IMAGE SECURITY ENHANCEMENT BY A DUAL PROCESS WITH J-STEG AND RSA ALGORITHM

A.Suganya[1], Mrs. N. Senthamarai Selvi[2]

[1]B.E, [2]Ph.d., Computer Science and Engineering, IFET College of Engineering, Villupuram

ABSTRACT

Text and images can be provided security by the process of steganography, an art of hidden writing process. Many algorithms are implemented to hide the text and images. The proposed work is based on hiding the image inside two images as a two-step process. The two steganography algorithms, namely jsteg algorithm and RSA algorithm, are combined to enhance the level of protection for secret image. With the input image and secret image is used for concealing. Jsteg algorithm is used to connect the input image and the secret image is encrypted using RSAalgorithm. The output image of jsteg algorithm is concealed in the RSA encrypted image. Thus this method enhances the protection level in such a way that the image is concealed and it makes the communication to hide the existence of image from a third party. Thus more security, confidentiality and lesser detectability is obtained and limits the unauthorized access during image transmission.

Keywords: Transform Domain Technique, Jsteg, RSA, MSE, peak-signal-to-noise ratio (PSNR).

I. INTRODUCTION

Steganography is a science of hiding important information by embedding messages within other, seemingly harmless messages. Steganography is different and distinct from cryptography, there are many analogies between the two, and some authors classify steganography as a form of cryptography since hidden communication is a form of secret writing. Different message hiding techniques have been developed and implemented in the past using audio/video files, digital images, and other medias[1] the proposed work makes use of two algorithms to hide an image namely jsteg and RSA images.one is such technique is digital media where digital images are used as a medium for hiding information's in the form:text,didital image, video or audio file as secret message[2].The word steganography derived from two Greek words: stains means covered and graphs means writing and often refers to secret writing or data hiding[3].The major goal of steganography is to increase communication security by inserting secret message into the digital image, modifying the redundancy or nonessential pixels of the image[4],and is recently become important in a number of application areas especially military and intelligence agencies which require unobtrusive communications. If the presence of hidden information is suspected or even revealed, the purpose of steganography is partly defeated [5]. Data security or data privacy has become increasingly important as more and more systems are connected to the Internet. There are information privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, hiding the data in a kind of form such as within an image is vital in order to make sure that security or privacy of the important data is protected [6].

Thus, anumber of algorithms are used for steganography to hide the information in images. The proposed work is based on two algorithm namely jsteg and RSA to enhance the security of image transmission. These algorithms is an enhanced version of LSB technique that is not very much robust. Also a compression technique is used to increase the hiding capacity. Thus demonstrated using an application is built in matlab.

The rest of the paper is organized as follows. Section 2 described proposed algorithms and section 3 presents the proposed method. The implementation of the system is discussed in section 4 and section 5 together with the discussion of various results obtained from testing the system based on the proposed algorithm with various sizes of data. The image is also tested using the PSNR value. Finally, we conclude the paper in section 6.

II. JSTEG AND RSA ALGORITHMS

The first recorded uses of steganography is traced back to 440 BC when Herodotus mentions an example of steganography in the history of Herodotus.

Ancient example is that history of Herodotus who shaved his head of his most trusted slave and tattooed a message on it.After his hair had grown the message was hidden. The purpose was to instigate a revolt against the Persians. During the “cold war “period, US and USSR wanted to hide their sensors in the enemy facilities. These device has to send data to their nation, without being spotted.

IN the October 2001,new York times published an article claiming that Qaeda had used steganography to encode message into images, and the transported these via e-mail and possibly via USENET to prepare and execute the September 11,2001 terrorist attack[12].

A. JPEG (joint picture expert group)

Discrete cosine transformation is very famous steganography techniques which is best suited for JPEG images. JPEG images are widely used over the internet and have lossy nature of compression. DCT is extensively used for image and video compression. Every block of DCT is quantized with the help of quantization table of JPEG. Quantized coefficients are used to embed the secret message. Afterward coding methods are applied such as Huffman coding. In this technique high frequency regions are better for information hiding as they often become zero after the process of quantization. Hence it is not necessary to modify the coefficient value if the embedded data is zero. JSteg/ JPHide, F5, YASS (Yet another stenographic scheme) and Outguess are some of the DCT steganography tools [7]. **For the** execution of image compression in the coordination of JPEG, initial step is to convert the RGB color coordination into the coordination of YUV. In this coordination the Y component refers to matching the brightness of a pixel and the U and V components refer to the color of a pixel [8]. Currie, D.L. & Irvine, C.E. Illustrate that the human eye is very sensitive to changes in brightness of pixels more than the changes in color of pixels [9].Some samples are taken from the bottom of color data to reduce the file size when applying JPEG compression. The use of a factor 2 will reduce the size of the file, where the color components (U and V) are reduce by half in the horizontal and vertical directions [8].

Next step is to Discrete Cosine Transform (DCT) is used for the transformation of the image into JPEG, The DCT is a mathematical transform that converts a signal from coordination into frequency coordination, Through grouping the pixels into 8 × 8 pixel blocks and converting the pixel blocks into 64 DCT coefficients each. That's where all 64 pixel images in that block will be affected when any DCT coefficient is modified.

Final stage is the quantization of the compression. One form biological characteristics of the human eye can be exploited: that the human eye is rather good to distinguish between differences in brightness or (luminance) in low frequencies, but they are not good at distinguishing between differences in lighting or brightness in the high frequencies. This identify that the strength of high frequency shrunk, without any effect on the appearance of the image. To further reduce the file size, the result is rounded to the integer values and the coefficients are encoded by using Huffman coding [8].

B. JSteg

There are different variety of features using images in JPEG format, an image used in Steganographic applications. Initial step is the JPEG image file format has a large scale patronage and has become standard for storing and transmitting images on the network. When using this types of JPEG images in the process of concealing data, the attention of the attacker or anyone else on the resulting image is less than that with most other formats.

Second, some considerable controls are available on the quantized image. Finally, JPEG file provides the ability to hide a large amount of stenographic data messages. [10]. Derek Upham's JSteg was the first publicly available stenographic system for JPEG images [11].

JSteg algorithm replaces LSBs of quantized Discrete Courier Transform (DCT) coefficients. In this process the hiding mechanism skips all coefficients with the values of 0 or 1. This algorithm is resistant to visual attacks and offers an admirable capacity for stenographic messages [12] Generally, JSteg steganography algorithm embedded the messages in lossy compressed JPEG images. It has high capacity and had a compression ratio of 12%. JSteg algorithm is restricted for visual attacks and it is less immune for statistical attacks. Normally, JSteg embeds only in JPEG images. In these JPEG images, the content of the image is transformed into "frequency coefficients‟ so as to achieve storage ina very compressed format. There is no visual attack in the sense presented here, due to the influence of one steganographic bit up to 256 pixels [12].

C. RSA

RSA was invented by for Ron Rives, Adi Shamir and Leonard Adleman. It is the algorithm used for encrypting and decrypting messages. RSA is asymmetric key algorithm, hence using two different keys. One is private key: it is kept secret and other is public key: can be shared. Using these two keys the message is encrypted and decrypted [13].

The RSA algorithm could be used in combination with advanced LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure [14]. RSA algorithm procedure can be illustrated in brief as follows:

- Choose two large prime no. p & q.
- Calculate N=p*q.
- Calculate f(z)=(p-1)*(q-1)Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (z)) = 1.
- Calculate a number d such that d = e-1 mod f (n).
- Encryption: Enter message to get cipher text. Ciphertext c= mod ((message. ^e), N).
- Decryption: The cipher text is decrypted by Message=mod ((c. ^d), N) [15].

III. PROPOSED METHOD

In this work, two algorithms are combined, namely JSteg algorithm and RSA algorithm, to enhance the level of protection for the hidden images. Once the input image is choosen,the secret image is selected and encrypted using RSA algorithm. The input image is converted into a Jsteg converted image. This jsteg image is hided in the encrypted image. The tricky nature of hiding an already hidden image using two different algorithms introduces some complexity and makes it more deceptive to a third party, hence reducing the suspension of in the existence of a secret image and significantly enhancing the protection level.

IV. MODULES DESIGN

The proposed work is divided into the following steps:

- Image enhancement and Intensity calculation.
- Watermarking by J-steg.
- Embedding with RSA.
- Secret image and encryption.

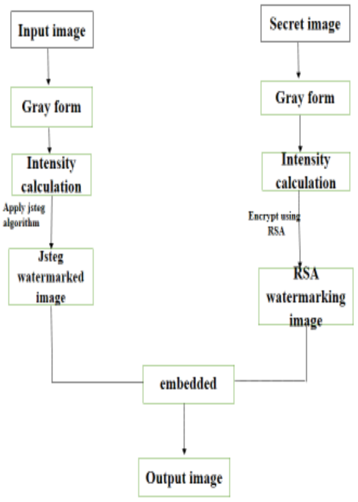

Figure 1. Describe module designs

A. Image enhancement and Intensity calculation:

Select the input image and secret image from file or any other directory. Convert into gray form for further processing. If not read the image, we can't go for further processing. Then initialize the cdf, pmf values for image enhancement. Calculate the intensity values for both input & enhanced images.

B. Watermarking by J-steg

The enhanced input image is watermark with the jsteg algorithm.

C. Embedding Algorithm

Image is encrypted with RSA algorithm and the resultant image is watermarked.

D. Embedding the images

The jsteg watermarked input images is embedded with the RSA watermarked secret image. The resultant image is an watermarked image where a third party cannot reveal what it is.

V. JSTEG AND RSA PROCESS

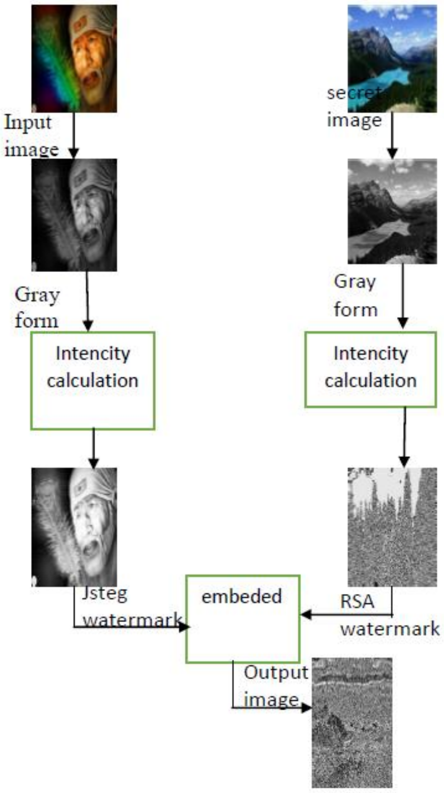

Figure 2. Describe jsteg & RSA process

Cover image1, cover image2, secret image1, secret image2

Step1: read cover image1. JPEG

a) JPEG partitions a cover image1 into non overlapping blocks of 8*8 pixels.

b) Calculate DCT coefficient for each block

c) Quantize the coefficients

Step2: hiding process by using JSteg algorithm while left to embed do

a) Get next DCT coefficients from cover image1.

b) If DCT ≠0, DCT ≠1 & DCT ≠ -1 then.

c) Get LSB from the message.

d) Replace DCT LSB with message bit.

End (if)

End (while)

Step3: calculate message capacity

Step 4: Write JPEG image by de-quantize and take inverse DCT to obtain stego image1 Secret image2= stego image1.

Step5: Read cover image2.JPEG.

a) JPEG partitions a cover image2 into non overlapping blocks of 8*8 pixels.

b) Calculate DCT coefficient for each block C. Quantize the coefficients.

Step6: hiding process by using RSA image algorithm While left to embed do.

a) Get pseudo random DCT coefficient from cover image2.

b) If DCT ≠0, DCT ≠1 & DCT ≠ -1 then.

c) Get LSB from the message.

d) Replace DCT LSB with message bit End (if) End (while).

Step7: calculate message capacity.

Step8: Write JPEG image by de-quantize and take inverse DCT to obtain stego image2.

The algorithm was implementation on Matlab 7.6 platform the results are shown in Figure (2) .And from the result it be seen can see that the proposed approach successfully combined two steganographic methods in frequency domain, where an intended secret image (hidden image1) is first hidden using JSteg algorithm and the resultant image is again hidden in another image using RSA image

A. Extraction algorithm

Input: Stego image2 Step1: read Stego image2.JPEG

a) JPEG partitions Stego image2 into non overlapping blocks of 8*8 pixels.

b) Calculate DCT coefficient for each block C. Quantize the coefficients.

d) Calculate message capacity.

Step3: Extracting process by using RSA algorithm while left to embed do.

a) Get pseudo random DCT coefficient from Stego image2.

b) If DCT ≠0, DCT ≠1 & DCT ≠ -1 then.

c) Get LSB from the message.

d) Replace DCT LSB with message bit.

End (if)

End (while)

Step4: Writ JPEG image by de-quantize and take inverse DCT to obtain secret image2. Stego image1= Secret image2.

Step5: Read Stego image1.JPEG.

a) JPEG partitions Stego image1 into non overlapping blocks of 8*8 pixels.

b) Calculate DCT coefficient for each block.

c) Quantize the coefficients.

d) Calculate message capacity.

Step6: Extracting process by using JSteg algorithm while left to embed do.

a) Get next DCT coefficients from Stego image1.

b) If DCT ≠0, DCT ≠1 & DCT ≠ -1 then.

c) Concatenate DCT LSB to secret message End (if) End (while).

Step7: Write JPEG image by de-quantize and take inverse DCT to obtain secret image1.

After the implementation of this algorithm in Matlab 7.6 program the results obtained are shown in Figure (3):

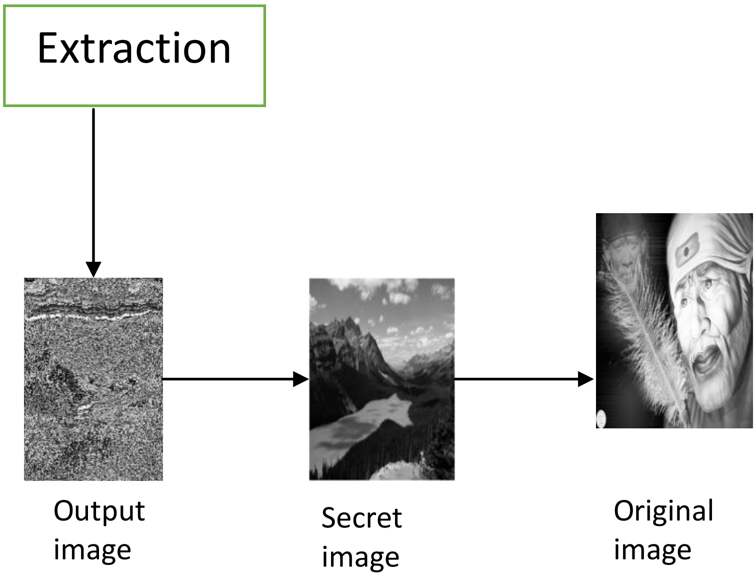

Figure 3. Decoding process

VI. EXPERIMENTAL AND RESULTS

The experiments were implemented on a set of images .Fundamental information hiding systems: capacity, security, and durability. The capacity is the amount of image that is possible to be hidden in a cover medium. Security refers to the inability of the attacker to detect hidden data. Robustness refers to the extent to which the stego medium can withstand the attacker, which can destroy the hidden information.

A. Embedding Capacity

It is the maximum size of the secret image that can be embedded in the cover image without deteriorating the integrity of the cover image. It can be represented in bytes or Bit Per Pixel (bpp), The calculated explain in equation 1.

Capacity =(X*Y)/64 * b *(n − 15) (1)

In this equation, X and Y are the dimensions of the cover image. By dividing the product of X, Y by 64, the number of 8*8 blocks is achieved. During data embedding process, no data are embedded in the last 15 coefficients, so the term (n-15) is used here, and in each coefficient b bits of data will be embedded.

B. Peak-signal-to-noise ratio (PSNR)

As a performance measurement for image distortion, the well-known peak-signal-to-noise ratio (PSNR) which is classified under the difference distortion metrics is applied to the stegoimages. It is defined as Eq (2):

PSNR= 10log(c2 max/MSE) (2)

Where MSE denotes mean square error which is given as Eq (3):

$$MSE=1/MN \sum_{x=1}^{M} \sum_{y=1}^{M} (sxy-(xy)2 \quad (3)$$

Table (1) illustrates the capacity and PSNR for the encoding process (1).

Table1.Capacity and PSNR for images

Image type	***PSNR value***	***MSE value***
Jsteg watermark image	63.9334	0.0263
RSA watermark image	65.25761	0.0493
Output image	61.2032	0.0194

Where x and y are the image coordinates, M and N are the dimensions of the image, Sxy is the generated stego-image and Cxy is the cover image. Also c2max holds the maximum value in the image, for example:

c2max <{1   double precision
c2max<{255   unit 8bit

Many authors, consider Cmax=255 as a default value for 8 bit images. It can be the case, for instance, that the examined image has only up to 253 or fewer presentations of gray colors. Knowing that C2max results in a severe change to the PSNR value. This Cmax can be defined as the actual maximum value rather than the largest possible value. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40 dB and above. In this paper, after combining two concealment algorithms specifically JSteg and RSA algorithm. We use the RSA algorithm to further enhance the level of protection for detection of a secret message (image), which has already been hidden inside another image using a Jsteg algorithm. And as such, the tricky nature of hiding an already hidden image is using two different algorithms introduces some complexity and makes it more deceptive to a third parties.This in effect reduces the suspension in the existence of the secret image, thereby significantly enhancing the image protection level .

VII. CONCLUTION

This paper presented a steganographic approach that combined jsteg and RSA algorithms. The approach allowed us to benefit from the potential features and strengths of both algorithms and this added a significant level of protection to hidden images. In principle what happened in our proposed approach is that an input image and secret image is used for concealing. Jsteg algorithm is used to connect the input image and the secret image is encrypted using RSA algorithm. The output image of jsteg algorithm is concealed in te RSA encrypted image. The act of hiding an already hidden image (stego image) in another image alone is tricky and deceptive for a third party. Besides that, the idea of combining two steganographic algorithm makes the approach more complex for a third party and this increases the chances that the intended secret massage (secret image) could go unnoticed.

Furthermore, the priority given to selecting a good image sizes and type further disguises the secret image and makes it more difficult for a third party to suspect the existence of a secret image. The experimental results indicated an average PSNR value of more than 50 dB for more than100 images and that is a good and acceptable steganography scheme. As future work, we could try the combination of other steganography techniques and compare the efficiency levels, as well as adding image encryption.

REFERENCE

[1] R.Rejani, D.Murugan and Deepu V. Krishnan3 “pixel pattern based steganography on images” ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, VOLUME: 05, ISSUE: 03,FEBRUARY 2015.

[2] DeepeshRawat, VijayaBhandari “steganography technique for hiding information in color image using improved LSB method”International Journal of Computer Applications (0975 – 8887) Volume 67– No.1, April 2013.

[3] Moerland.TJ.R. Krenn“steganography and steganalysis”Leiden institute of advanced computingscience,January 2004.

[4] Feng,J.B,lin “reversiblewatermarking current status and key issues”.International journal of network security2,April2006.

[5] Wang,H&wang, “cylerwarefare steganographyand steganalysis”communications of the ACM:October 2004.

[6] RosziatiIbrahim and Teoh Suk Kuan “steganography algorithm to hide secret message inside an image”, Computer technology and applicationfeb 25(2011).

[7] C. Vanmathi, S. Prabu “state of the art review on steganography techniques”International journal of signal processing 2015.

[8] Y.shi, D.zou, &g.xuan. “JPEG steg using empirical transition matrix in block DCT domain”, IEEE:8th workshop on multimedia signal processing 2006.

[9] Curril, D.L&Irvine,C.E, “surmounting the effects of lossy compression on steganography”, in 19th national information system security conference,1996.

[10] Tao zhang & xijian pin “A fast and effective steganalytic technique against jsteg_like algo”SAC 2003.

[11] Niels porous and peter honey man “hide and seek: an introduction to steganography”IEEE computer society, May 2003.

[12] Mani koduri.infomation “security through image steganography using least significant bit algorithm”feb14,2011.

[13] Jatinder kaur,ira gabba, “steganography using RSA algorithm” international journal oh innovative technology and exploring engineering ISSN:2278-3075,volume-3,issue-3,august 2013.

[14] Anil kumar,rohini Sharma “A secure image steganography based on RSA algorithm and hash LSB technique”. International journal of advanced research in computer science and software engineering issue 7, july 2013.