Enhanced Password Securityusing Image Steganography and OpenSSL Base64 Encryption

Aravind Nair A[1], Vishnu K.S[2], Jebin C Varghese[3], Ajith G.S[4]

[1,2,3]PG Scholar, MCA Department, Amal Jyothi College of Engineering,Kanjirappally
[4]Asst. Professor, MCA Department, Amal Jyothi College of Engineering,Kanjirappally

Abstract:Image steganography algorithms can be combined with encryption techniques to provide enhanced data security. This papersuggests Least Significant Bit algorithm which is combined with OpenSSL Base64 encryption technique to provide two layer password security. The proposed method uses one of the three colours (RED, GREEN and BLUE) present inside an image pixel to hide data. This algorithm successfully hides the data with the LSB of BLUE colour pixel value present in an image with no remarkable changes in the resulting image.This method is an improved version of Least Significant Bit (LSB) method for hiding information in images.Before applying the Steganography technique,the secret message will be encrypted into cipher text using a random system generated key to ensure password protection.The proposed selective approach results in better data security and reliability.

Keywords-Cipher text,Image Steganography,LSB Image Steganography,OpenSSL Base64 encryption, Stego image

I.INTRODUCTION

Steganography is the conceptof storing data in a way which hides the existence of the data.In Steganography, the cover media such as text, audio, video, and image are used to hide data where the attackers don't have any idea about the original message that the media contain and the algorithm which is used to embed or extract it. Ciphering techniques are used widely for encryption and decryption of data. But sometimes data encryption itself does not seem to be secure enough. Thus a higher level ofinformation hiding scheme is required. This leads to the developmentof Steganography.

A digital image is made up of a collection of pixels. These pixels are placed horizontally row by row to display the image. The best knownSteganography method that works in the spatial domain is the LSB, which replaces the least significant bits of pixels selected to hide the data. This method has differentimplementation versions that enhances the algorithm in certain other aspects. In spatial domain scheme, the secret messages are embedded directly into the pixel values of the image.The most common and simplest Steganography method is the least significant bits (LSB) insertion method where the least significant bit of the pixels values are replaced by the message bits which is encrypted before embedding. In RGB images, all the three pixel values (Red, Green, and Blue) can be selected for storing data in their LSB. But the proposed idea selects only the blue colour pixel values which is least perceived by human eyes.

In Cryptography, the attacker is allowed to detect, intercept and modify messages without being able to violate certain rules or security regulations guaranteed by a cryptosystem. The main goal of steganography is to hide the existence of message from the intruder. We can hide as much data as possible based on the capacity of the media selected.Sometimessteganography will not cover the overall security of secret message. This arises the need for an additional security layer for the secret message. For this purpose OpenSSL Base64 encryption technique is used in the proposed algorithm that provides a secret key to enhance protection.The OpenSSL Base64 encryption is a symmetric-key cryptographic algorithm which make use of a private key for encryption and decryption process. This encryption includes AES-256 and SHA-512methods in its encryption process.

II.LITERATURE REVIEW

There are lots of techniques available to implement steganography on a variety of different electronic mediums.Md. Islam et.al [1] proposed a concept based on the LSB steganography using AES encryption. A secret key is used to encrypt the secret information before it is stored in the LSB image. This method checks for lighter and darker pixel areas in an image by checking the MSB of pixel values and stores information in either of them. Hence this algorithm does not efficiently utilise the storage space in an image.

Mr. Singh et.al [2] suggests simple LSB image steganography without any additional security. This method simply stores the data inside the image in a specified order. Hence this method cannot be used with sensitive or confidential data. This approach is less complex and requires less time and space compared to other methods.

Mrs. Kavitha et.al [3] proposed the idea of steganography using LSB substitution method with an additional authorisation mechanism at the time of data embedding and retrieval. So, it is not possible to damage the data by unauthorized personnel. The major limitation of the proposed method is that it is designed only for bit map images (.bmp). It accepts only bit map images as a carrier file, and the compression depends on the document size and carrier image size.

Mr. Sharma et.al [7] suggested a method for hiding an image inside another image using improved LSB substitution technique. Here the MSB pixel values of an image is extracted and then embedded into the LSB pixel values of another image (cover image). This hides the existence of an image. But the quality of the embedded image will be affected after retrieved from the stego image with a minor distortion.

III.PROBLEM DEFINITION

The main aim of the algorithm is to encrypt and hide the data or information over an image using least significant bit steganography algorithmand store the image at the server side. The image in which the secret message is embedded is called cover image and the image containing the secret message is stegoimage .

A. Solution to the problem

This method is developed for hiding the information in any image file. In this method, a stego image is generated from the cover file behind which the data is to be hidden after OpenSSL Base64 encryption. The proposed method should provide better security and reliability while accessing the data from the image. So the data encryption, decryption and steganography plays an important role in this paper.

B. Method Used (LSB Algorithm)

The “Encryption phase” uses two types of objects for encryption purpose. One is the secret key which is to be stored securely, and the other is a cover file such as image. In the encryption phase the data is encrypted using OpenSSL Base64 encryption algorithm and store the encrypted data into the image using Least Significant Bit algorithm (LSB) where the least significant bits of the cover image are swapped with the bits of the encrypted secret data.

In “Decryption phase”, the stego image in which the data is hidden is given as an input file. It uses the Least Significant bit algorithm (LSB) by which the encoded bits in the image areextracted and gives the output as a cipher text.The decryption phase uses the same secret key which was given for the encryption in order to prevent unauthorized data access.Then the secret key is applied to extract the original text from the encrypted text.

A.RGB Image Files

The RGB image has 24 bit values per pixel represent by (11111111, 11111111 and 11111111) for white colour and (00000000, 00000000 and 00000000) for black colourpixels. The RGB images are bettersuitable for the proposed idea because it uses 24 bit pixel representation that helps in hiding the secret information with a bit change in the image pixel which does not affect the image quality and make the message more secure. In this research paper the RGB images are selected as a media to hide the secret message.

B.Data hiding using LSB

LSB (Least Significant Bit) substitution is the process of altering the least significant bit pixels of the cover image. Both grey scale and monochrome images utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colour shades of grey. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed with respect to the bit of secret message. For 24 bit image, the pixel value of blue component from RGB (red, green and blue) is changed.

LSB is effective when using with BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a high resolution cover image to store information. LSB substitution is also possible for GIF formats, but the problem with the GIF image is that whenever the least significant bit is changed, the entirecolour palette will be changed. This problem can be avoided only by usingthe gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually which makes it very hard to detectthe data. For JPEG, the direct substitution of steganographic techniques is not applicable since it uses lossy compression. So LSB substitution is applied for embedding the data into JPEG images.

The basic steps in the LSB algorithm are as follows:

Step 1: Select a cover image of resolution M*N as input.

Step 2: Secret message to be hidden is converted into binary format.

Step 3: The binary values are embedded in the LSB of RGB pixel component ofthe image using bit replacement method.

Step 4: The corresponding stegoimage is stored at server.

IV.PROPOSED ALGORITHM

The proposed algorithm uses two layers of security to maintain the privacy, confidentiality and accuracy of the data. Fig.1 shows the flowchart for the overall encryption process of the system. Once the user register into the system, user have to provide a user id and password to hide.

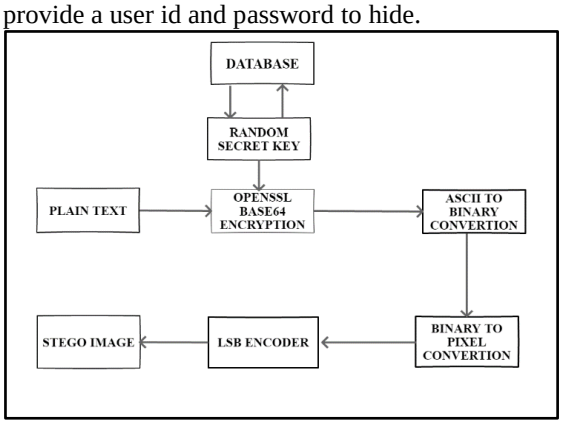

Figure 1*: Algorithm Flowchart (Encryption)*

First, the given password is encrypted using the OpenSSL Base64 encryption technique. Then a random secret key is generated for the corresponding user.After that the encrypted passwordis stored inside the chosen image with almost zero distortion of the original image. A secret key is required to decrypt the data retrieved from the image. Without the secret key, the actual data cannot be retrieved from the encrypted message stored inside the image. This is to ensure the integrity and confidentiality of the data. During the login process the corresponding password retrieved back from the stego imageis needed for authentication. The secret key is extracted from the database and passed to the decryption function.

V.METHODOLOGY

The proposed technique has two main parts:

- Changing the secret message (plain text) to cipher text using OpenSSL Base64 encryption technique.
- Hiding the cipher into image by the LSB Steganography technique.

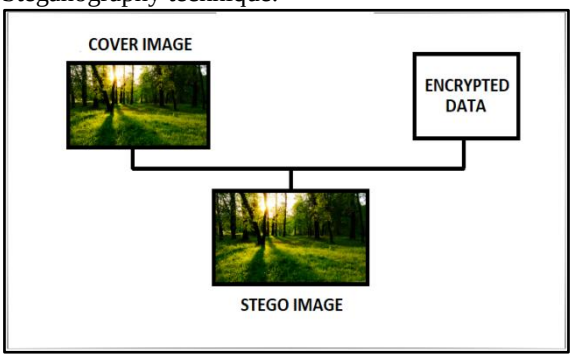

Figure 2*: Encryption Process*

For instance, suppose the data "AID" with the following property is to be stored in the first 8 pixels of 200 by 400 Pixels with 24 bits in a pixel that made up the image.

Letter	ASCII Values	Binary Values
A	65	01000001
I	73	01001001
D	68	01000100

Table 1: *Showing 3 letters with ASCII values and corresponding BINARY values*

Each pixel is represented as 3 bytes: one for Redcolour, one for Green colourand one for Bluecolour. The composition of these three colours determines the actual colourof that pixel.

Eg: Red-Binary: 11001010, Decimal: 202
Green-Binary: 11111001, Decimal: 249
Blue- Binary: 00000011, Decimal: 3

We can change the LSB of all Red, Green and Blue component if we want. Red is the most perceived colour whereas blue is the least perceived colour by human eyes. So blue colour is chosen in which no one suspects the existence of the message inside the image.

First, convert the secret message into corresponding cipher value. Suppose we want to hide the character 'a' in the cipher text using this method. Then get RGB value of each pixel in the image. Then convert the character 'a'into corresponding ASCII value (97) and then to its binary format (01100001). Since we are hiding 8 bit data, we need 8 pixels of the image.For the first 8 pixel values, we will replace last bit of each pixel's RGB value with the corresponding binary value of text consecutively.So, the new RGB value becomes:

- *11001100 10010001 00101010*
- *10010001 11110000 11111111*
- *00100101 11100010 01010101*
- *11100010 00001010 01000010*
- *11001100 11111101 00101010*
- *00011000 11110000 11111110*
- *00100101 11100010 01010100*
- *11111101 00001010 01000011*

The highlighted bit represents the message we are hiding in the image. We set the new RGB value to the pixel. This change is not detected by human eye and the image looks exactly the same.

VI.IMPLEMENTATION

Step1: Users register into the system by using password and it is encrypted using OpenSSL Base64 encryption techniquewith the help of randomly generated secret key.

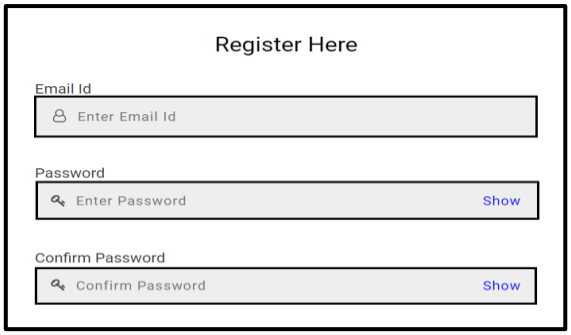

***Figure 3**: Registration Form*

Step2: The corresponding stego imageis created in the server and the encrypted password is stored in it.

***Figure 4**: Stego Image*

Step3: The random secret key encrypted using md5 and stored in database

User Id	Secret Key
aravind7850	ef6d150508fa4459a77f95c81f8c0068
vishnu7228	2814ec02ed7fdaa7ad3e4b2f5f6292f0
jebin7200	10392810aedfe7551d7871ed2547dec9

***Table 2:** Corresponding Secret Key stored in Database*

VII.RESULTS

The space and time complexity is higher than the existing LSB algorithm. The average computing time of the proposed method was found to be approximately 2.2 seconds. The size of the stego image is purely based on the resolution of the original image chosen for steganography and is independent of the size of secret message. So the space complexity can be reduced by using a low resolution image as cover image. Considering higher data security, the space and time complexities of this algorithm are negligible.

Cover Image	Username	Password	Secret Key (MD5 Encoded)
image.jpg	jebin7200	Hello123	10392810aedfe7551d7871ed2547dec9

***Table 3:** Values before OpenSSL Base64 Encryption*

Cipher Text	Stego Image
eBwbWXzwmyi1T0UhIfOx5nD8lJymjRpMgrwi7WMsxbw0AhcGbz+ZsEJeNv+lGPFsUEVnVriQi/0kkmiF9f5TVFblWa3JbjnED6OcnWNPPhKiWGNFloEizsE7uzllr1Tb	jebin7200.png

***Table 4:** Values after OpenSSL Base64 Encryption*

VIII.CONCLUSION

The use of steganography is considered to grow in importance as a data protection mechanism.We printed out the scopeofLSB image steganography system combined with OpenSSL Base64 encryption method to provide asecure means of information storage. Even if the person gets stego image he cannot retrieve the original data, without thesecretkey.Thus additional security is incorporated to the normal Steganography technique.Cover object has been divided into different colour regions from a particular true colourimage.In the processing of division of image into separate colourssuch as red, green and blue has been extracted from the particular imageto embed the secret data.This paper proposes a steganography algorithm with double layer security. A stego image has been created using the proposed algorithm. With the proposed algorithm, it is found that the quality of stego image does not have a noticeable distortion on it (as seen by the naked eyes). Hence this algorithm is very efficient to hide sensitivecontentwith the help of images. Stego image can be used by various users who want to hide the data inside the image without revealing the hidden data to other parties.Itmaintains proper privacy for sensitive data like passwords.Steganography is a useful mechanism which adds strength to mainstream cryptography .This method can be placed on the areas of copyright protection and privacy protection.A more sophisticated approach can be implemented by using a pseudo-random number generator to distribute the message over the image file in a random manner.The order in which RGB channels are selected to store data can be used as a key for the proposed method.Thisconcept can be extended by using other media files like audio, video and other complex formats of image.

REFERENCES

[1] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. DelowarHossain ”An Efficient Filtering Based Approach ImprovingLSB Image Steganography using Status Bit alongwith AES

Cryptography", **2014** International Conference on Informatics, Electronics & Vision (ICIEV),23-24 May 2014

[2] Amritpal Singh, Harpal Singh "An Improved LSBbased Image SteganographyTechnique for RGB Images", 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 5-7 March 2015

[3] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav,"Steganography Using Least Signicant Bit Algorithm", InternationalJournal of Engineering Research and Applications (UERA), Vol. 2,Issue 3, pp. 338-34 1, 2012

[4] ZaidoonKh. AL-Ani, A.A.Zaidan, B.B.Zaidan andHamdan.O.Alanazi,"Overview: Main Fundamentals for Steganography",JournalofComputing, Volume 2, Issue 3, March 2010, ISSN 2151-9617

[5] William Stallings, "Cryptography and NetworkSecurity: Principles and practices", Pearson education,Third Edition, ISBN 81-7808- 902-5

[6] Fridrich, Jessica, "Detecting LSB Steganographyin Colour and Grayscale Images", Magazine of IEEEMultimedia Special Issue on Security, Nov. 2001

[7] Vijay Kumar Sharma, Vishal Shrivastava, "A Steganography algorithm for hiding image in image by improved LSB substitution by minimize detection", Journal of Theoretical and Applied Information Technology, 15th February 2012. Vol. 36, 2005 - 2012 JATIT & LLS,E-ISSN: 18173195