International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

E-mail Security using Advanced Cryptography and Steganography

V. M. Ashiq[1], K. Anoop[2]
[1]*Student, Department of Computer Science, IHRD College, Palakkad, India*
[2]*Software Engineer, Cabal Technologies, Calicut, India*

***Abstract*: Email is an important method of business communication that is fast, cheap, accessible and easily replicated. Using email can greatly benefit businesses as it provides efficient and effective ways to transmit all kinds of electronic data. In this paper, we propose a new way to make secure the emails by using an advanced encryption standard(AES) for cryptography and steganography. The Advanced Encryption Standard (AES) algorithm is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes. AES is largely considered impervious to all attacks. The Least-Significant-Bit (LSB) technique is a kind of substitution algorithm spatial domain algorithm which embeds data by substituting carefully chosen bits from the cover image pixels with secret message bits. This technique involves the modification of the LSB planes of the image.**

***Keywords*: Steganography, Cryptography, Advance encryption standard, LSB.**

1. Introduction

The proposed system provides the facility to hide data within the file, before the end of the file. This is efficient while transferring the image through the network. In this system, the data will be Steganographed using LSB method. The simplest approach to hiding data within an image file is called the least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye.

Any color pixel is made of a combination of RED-GREEN-BLUE (RGB) wherein each RGB components consists of 8 bits. If the letters in ASCII are to be represented within the color pixels, the rightmost digit, called the Least Significant Bit (LSB), can be altered. Any variation in the value of this bit leads to minimal variation in color. GIF and 8-bit BMP files employ what is known as lossless compression, a scheme that allows the software to exactly reconstruct the original image. JPEG, on the other hand, uses lossy compression, which means that the expanded image is very nearly the same as the original but not an exact duplicate.

If we have to hide word 'AIG' in the image, we take the LSB of every color and hide each bit of the word in its RGB Combination. To insert letter "A", we modify three color pixels with 3 bits in each color pixel For e.g The letter A can be hidden in three pixels. The binary value of A is 10000011. The original raster data of 3 pixels may be. (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001). After inserting the binary value for A. (00100111 11101000 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)

2. Modules

There are 2 main modules in this system. Those are

- Cryptography
- Steganography

A. Cryptography

The word cryptography has come from a Greek word, which means secret writing. In the present day context, it refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. For private communication through the public network, cryptography plays a very crucial role. The role of cryptography can be illustrated with the help of a simple model of cryptography as shown in Fig. 1. The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as ciphertext, which is received at the other end of the medium and decrypted to get back the original plaintext message. In this lesson, we shall discuss various cryptography algorithms, which can be divided into two broad categorize - Symmetric key cryptography and Public key cryptography.

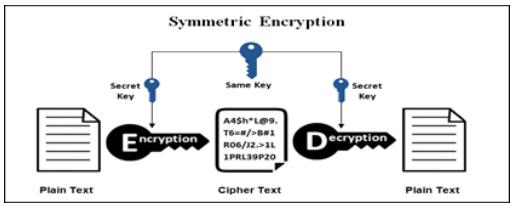

Fig. 1. Cryptography

B. AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for

secure and classified data encryption and decryption.In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies the application of the Rijndael algorithm to all sensitive classified data. The Advanced Encryption Standard was originally known as Rijndael

The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network.

In 1997, the NIST initiated a five-year algorithm development process to replace the DES and Triple DES. The NIST algorithm selection process facilitated open collaboration and communication and included a close review of 15 candidates. After an intense evaluation, the Rijndael design, created by two Belgian cryptographers, was the final choice.

The AES replaced the DES with new and updated features:

- Block encryption implementation
- 128-bit group encryption with 128, 192 and 256-bit key lengths
- Symmetric algorithm requiring only one encryption and decryption key
- Data security for 20-30 years
- Worldwide access
- No royalties
- Easy overall implementation
- How AES Works
- Like many other block ciphers, AES uses rounds of encryption that carry out the cipher transformations. Each round typically consists of several building blocks designed jointly to create a function, which is then run multiple times. The number of rounds AES performs depends on the length of its key. At 128 bits, it does 10 at 192 – 12, and at 256 – 14.
- Unlike its predecessor – the aforementioned DES – which can only encrypt about half of the data path in each round, AES is capable of encrypting the whole data path in one round.

Each round consists of four layers:

- *SubBytes provides excellent confusion* – "confusion," as it relates to AES, is a property of a secure cipher's operation. It makes the relationship between the ciphertext and the symmetric key as complex as possible. This creates non-linear tables, which are extremely good at eliminating patterns.
- *ShiftRows provides diffusion* – where "diffusion" is another property of the operation of a secure AES cipher. The goal here is to dissipate the statistical structure of plaintext over the ciphertext by spreading every part of the input to every part of the output.
- MixColumns provides further diffusion for added effectiveness.
- Add Round Key mixes the key, making it impossible for an attacker to calculate what the cipher does.
- Interestingly, the last round does not have a Mix Columns layer. This makes the encryption and decryption scheme symmetric.

C. Steganography

STEGANOGRAPHY comes from the Greek Words: STEGANOS – "Covered", GRAPHIE – "Writing". Generally, the sender writes an innocuous message and then conceals a secret message on the same piece of paper. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. The data can be hidden in basic formats like Audio, Video, Text, and Images, etc. The various types of steganography include:

- Image steganography
- Audio steganography
- Video Steganography

1) Least-Significant-Bit (LSB) Algorithm

The Least-Significant-Bit (LSB) technique is a kind of substitution algorithm spatial domain algorithm which embed data by substituting carefully chosen bits from the cover image pixels with secret message bits. This technique involves the modification of the LSB planes of the image. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise. Therefore altering them does not significantly affect the quality of the cover image. Variations of the LSB algorithms include one or more LSB bits to be changed to a bit of secret massage. The main aim is to provide security to confidential RGB images such as maps or sensitive signed documents. The basic principle of steganography is to hide the secret information in the cover object, which can be a digital medium such as image, audio or video file, to obtain a stego file that has secret information hidden in it. For example, for a 24-bit image, each of the red, green and blue color components of bit can be used, as each is represented by a byte. In other words, one can store 3 bits in each pixel An 800 × 600-pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data . A grid for 3 pixels of a 24-bit

image can be as represented as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows: (00101101 00011101 11011100)

(10100110 11000101 00001100)
(11010010 10101100 01100011)

In the above example, the number was set in the first 8 bytes

of the grid, only the 3 underlined bits need to be varied according to the implanted message. So, only half of the bits in an image will be modified to hide a secret message using the maximum cover size. For each primary color, there are 256 possible intensities. If we change the LSB of a pixel it results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With an appropriate image, we can even hide the message in the least as well as second to least significant bit irrespective of noticing the difference.

3. Implementation

It provides the facility to hide data within the file, before the end of the file. This is efficient while transferring the image through the network

There are two users in this

- System Admin
- Normal user

A. Admin

Admin is the superuser because they have all the controls of this system. They can block, delete a user based on complaints.

Normal user

User can send, receives emails. The special purpose of this system the user can send their mail with encryption. In this case, the receiver must decrypt the data with the encryption key.

B. Other modules are

In admin

- *Login:* Admin must login with their username and password for further actions. We cannot login with invalid username and password and also cannot use any blank username and password.
- *View all users:* Admin can view all the users with their status. Our default status is active when we register with this system
- *View all complaints:* Admin can view all the complaints. If the abused person object the complaint then the admin can see the response abused person
- *Block a person:* Admin can block a person based on the complaint. Also, they can unblock a person based on the response of blocked person and fake complaints

In normal user,

- Login: User must be login with their username and password for further actions. We cannot log in with invalid username and password and also cannot use any blank username and password. If a user is in a blocked state then they can't log in.
- Registration: If we are a new user then we must register with this site. In the register section, we must select a question and give an answer for security purpose. If we forget our password then this question will help us.
- Compose a mail: We can compose our mail in two ways.

1. *Compose a mail with encryption* :Main with encryption means we can encrypt our message with an encryption key and after we can hide it in an image. In this case, our message is more secure than the normal message. The encryption key and message will embed in that image as our requirements.
2. Normal composing: We can send a mail-in normal way. It means in this mailing the mail is less secure. We can send a message using this way when the message is less important.
3. *Inbox:* We can view all the messages we received in our inbox. We can get both secure and normal messages here. If we want to see our secure messages then click the content image and we are redirected to a new page. In that page, there is a textbox for entering our encryption key. After entering the correct encryption key the code will decrypt the message and we can view the message that hide in the image
4. *Sent mail:* User can view all sent emails here. Also, they can delete their emails. If we want to delete multiple emails then we can select using the checkbox and delete it.
5. Draft: If u compose a mail and cancel it then that mail will save in our draft section. We can see it there and resend it.
6. *Trash:* Our all deleted mail will be here. If we want to delete it permanently then we should delete the mail from trash.
7. *All mail:* We can view our all emails here. In this section, we can see the messages from sent, inbox, draft, etc.
8. Register complaint; If we want to register a complaint about a person or anything we can do it here. This will be sent to admin and admin will take an action based on our complaint. And otherwise, we will be blocked by the admin based on complaint then we can respond about that complaint
9. *Settings:* The user can set their own account. In this section, they can change their password. In password change, they must give their old password for user verification. They can deactivate their account using username and password. Also, they can update their all details except username and password in the section of update profile
10. *Profile change:* User can upload their new profile pic using file upload.
11. *Search a mail:* User can search the mail based on sender or receiver and content of the mail.

(a)

(b)

Fig. 2. (a) Original image (b) Image with hidden message

4. Conclusion

In this paper E-mail security using advanced cryptography and steganography is proposed. By using this method, we can hide any information within an image and extract them without much pain and there is no way to decrypt the embedded message without knowing the encryption key

This method provides an option to compress the output file. Thus the size of the output file can be set to that of the original file. So an outsider cannot find whether the image contains any data by checking the original file and encrypted file

References

[1] V. Lokeswara Reddy, A. Subramanyam, P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats," in Int. J. Advanced Networking and Applications, vol. 2, no. 5, pp-868-872, 2011.

[2] M. Rajkamal and B.S.E. Zoraida, "Image and Text Hiding using RSA & Blowfish Algo rithmswith Hash-Lsb Technique," International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.

[3] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bitColor Images," World Academy of Science Engineering, and Technology, 50, 2009.

[4] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, June/July 2005.

[5] Kharrazi, M., Sencar, H. T. and Memon, N. (2006), "Performance study of common image steganography and steganalysis techniques", Journal of Electronic Imaging, SPIE Proceedings Vol.5681.15(4), pp. 1-16.

[6] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption," International Journal of Database Management Systems, Vol.4, No. 6, December 2012.

[7] B. Xu, J. Wang and D. Peng, "Practical Protocol Steganography: Hiding Data in IP Header," *First Asia International Conference on Modelling & Simulation (AMS'07)*, Phuket, 2007, pp. 584-588.

[8] D. D. Dhobale, V. R. Ghorpade, B. S. Patil and S. B. Patil, "Steganography by hiding data in TCP/IP headers," *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, Chengdu, 2010, pp. V4-61-V4-65.

[9] D. K. Kamran Ahsan. "Practical Data Hiding in TCP/IP", Workshop on Multimedia Security at ACM Multimedia, 2002.

[10] Jain Ankit, "Steganography: A solution for data hiding."