrypt it.

This research presents hidden information in digital image with advance encryption system and least significant bit as a means of securing data transmission and data storage. Hereby, important files carrying confidential information can be stored under a digital image in the server in an encrypted format. Access to these files is limited to certain authorized people only i.e. people with access key. Transmission also takes place in an encrypted format so that no intruder can get any useful information from the original file during transit. There are many cases where organizations and/or individuals would want to share secrete information. The communication of this secrete information should be carried out over the network without any interference or hacking process or damage to packet data being sent.

II. LITERATURE REVIEW

Various researchers have done related works on advance encryption system (AES) and least significant bit (LSB) as means of securing data; some of their works are listed below:

[13] proposed an efficient data encryption to encrypt sensitive data before sending to the cloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. In addition, data users can reconstruct the requested data from cloud server using shared secret key. They analyzed the privacy protection of outsourced data using experiment carried out on the repository of text files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10512

[15] presented a steganographic approach of concealing the secret data so as to facilitate secure communication. Arnold transformation has been imposed on the chosen cover image in the first stage. This results in the scrambling of the data bits, thereby disrupting the normal pixel orientation. Thereafter, Mid Position Value (MPV) technique is implemented to embed data bits from the secret image within the scrambled cover. Lastly, inverse Arnold transformation is applied on the above image. This results in a descrambling operation, i.e. reverting back the normal orientation. Henceforth the stego is generated. All the experimental results analyze the outcome of the full methodology. For this purpose, several quantitative and qualitative benchmark analysis pertaining to this approach have been made. All the results show that the imperceptibility, i.e. non-detectability of secret data is well maintained. Also the payload is high with negligible distortion in the image quality.

[14] observed that a cryptography and steganography could be used to provide data security, each of them has a problem. Cryptography problem is that, the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. Steganography problem is that once the presence of hidden information is revealed or even suspected, the message is become known. According to the work in this paper, a merged technique for data security has been proposed using Cryptography and Steganography techniques to improve the security of the information. Firstly, the Advanced Encryption Standard (AES) algorithm has been modified and used to encrypt the secret message. Secondly, the encrypted message has been hidden using method in. Therefore, two levels of security have been provided using the proposed hybrid technique. In addition, the proposed technique provides high embedding capacity and high quality stego images.

[2] presented a security system that can provides privacy and integrity for exchanging sensitive information through the internet or the communication networks, based on the use of recently developed encryption algorithms, such as AES, IDEA and RSA. The aim of the work is to develop a simple file transfer system that can obtain privacy, integrity and authentication for the file transfer process. The proposed system uses symmetric cryptography system. File transfer must provide end-to-end visibility, security and compliance management.

[12] described the information security using the poly-substitution method in a linear way. The method generated ASCII values of the given text and then applying conversion, transposition with the features of the cryptography. Cryptography is the science of using mathematics to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure networks. In the poly-alphabetic substitution method, the same plain text letters could be encrypted in a different ways in different part of the data. As the name poly alphabetic that more than one key and random keys with combinations can be used. In case of two keys e1, e2 and let the ASCII values of e1 be 1 and e2 be 2 and take the text, add ASCII values of e1 to first character and ASCII values of e2 to second character and add alternatively to consecutive characters.

III. STATE OF STEGANOGRAPHY

Currently, the emphasis has been on various forms of digital steganography. Commonly there are a number of digital technologies that the community is concerned with, namely text files, still images, video and audio [4]. It is beyond the scope of this project into go into the details of steganographic methods. The majority of today's steganographic systems use multimedia objects like image, audio, video etc, as cover media because people often transmit digital pictures over email and other Internet communication [6]. Modern steganography schemes provide a complementary goal of security for the privacy of digital data: Moreover, the Internet provides a huge amount of data of a given format and for each format of cover media, many specific steganography schemes exist [11]. The modern concept of data hidden is shown in figure 1.

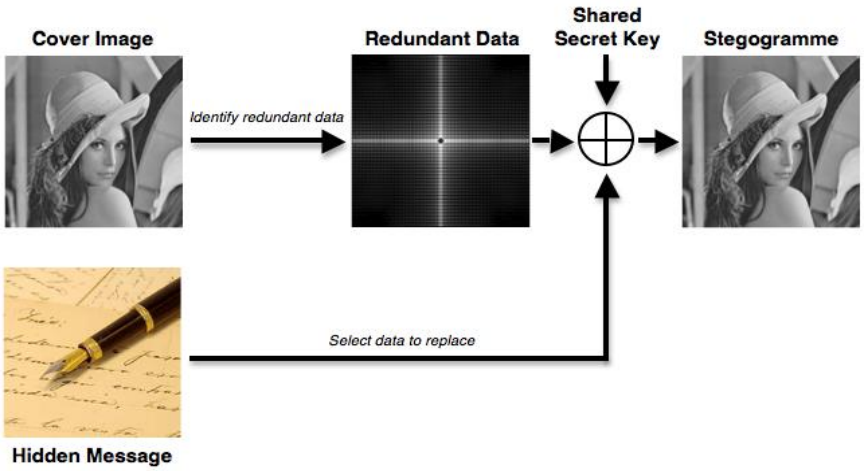

Figure 1: steganography and steganalysis
Source: Steganography Wikipedia, 2015

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10512

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [3]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily according to [9]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding [1]. In modern approach, depending on the nature of cover object, steganography can be divided into [8] and [11]:

a) *Text Steganography*: Text steganography is a mechanism of hiding secret text message inside another text as a covering message or generating a cover message related with the original secret message. There are three main categories used to hide text-in-text messages, that is, format based, random and statistical generations, and linguistic method.
b) *Image Steganography*: To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications.
c) *Audio Steganography*: Audio steganography is about hiding the secret message into the audio. It is a technique uses to secure the transmission of secret information or hide their existence. It also may provide confidentiality to secret message if the message is encrypted. For example, two individuals who just want to send the occasional secret message back and forth might use the LSB coding method that is easily implemented.
d) *Video Steganography*: Video file is a combination of both images and audio. So, video steganography is nothing but a combination of image and audio steganography. So, the combined evaluations i.e., the evaluations for image and audio steganography can be taken together for the evaluation of video steganography. While doing video steganography, the effect on video has to be kept in mind to achieve a secure communicating media.

IV. METHOD AND MATERIALS

Various modules are present in the framework of the proposed system as shown in figure 2.

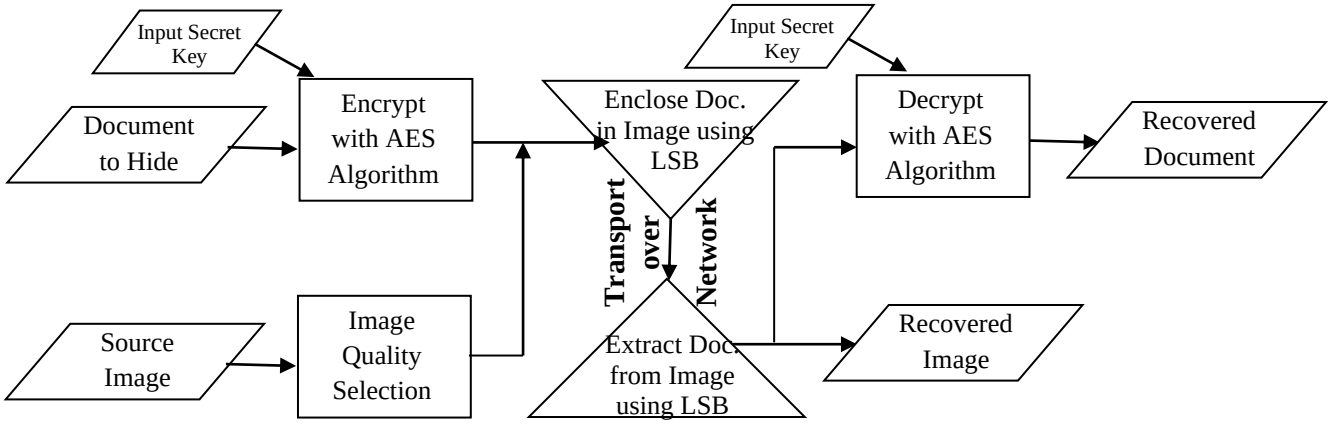

Figure 2: Proposed system architecture

AES Encryption

AES encryption is used for encryption of the secret data. It provides double layer of security check. If by chance the hacker decodes the text in image file, it will not be able to decode the AES encrypted information. AES is responsible for performing encryption/decryption on the data. In case of 128 bit key, AES perform substitution and permutation to transform the input data to ciphered data. The first Nr-1 rounds of encryption, AES makes use of SubByte, ShiftRow, MixColumn and AddRoundKey operations but MixColumn operation is skipped in the final round to complete the encryption process as shown in figure 3.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10512

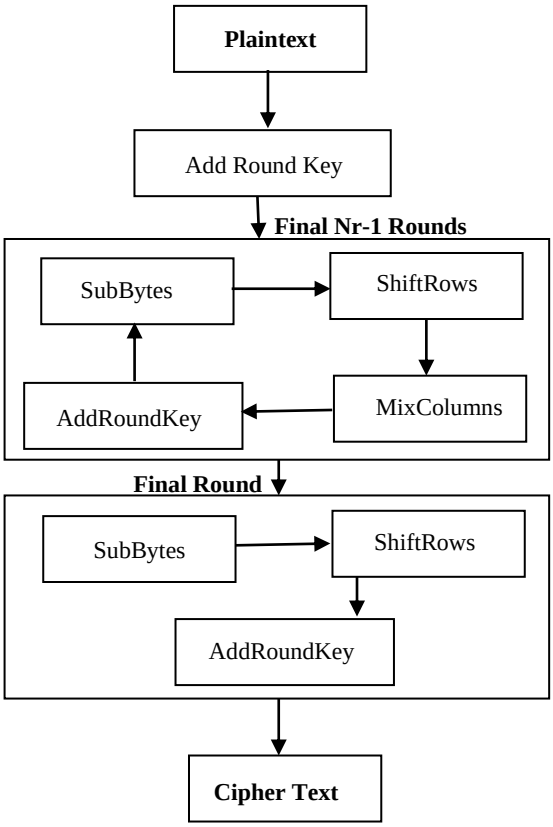

Figure 3: AES Encryption Process

The four steps involved in the implementation of AES as shown in figure 3 can be described as thus:

a) SubBytes Step: This step is same as SubBytes step of AES algorithm. In the S-Box Substitution step, each byte in the matrix is reorganized using an 8-bit substitution box. This substitution box is called the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF (28), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points. This step causes confusion of data in the matrix. S-Box Substitution is carried out separately for LPT and RPT. This is the first step of iterative round transformation. The output of this round is given to the next round.

b) ShiftRows Step: The ShiftRows step is performed on the rows of the state matrix. It cyclically shifts the bytes in each row by a certain offset. The first row remains unchanged. Each byte of the second row is shifted one position to the left. Similarly, the third and fourth rows are shifted by two positions and three positions respectively. The shifting pattern for block of size 128 bits and 192 bits is the same.

c) MixColumns Step: In the MixColumns step, the four bytes of each column of the state matrix are combined using an invertible linear transformation. A randomly generated polynomial is arranged in a 4*4 matrix. The same polynomial is used during decryption. Each column of the state matrix is XOR-ed with the corresponding column of the polynomial matrix. The result is updated in the same column. The output matrix is the input to AddRoundKey.

d) AddRoundKey: The AddRoundKey operation is the only phase of AES encryption that directly operates on the AES round key. In this operation, the input to the round is exclusive-ored (XORed) with the round key. For every round a new round key is generated using Rijndael‟s key scheduling algorithm.

LSB Algorithm

LSB algorithm is used to hide information on the lower bits of the image. The LSB algorithm is efficient and can hide vast amount of information. Embedding in the cover image is done by least two-significant-bit substitutions (2LSB) [7], which means that each of the least two significant bits holds one bit of message. Bits of a pixel are flipped whenever they are not equal to the message bits.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10512

In digital steganography, sensitive messages may be concealed by manipulating and storing information in the least significant bits of an image or a sound file. In the context of an image, if a user were to manipulate the last two bits of a color in a pixel, the value of the color would change at most ±3 value places, which is likely to be indistinguishable by the human eye. The user may later recover this information by extracting the least significant bits of the manipulated pixels to recover the original message [7]. This allows for the storage or transfer of digital information to be kept concealed. Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works for image, audio and video steganography. To the human eye, the resulting Image will look identical to the cover object [8].

It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in $2^{31}\ldots 2^{0}$) [7]. By extension, the least significant bits (plural) are the bits of the number closest to, and including, the LSB. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits (MSBs) stay unchanged (000 to 000).

V. RESULT AND DISCUSSION

A variable length text of string is supplied either from keyboard or from disks file and the user selects one of five different encryption schemes. The scheme consists of all a list five different concentration of randomly generated number and characters, based on the system timer. Once a scheme is chosen, the user supplies an encryption key and calls for encryption process. Assuming the user type the plain text "Visual basic is here to stay forever" and supplies "dog" as the encryption key, system takes the first character of the plaintext which is V in this case and also take the first character of the key, which is d. it then find their ASCII codes and adds them together (86+100) to attain 186. This V is converted to the represented by ASCII code ‖. Next, it takes 'i' in the plaintext and 'o' in the key and obtain (105+111) or the character ╬ then 's' and 'g' yield (115+103) or the character ┌. 'u' and 'd' give 217 or ┘, 'a' and 'o' yield 208 or ð while 'l' and 'g' also give 208 or ð. In such, the word "Visual" can be converted to ASCII code ‖╬┌┘ ðð. The same process goes for other words in the sentence. The output will be embedded in the secret image to be transported over the network.

The proposal system is a pc-based data encryption system that works in the windows OS environment. It is designed to be able to accept text input and apply a series of transformations on the input text to produce an encrypted text. The system is based on the basic creaser substitution techniques, which involves shifting of alphabets of the given plain text by a specified number of place in a specified direction. The new system operates on a slightly different principle of substitution, but the security is significantly greater than that of the ordinary substitution method.

VI. CONCLUSION

Many different techniques of steganography, which are emerging areas used for secured data transmission over any public media, exist and will continue to be developed. However, hackers have devised advanced ways of detecting hidden messages. Having this in mind, efficient steganography techniques such as the one presented in this research work will be of optimum relevance. The software is developed in such a way that the secret key will merely point out parts of a cover source which leave the message undetected as it contains no information about the secret message at all when passed over a computer network. The author incorporated the idea of secret key and password security features for authentication at both ends in order to achieve high level of security. As a further improvement of the security technique, the information has been permuted, encoded and then finally embedded on an image to form the stego image. The carrier can be sent to a receiver without anyone except the authenticated receiver knowing the existence of this information.

REFERENCES

[1]. Abrams, M. and Podell, H. (2001). Cryptography Potentials, *IEEE*, pp. 36 – 38, **20 (1)**, Feb.-Mar., 2001.

[2]. Akanksha, S. and Ajeet, B. (2016). Design of Secure File Transfer over Internet. International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 11, pp 471-473. IJARCCE ISSN (Online) 2278-1021 ISSN (Print) 2319 5940.

[3]. Ash, S., Mukherjee, S., and Sanyal, G. (2015). A DWT Based Steganographic Method using Prime First Mapping (PFM). Advances in Computing and Communicational Engineering, ICACCE, 471-476.

[4]. Blakley, G.R (1999). Twenty Years of Cryptography in the Open Literature, Security and Privacy 1999. *Proceedings of the EEE Symposium*, 9 – 12 May 1999.

[5]. Eijk, N.V. (2011). File Sharing. Manuscript completed in March 2011/rev May 2011. © European Parliament, Brussels, 2011. Accessed http://www.europarl.europa.eu/studies on 12/5/2021.

[6]. Imai H. Hanaoka G., Shikata J., Otsuka A. and Nascimento A.C. (2002). Cryptography with Information Theoretic Security. *Information Theory Workshop*, 2002, *Proceedings of the IEEE*, 20 – 25.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10512

[7]. Joshi, R. Gagnani, L., and Pandey, S. (2013). Image Steganography with LSB. International Journal of Advanced Research in Computer Engineering & Technology. **2**.
[8]. Kanan, H. and Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst. Appl. **41 (14)**: 6123-6130.
[9]. Menezes, J., Van, P.C. and Vanstone S.A. (2000). Handbook of Applied Cryptography. National Institute of Standards and Technology, Advanced Encryption Standard, FIPS-197, http:// csrc.nist.gov/archive/aes/index.html, 2000. General References for Cryptography.
[10]. Mukherjee, S. and Sanyal, G. (2017). Enhanced Position Power First Mapping (PPFM) based Image Steganography. International Journal of Computers and Applications (IJCA), Taylor and Francis **39**:59-68.
[11]. Nagpal, K. D., and Dabhade, P. D. S. (2015). A Survey on Image Steganography and its Techniques in Spatial and Frequency Domain. International Journal on Recent and Innovation Trends in Computing and Communication **3 (2)**: 776-779.
[12]. Navnish, S., Amitabh, L., and Babloo, E. (2011). Information Security: Encryption and Decryption with Polyalphabetic Substitution Method. International Journal of Computer Science and Communication. Vol. 2, No. 1, pp 41-44.
[13]. Prakash, G. L., Manish P. and Inder S. (2014). Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System. International Journal Of Engineering And Computer Science. Volume 3 Issue 4 pp 5215-5223.
[14]. Saleh, M. E., Abdelmgeid, A. A. and Omara, F. A. (2016). Data Security Using Cryptography and Steganography Techniques. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016. Pp 390-397.
[15]. Srilekha M., Subhajit R. and Goutam S. (2018). Image Steganography using Mid Position Value Technique. International Conference on Computational Intelligence and Data Science (ICCIDS). Procedia Computer Science 132(2018), pp 461-468.