Image Steganography combined with Cryptography

Dr.R.Sridevi, Vijaya Lakshmi Paruchuri, K.S.SadaSiva Rao
Professor, Dept of CSE, JNTUCEH, Hyderabad
sridevirangu@yahoo.com
Assistant Professor, CSE Dept, CBIT, Gandipet, Hyderabad
parchuri.vijaya@gmail.com
Associate Professor, Sri Indu PG College, Vanasthalipuram, Hyderabad
karrisrini@yahoo.co.in

ABSTRACT

Steganography is the science of invisible communication. Apart from the sender and intended recipient no one suspects the existence of the message. Using Steganography, information can be hidden in various mediums known as carriers. The carriers can be images, audio files, video files and text files. Image Steganography is a technique of using an image file as a carrier. Cryptography protects the information by applying the encryption and decryption techniques, so that the secret message can be understood only by the right person.

This paper proposes a method, which combines the techniques of Steganography and cryptography, to hide the secret data in an image. In the first phase, the sender will embed the secret data in an image by using the Least Significant Bit (LSB) technique. The embedded image will be encrypted by using an encryption algorithm. At final, the encrypted image will be decrypted and the hidden data will be retrieved by supplying the valid secret key by the receiver. The process includes the phases of Data embedding, Image Encryption and recovery of both original image and secret data from the encrypted image.

Indexing terms/Keywords

Steganography, Cryptography, cover image, stego image, Image encryption, Image decryption and Data recovery.

1. INTRODUCTION

Internet is one of the most important factors of communication and information technology, providing the security can be achieved through the techniques of Steganography and Cryptography. Steganography can be accomplished through hiding the secret information in any of the forms like image, audio or video files. The purpose of Steganography fails if the presence of hidden information is revealed or even suspected.

Cryptography is another technique for securing the secret information. Sender encrypts the message using the secret key and then sends it to the receiver [1]. The receiver decrypts the message to get the secret information. Cryptography focuses on keeping the content of the message secret where as Steganography concentrates on keeping the existence of the message secret. The strength of Steganography gets amplified if it combines with cryptography. The work proposed in this paper is the combination of both Steganography and cryptography. It shows how effectively the information can be transferred between two parties without security lapse.

The terminologies used in Steganography are cover-image, Stego-image, secret message, secret key and embedding algorithm. Cover-image is the carrier of the message such as image, video or audio file. Cover-image carrying the embedded secret data is the Stego-image. Secret message is the information that is to be hidden in a cover image. The secret key is used to embed the message depending on the hiding algorithm. The embedding algorithm is the way, which is used to embed the secret information in the cover image.

2. IMAGE STEGANOGRAPHY

Images are the most powerful file formats used in Steganography. Image Steganography is about exploiting the limited powers of Human Visual System (HVS) [2]. Any plain text, cipher text, other images can be embedded in a bit stream can be hidden in an image. To a computer, an image is a collection of numbers that constitutes the different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels.

Most of the images consists of a rectangular map of the image's pixels where each pixel is located and its colour.

These pixels are represented horizontally row by row. Number of bits in a colour scheme is called bit depth, refers to the number of bits used for each pixel. Monochrome and grayscale images use 8 bits for each pixel and are able to display 256 different colours of grey. Colour images are stored in 24-bit files and use the RGB colour model. All colour variations for the pixels of a 24-bit image are derived from three primary colours red, green and blue and each colour is represented by 8 bits.

Image Steganography technique can be divided into two groups. Image domain and Transform domain. Image domain technique embeds the message in the intensity of the pixels directly where as in the transform domain, images are first transformed and then the message is embedded in the image. Image domain techniques operate on bit-wise methods that apply bit insertion and noise manipulation methods. Image domain techniques are lossless and are dependent on the image format. Transform domain involves the manipulation of algorithms and image transforms. Transform domain methods are independent of the image format.

3. PROPOSED METHOD

In the proposed method, before the hiding process, the sender must select the image of size 512*512 and select the secret message as well as secret key. Secret data hidden into the cover image using the LSB embedding technique. Stego-image which contains the hidden secret data is encrypted using the AES (Advanced Encryption Standard) encryption algorithm. Then the sender may send the encrypted image to the receiver. Receiver applies the decryption algorithm to get the original image and supply the same secret key to retrieve the secret message.

In this paper, a specific secret-key image based data hiding model has been proposed which uses an image as the cover object and secret information is embedded into the cover image to form the stego image. Stego image is encrypted in the next step. From the encrypted image recovery of the original image and extraction of the secret data operations are performed. Proposed method is explained with the following figure

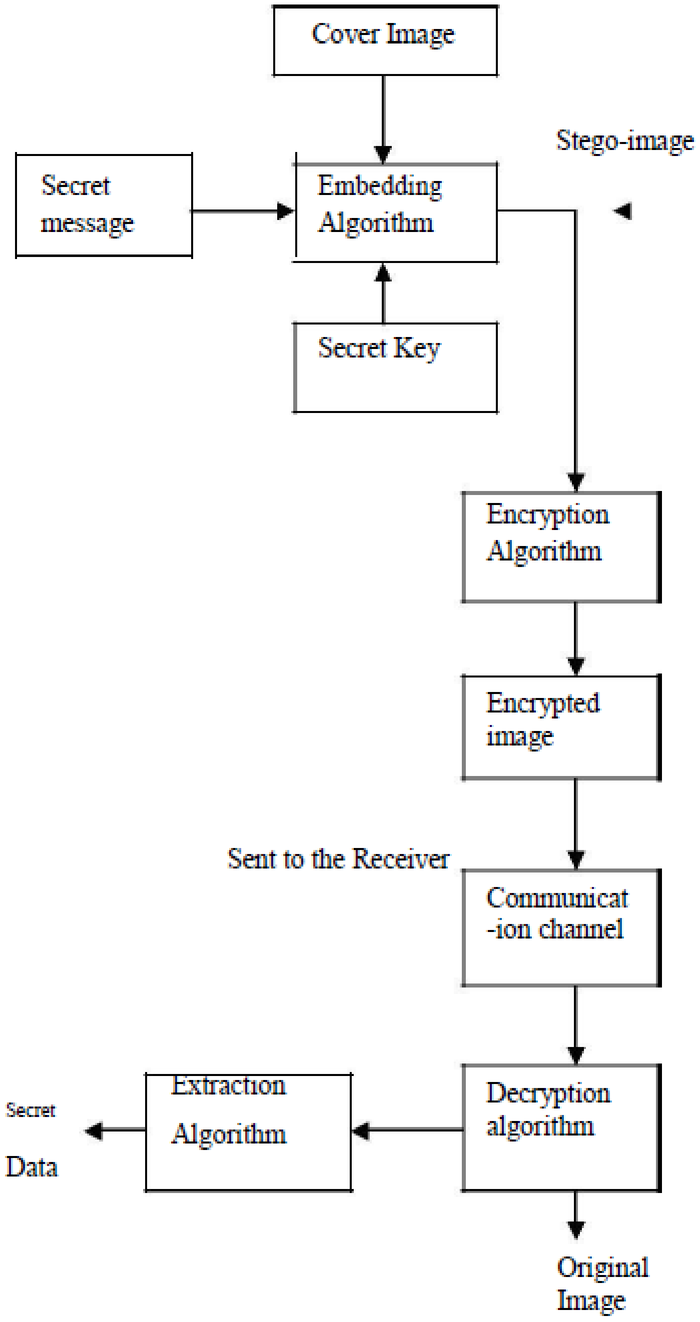


Fig.1. Process of image steganography with cryptography

4. IMPLEMENTATION

The work proposed in this paper was implemented by dividing into 3 modules.

1. Data Embedding
2. Image Encryption
3. Image Recovery and Data Extraction

4.1 Data Embedding

This module deals with the process of hiding the secret data into the cover image. The sender should be able to conceal the secret message in an image file without any visible alterations to the image. Least Significant Bit (LSB) technique is used to hide the secret data into an image [3].

In LSB technique, the embedding process consists of the sequential substitution of each least significant bit of the image pixel is replaced with the bit values of the secret message that is to be hidden.

When using the 24-bit image,a bit of each of the red,green and blue colour components can be used, since they are each represented by a byte. we can store 3 in each pixel. On an average, only half of the bits in an image will need to be modified to hide the secret message. Changing the LSB image steganography of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye. So message is successfully hidden.

4.1.1 Embedding Algorithm

Steps of embedding algorithm are given as follows.

Input: A 512x512 size cover image and data to be concealed.

Output: Stego image.

Step 1. Accept the cover-image file by specifying the path of the folder containing the image, name of the image to insert the data, file extension of the image and secret data that is to be hidden.

Step 2. Extract all the pixels in the cover image and store it in the pixel array. Extract all the characters in the secret message and convert into byte array.

Step 3. Calculate the length of the secret message that is going to be placed in a cover image.

Step 4. Retrieve the first byte of the image and perform the logical AND operation with oxfe to mask the LSB bit. After this operation LSB position of the first byte contains zero.

Step 5. Perform the logical OR operation with the secret data bits and cover image LSB bits, to place the secret data bit into LSB position.

Step 6. Offset 32 bit is used in this method, so the secret data inserted into 0 -bit, 32-bit, 64-bit and so on. Repeat the procedure until all the secret data bits are inserted into the cover image.

After performing the above steps Stego image is produced as an output.

4.2 Image Encryption

This module deals with the encryption of the stego image. Sender inserts the secret message into the cover image and the stego image is encrypted to provide the better security. At the receiver side, receiver applies the decryption algorithm to recover the original image and extraction algorithm to retrieve the hidden message. Advanced Encryption Standard (AES) is used for the encryption process.

4.2.1 AES Algorithm

The AES algorithm is a symmetric key block cipher with a block length of 128 bits and a support for key lengths of 128,192 and 256 bits.AES algorithms is a symmetric key algorithm which means the same key is used for both encryption and decryption. Cipher text produced by the AES algorithm [5] is same size as the plain text. AES is based on a design principle known as Substitution permutation network.

AES operates on 4x4 matrix of bytes termed as the State. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into final output cipher text. Each round consists of several processing steps including the one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plain text using the same encryption key.

AES algorithm has the following steps

1. Key Expansion: Round keys are derived from the cipher key.

2. Initial Round:

   (a). Add round key--each byte of the state is combined with the round key using bitwise XOR .

3. Rounds:

   (a). Substitute bytes--each byte is replaced with the another according to the lookup table.

   (b). Shift Rows--a Transposition step where each row of the state is shifted cyclically a certain number of steps.

   (c). Mix columns--a mixing operation which operates on the columns of the state, combining the four bytes in each column.

   (d). Add Round key

4. Final Round (no Mix columns)

(a). Substitute bytes

(b) Shift rows

(c) Add Round Key

4.2.2 Encryption Procedure

In the Proposed method, Encryption of the stego image is carried out in five intermediate levels. Stego image pixels are converted into bit streams and these bit values are distributed to five shares. This pixel value share is indicated with small image. No one can obtain the hidden information from a single share, hence it ensures the security.

Steps in implementing the encryption of the stego image are

Input: 512 x 512 bytes size Stego image (4096x4096 bits).

Output: Fully encrypted image.

Step 1. Accept the Stego image and extract the few pixels of the stego image as the first share. Here 512 bit position is used as the index, so get the pixel values of the 0 bit position ,512 bit,1024 bit and so on. Repeat the procedure until last index of the stego image. This pixel array represents the First share.

Step 2. To form the second share, extract the pixel values of 1-bit position, 513-bit(1+512) position, 1025-bit (513+512) position and so on from the stego image. The resultant pixel array represents the Second share.

Step 3. For the third share, retrieve the pixel values in 2-bit position,514-bit(2+512)position,1026-bit(514+512) and so on. These values represents the Third share.

Step 4. Fourth share is formed with bit position of 3-bit, 515-bit(3+512), 1027-bit and so on.

Step 5. Fifth share is the combination of bit values at bit positions 4-bit,516-bit,1028-bit and so on.

Step 6. Pixel values are the integers that ranging from 0(black) to 255(white). Reducing the intensities of the pixel leads to the conversion of the image colour. Colour pixel is converted into black by performing the operation (255-red | 255-green|255-blue).

Step 7. First image is the first share, convert these pixels into black by applying the method specified in Step 6.

Step 8. Mouse motion listener is defined such that, when we drag the mouse to the next image that share pixel values are converted into black.

Step 9. Repeat the procedure for all five shares, each step performs the partial encryption of the image. At final step AES algorithm is applied which produces the fully encrypted image.

After performing all the steps of above procedure, Output is the fully encrypted image which is more secure. This encrypted image is sent to the receiver. The Receiver performs the reverse operations to get the original image and produce the same key used by the sender, which is used in the embedding process, to get the secret information.

4.3 Image Recovery and Data Extraction

This module deals with the recovery of the original image and extraction of the secret data from the encrypted image.

4.3.1 Image Recovery

Image Recovery is done by the following steps.

Step 1: Accept the Encrypted image.

Step 2: Pixel values of the image are divided into five shares. Original image can be obtained by combining all these shares.

Step 3: In the encryption phase, all these shares pixel values are converted into black, by reducing the light intensities of the pixels. We should get back the intensities by performing the reverse operations.

Step 4: Cyan, Magenta, Yellow are the remaining colour intensities which forms the colour image other than red, green, blue colours. Conversion of black colour to RGB is performed by the operation

Rgb= (255- cyan) | (255-magenta) | (255- yellow)

Step 5: Perform the step 4 for each share to get the RGB values of the pixels.

Step 6: As the Mouse motion Listener is defined, drag the mouse by clicking share5,share 5 to share 4,share 4 to share 3, share 3 to share 2 finally share 2 to share 1.Original image is displayed as an output at the share1.

After performing the above steps, original image is produced from the encrypted image.

4.3.2 Data Extraction

After the image recovery next step is to extract the hidden data from the image. LSB technique is used as the embedding algorithm, we should extract the least significant bits from the image to get the secret information.

Steps in implementing the extraction process are

Step 1: Read the image which contains the secret data and convert into byte array.

Step 2: Now Start scanning the pixels from the first pixel and extract the key characters and place it in another array.

Step 3: If this extracted key matches with the key entered by the receiver then follow the step 4, otherwise terminate the program by specifying the message as entered key is invalid.

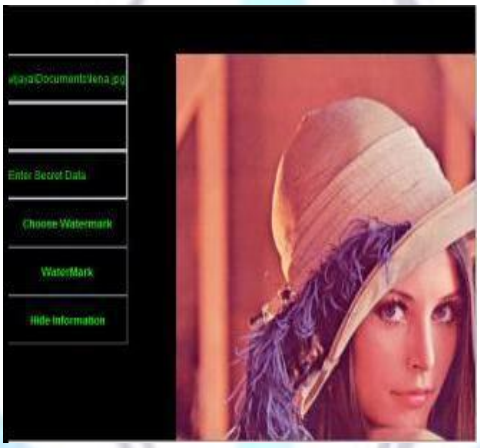
Step 4: If the key is valid, then again start scanning the LSB positions to extract the secret message bit values and place it in the character array. This process is continued until the length of the secret message.

Step 5: Extract the secret message from the character array.

5. EXPERIMENTAL RESULTS

In the proposed method, secret data can be hidden into the cover image and stego image is encrypted by the sender. Receiver performs the decryption operation to recover the original image and supplies the valid secret key to extract the hidden data.

Results of the proposed method are shown with the help of following figures.

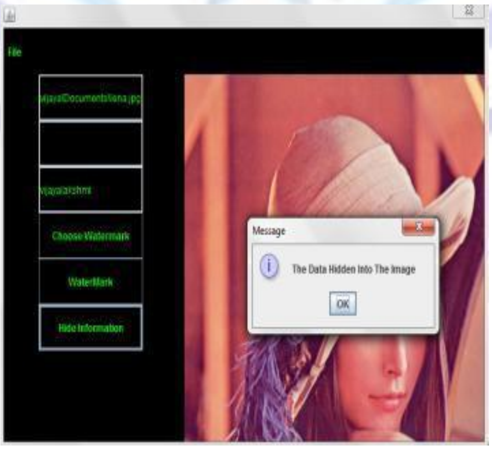


vijaya\Documents\lena.jpg

Enter Secret Data

Fig 1.Original image

ecret date embedded into the original image using the LSB technique. The resultant stego image is the following figure.



vijaya\Documents\lena.jpg

vijayalakshmi

Message

The Data Hidden Into The Image

Fig 2. Stego- image

Next step is the encryption of the stego-image. This encryption process carried out in five intermediate steps. Results of this operation are

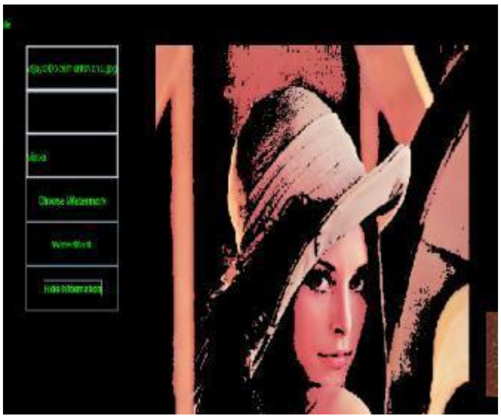


Fig 3. Encryption is in progress (share 2)

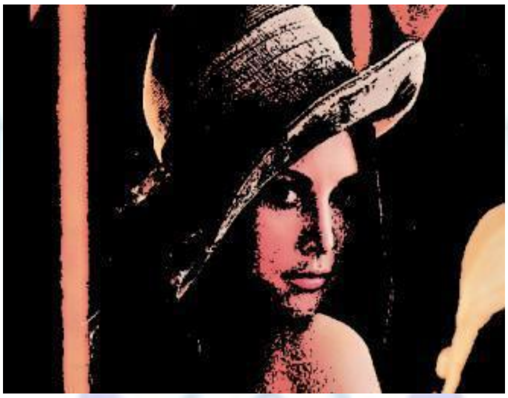


Fig 4. Encryption (share 3)

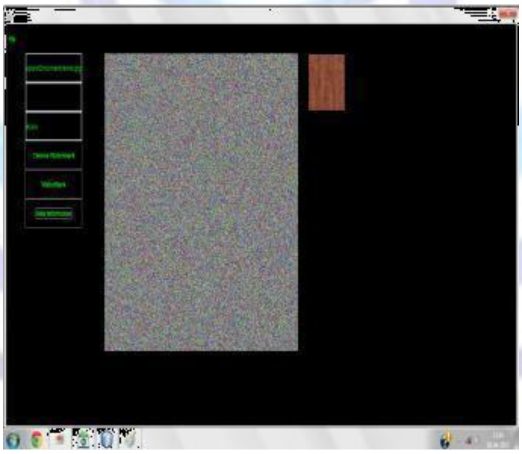


Fig 5. Fully Encrypted image

Encrypted image sent to the receiver. Image recovery process is shown with the following figures

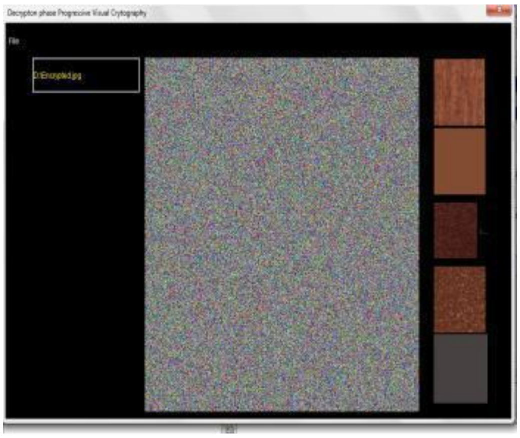


Fig 6. Image recovery is in progress(share 1)

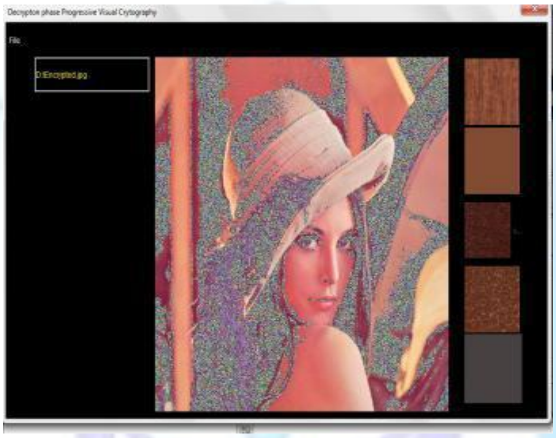


Fig 7. Image recovery in progress (share 3)

Extract the Secret information by entering the secret key.

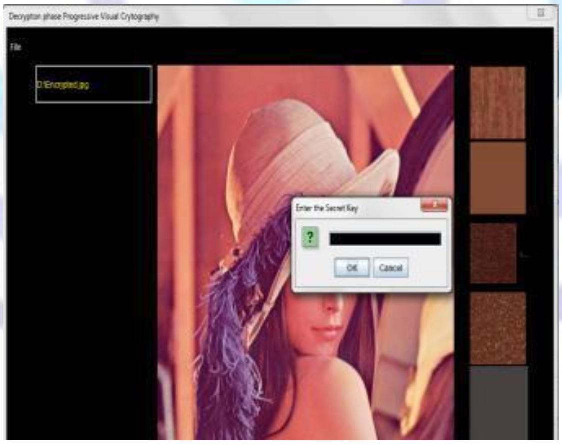
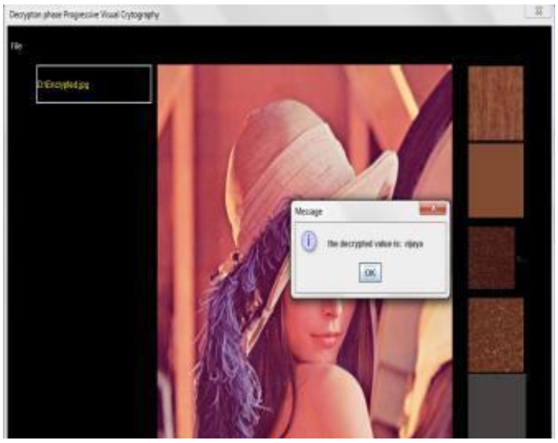


Fig 8. Enter the secret key



Decryption phase Progressive Visual Crytography

D:\Encrypted.jpg

Message

the decrypted value is: vijaya

Fig 9. Retrieval of secret message

6. CONCLUSION

In this paper, we proposed the combination of Image Steganography and cryptography has been achieved by using the LSB technique and AES algorithm. LSB technique is used to hide the secret data into an image and AES (Advanced Encryption standard) is used to encrypt the stego image. From the encrypted image, recovery of the original image and extraction of the hidden data operations are performed. Finally we conclude that the proposed technique is effective for secret communication and provides the better security. In future combination of image encryption and data hiding capable with lossy compression deserves the further investigation.

7. REFERENCES

[1] **S**eparable Reversible Data Hiding in Encrypted Image,Xinpeng Zhang,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[2] An Overview of Image Steganography, T.Morkel, J.H.P Eloff , M.S.Olivier, ICSA Research Group.

[3] A secure Robust Image Steganographic Model**,** Yeuan Kuen Lee and Ling-Hwei Chen .

[4] Image security using Steganography and Cryptographic Techniques. International Journal of Engineering Trends and and Technology-Volume 3Issue 3-2012.

[5] Novel Security Scheme for image Steganography using cryptographic Technique, Volume 2,Issue 4,April 2012.

[6] Steganography- A Data Hiding Technique, International Journal of Computer Applications ,Volume 9-No 7,Nov 2010.

[7] M. Kuribayashi and H. Tanaka, " Finger Printing Protocol for images based on additive homomorphic property "

IEEE Trans. Image Process., Vol 14, no 12, pp 2129-2139, Dec 2005.

[8] M.Deng,T.Biyanchi, A.Piva and B.Praneel, "An Effective buyer-seller watermarking protocol based on composite

Signal representation ", in Proc 11th ACM workshop Multi Media and Security 2009.

[9] S. Lian,. Z. Liu, Z. Ren, and H. Wang, commutative encryption and watermarking in video compression IEEE Trans. Circuits Syst.jun 2012.

[10] Image. Steganography concepts and practices, WSPC/ Lecture Notes Series 9 in x 6 in April 2004.