International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 3136–3141

Securing Data on Cloud Using Image Steganography and Cryptography

Kiran D. Yesugade[1], Isha R. Sangrolkar[2], Gayatri P. Patil[3], Pooja A. Kashid[4]

[1]Professor, Department of Computer Engineering, BVCOEW, Pune, India

[2,3,4]Department of Computer Engineering, BVCOEW, Pune, India

[1]kiran.yesugade @gmail.com,
[2]ishasangrolkar@gmail.com, [3]pgayatri994@gmail.com, [4]poojakashid1811@gmail.com

Abstract

Cryptography and steganography can be used to provide data security, but if used solely, each of them has a problem. In Cryptography the cipher text is in unreadable form. Hence, attacker might suspect the encrypted data and can read the data by decrypting it. In Steganography, once the presence of the hidden data is suspected, the data can be revealed, and the hidden data can be read. In our proposed methodology, a more secure version of Image steganography is given which provides an extra security and makes it harder to uncover the hidden message by steganalysis. Firstly, the message to be hidden will be encrypted using AES algorithm followed by the proposed image steganography method. The proposed image steganography method will convert the cover image into grids, swap these grids and embed the encrypted message into the swapped gridded image using LSB technique.

Keywords: *Steganography, Image Steganography, Cryptography, AES*

1. Introduction:

Steganography and Cryptography are the most commonly used methods to secure the data transmission over network. Cryptography is the art and science of protecting data by making it unreadable. This unreadable text is called as the ciphertext. Image Steganography is an art of concealing the information under some image such that only sender and receiver knows the existence of data. Safety of the embedded data can be improved by the blending of these two procedures. This blend of two procedures will satisfy the numerous requirements as, safety, volume and robustness for safe broadcasting of data over network that is open. Although both techniques are providing the security separately, to offer strong security we recommend combining both techniques Steganography as well as Cryptography into one system. First the information is encrypted and then the encrypted information is hidden behind an image using Image Steganography technique which is least significant bit (LSB) in our case. Hence, combination of Cryptography and Steganography will secure the data while transmitting it over the network.

2. Literature Survey:

Cryptography and steganography are the most popular security techniques used to get rid of the security risks.

In [1], firstly, the study of safety and security attacks on cloud is done, and after to fix these attacks steganography as well as cryptography methods are discussed.

ISSN: 2233-7857 IJFGCN

In [2], a model is proposed to defend or secure the data on cloud from illegal entry using SHA, AES procedure for encryption and finally LSB is used to embed the encrypted information in any type of image. This model is used to hide any data file in any picture types without converting.
In [3], a method is proposed to protect the secret pictures in cloud storage using Steganography methods. The proposed method not only enhances image safety but as well increases the cloud storing size.
In [4], for securing the data Mary and Dr, George have proposed the model using steganography along with Obfuscation. Obfuscation is the way to transform the data into the new form and steganography hides the presence of the data using LSB technique.
In [8], the cryptography and steganography techniques are used to secure the real time sharing of data on the cloud. Cryptography makes the data unreadable and steganography hides the presence of the data.

3. Theoretical Background for Proposed System:

In our system we will use AES technique to encrypt and decrypt the information to ensure data security. Once the data is encrypted, we will embed the data into cover image using LSB algorithm.

A. AES procedure/algorithm

The AES is a symmetric-key cryptographic technique implemented using a 128bit block area and key measurements of 128 bits, 192 bits and 256 bits. AES practices number of transformations rounds to convert the plaintext into the ciphertext. The figure/number of rounds of AES are determined by the length of key used.
Number of rounds are:
1. 128 bits key = 10 rounds
2. 192 bits key = 12 rounds
3. 256 bits key = 14 rounds

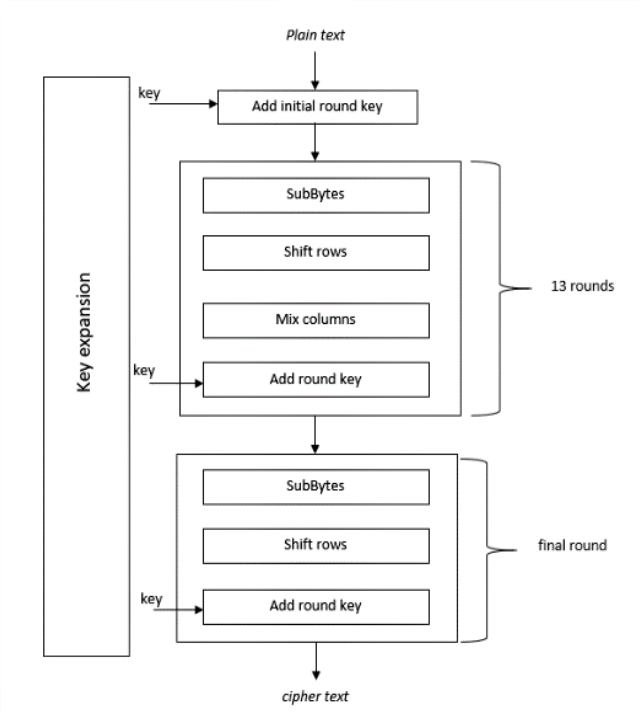

Figure 1. AES Encryption

ISSN: 2233-7857 IJFGCN

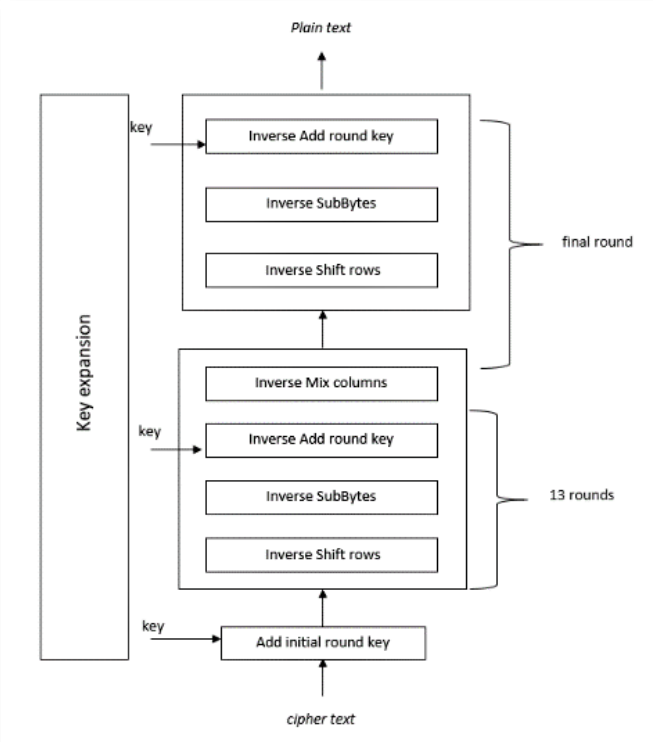

Figure 2. AES Decryption

SubBytes*:* It substitutes bytes using substitution matrix(S-box).

Shift Rows: Depending upon the index of rows, the contents in the rows are left shifted in circular way.

Mix columns*:* Each byte in the matrix-column is converted to a new value that relies on the value other 4 bytes in the same matrix-column.

Add Round Key*:* Normal XOR operation between recent state and round key.

B. LSB algorithm

The LSB algorithm is most widely used Image Steganography technique which pours or embeds the secret message into a cover picture or image. The binary of pixels of image are extracted and the confidential message (message to be hidden) is inserted in the Least Significant Bits (LSB) of the pixels as the LSBs are considered as the noise bits in the image.

Working of LSB:

If the message is 01000001, it can be embedded as:

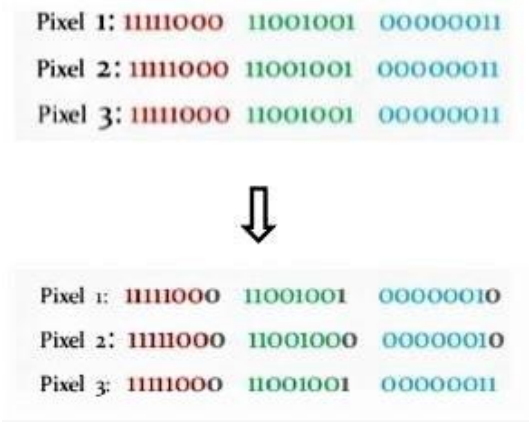

Figure 3. LSB Working

ISSN: 2233-7857 IJFGCN

In our system, we will use the proposed Image steganography method to embed the data.

4. Proposed System:

In this paper, we are presenting the model to secure the data while uploading on the cloud using combined cryptography and steganography techniques. The working of model in steps will be as followed:

For data hiding:

Step 1. Data Encryption

In this step, we will encrypt the data using AES-256 algorithm and pass this encrypted data to the embedding step.

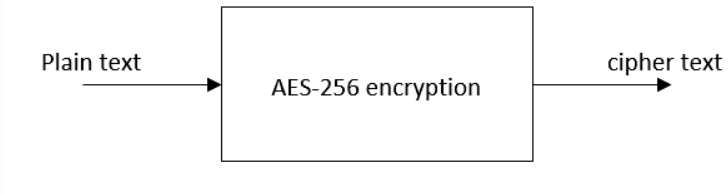

Figure 4. Data Decryption

Step 2. Image gridding and swapping

In this step, we will accept the cover image, convert the cover image into the grids and will swap these grids. We will pass this swapped gridded image to the embedding step.

Step 3. Embedding the data

In this step, now we have the encrypted data from step (1) and swapped gridded image from step (2). Now, we will embed the encrypted data in the swapped gridded image using LSB technique. And after embedding the data, we will swap back the grids to form the original image.

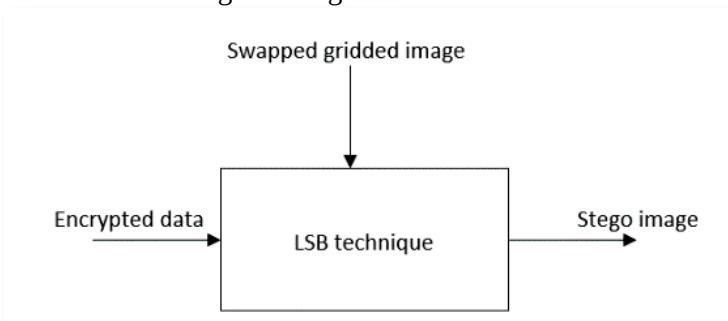

Figure 5. Embedding encrypted data into swapped gridded image.

Complete working of step (2) and step (3) together can be given as:

ISSN: 2233-7857 IJFGCN

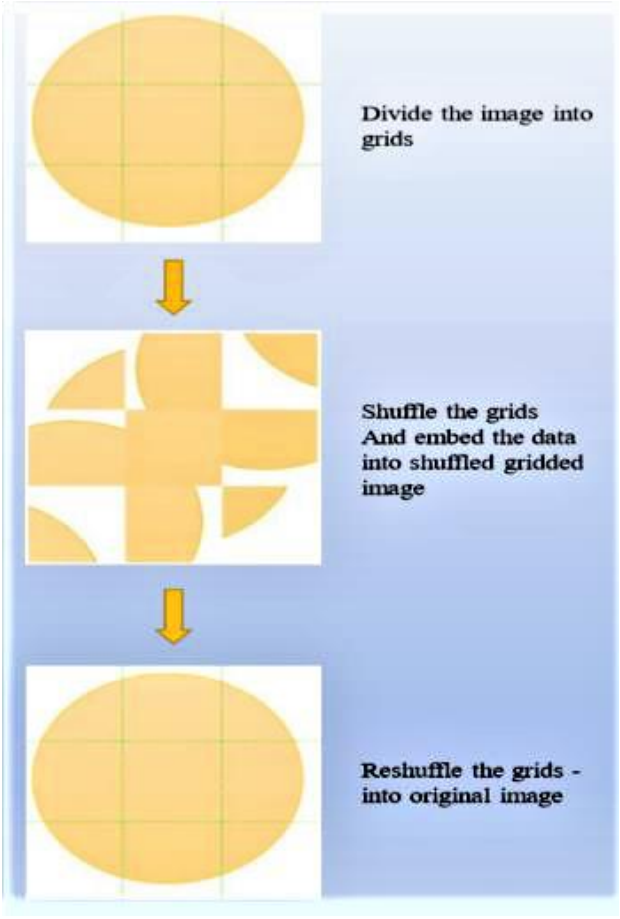

Figure 6. Combined working of step 2 and step 3

For data retrieval:

Step 1: Download the stored stego image from the cloud.

Step 2: Swap the grids of the stego image using same technique used while hiding the information.

Step 3: Retrieve the hidden information from the swapped gridded image using LSB technique.

5. Advantages and Limitations of Proposed Technique:

The advantages are: The proposed technique is providing the two layers of security to the data. The shuffling of the grids and then embedding the data makes it very difficult to hack. Even if any third person tries to access the data what he will get is only garbage.
The disadvantage of the system is if the stegnalyst gets to know the shuffling algorithm of the grids, the data can be accessed by him also cryptography followed by steganography increases the overhead.

ISSN: 2233-7857 IJFGCN

6. Conclusion

Proposed system provides two levels of security i.e. cryptography followed by steganography. Even if the presence of message is detected, the original message cannot be accessed without knowledge of the algorithm for shuffling grids.

References:

[1] Mr. Abhijeet Murali, Mr. Akshay Sangrolkar, "Steganography by scattering the cover image.", 2018.

[2] Surbhi Singla, Anju Bala, "A Review: Cryptography and Steganography Algorithm for Cloud Computing", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), 978-1-5386-1974-2/18/$31.00 ©2018 IEEE.

[3] Moshira A. Ibrahim, Islam A. M. El-Maddah, Hoda K. Mohamed, "Hybrid Model for Cloud Data Security using Steganography", IEEE, 978-1-5386-1191-3/17/$31.00, 2017 IEEE.

[4] Wen-Chuan Wu and Shang-Chian Yang, "Enhancing Image Security and Privacy in Cloud System Using Steganography", 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 978-1-5090-4017-9/17/$31.00 ©2017 IEEE.

[5] Dr.D.I. George Amalarethinam, B. Fathima Mary, "Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography", World Congress on Computing and Communication Technologies (WCCCT), Communication Technologies, 978-1-5090-5573-9/16 $31.00 © 2017 IEEE.

[6] R. Garg, "Various audio Steganography techniques for audio signals", International Journal of Engineering and Computer Science, 2016.

[7] Lejeune, J., Tunstall, Cara, Yang, Kuo Pao, & Alkadi, Ihssan. (2016). An algorithmic approach to improving cloud security: The MIST and Malachi algorithms. 2016 IEEE Aerospace Conference.

[8] Subhasish MandaI, Dr. Souvik Bhattacharyya, "Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA", 2015 International Conference on Green Computing and Internet of Things (ICGCloT), 978-1-4673-7910-6/15/$31.00 ©2015 IEEE.

[9] Vinay kumar pant, Jyoti Prakash, Amit Asthana, "Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques", 2015 International Conference on Green Computing and Internet of Things (ICGCloT), 978-1-4673-7910-6/15/$31.00 ©2015 IEEE.

[10] Hu S, KinTak U (2011) A novel video steganography based on nonuniform rectangular partition. In: IEEE 14th International Conference on Computational Science and Engineering (CSE) 57–61.

[11] Sherly AP, Amritha PP (2010) A compressed video steganography using TPVD. Int J Database Manag Syst 2(3). doi: 10.5121/ijdms.2010.23076.

ISSN: 2233-7857 IJFGCN