Color Image Steganography with Double Encryption

Bowsiya Begum M [*], Selvamary D

Department of Electronics and Communication Engineering, Oxford Engineering College, Trichy, Tamil Nadu, India

Article Info

Article history:
Received 4 February 2015
Received in revised form
20 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords
Cryptography,
Steganography,
OPAP,
RSA

Abstract

Cryptography is the science of using mathematics to encrypt and decrypt data and Steganography is the art of hiding data behind cover data. Combination of cryptography and steganography provides enhancement in data security i.e, forms a new security system. In this paper we have used double encryption using RSA algorithm and OPAP method is used for steganography this sort of encryption and stego-processing results in highly secured data transmission .the comparison between original & stegno-encrypted image is also done by using the image quality metrices such as MSE & PSNR.

1. Introduction

Steganography is the art of hiding a file, message, image, or video within another file, message, image, or video. Steganography combines the Ancient Greek words steganos (στεγανός), meaning is covered, and graphein (γράφειν) meaning is writing. Steganography literally means covered writing.

1.1. Steganography

Steganography's primary goal is to hide data within some other data such that the hidden data cannot be detected even if it is being sought. Secondary goal is prevent extraction from the cover file without destroying the cover& prevent destruction of the stego-message without destroying the cover .Most frequently, steganography is applied to images, but many other data or file types are possible such as audio, video, text, executable programs.

1.2. Cryptography

Cryptography is the art of protecting information by *encrypting* it into an illegible format, called cipher text. Only those who possess a secret *key* can *decrypt* the message into text. Cryptography systems can be classified into symmetric-key systems that use a single key that both the sender and recipient have, &*public-key*systems that use two keys, a public key known to everyone & a private key that only the recipient of messages uses. Shortly, one can say that cryptography is about securing the content of messages, steganography is about hiding its very existence.

1.3. Steganography Vs cryptography

*Ste*ganography methods usually no need to provide strong security against removing or modification of the hidden message. Watermarking methods are need to to be very robust to attempts to remove or modify a hidden message. The advantage of steganography is that messages do not attract attention to themselves. Plainly visible encrypted messages-no matter how unbreakable-will arouse suspicion, and may in themselves be implicate in countries where encryption is illicit. Therefore, whereas cryptography preserve the contents of a message, steganography can be said to protect both messages and communicating parties. Cryptography is a method of scrambling information by rearrangement and interchange of content, making it unreadable to anyone except the person capable of unscrambling it. Steganography is useful for hiding messages for transmission.

Steganography detection can be used to prevent communication of malicious data. Modern cryptography concerns itself with the following objectives:

- *Confidentiality* (the information cannot be understood by anyone for whom it was unintended)
- *Integrity* (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected).

To enhance the image qualities of the stego-images, optimal pixel adjustment process (OPAP) is used. It also minimizes the embedding error. OPAP reduces the distortion caused by the LSB substitution method.

2. Existing System

LSB Substitution Technique of steganography embeds the message bits directly into the least-significant bit plane of the cover image. The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (a) 24 bit images and (b) 8 bit images. In 24 bit images we can embed3 bits of data in each pixel, one in each LSB position of the 3 eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, 1 bit of data can be hidden. A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. Advantage of LSB Substitution is Simplicity, popularity, Easy to understand, Low degradation in the image quality Disadvantage of LSB Substitution is Attacker can easily destruct the message by removing the entire LSB plane, Scaling, rotation, cropping, addition of noise, to the stego image will destroy the message, The message size must be smaller than the image, Low robustness to malicious attacks, Vulnerable to environmental noise.

Corresponding Author,
E-mail address: bowstar.m@gmail.com;

3. Proposed System

In the proposed system, we have combined steganography & cryptography .double encryption is followed for increased security. Here OPAP algorithm is used for Steganography & RSA algorithm is used with double encryption.

3.1 Embedding procedure of Optimal Pixel Adjustment Process

Step 1: In the embedding process of a secret data, a cover image is partitioned into non-overlapping blocks of 2 consecutive pixels.
Step 2: A difference value (d) is calculated from these values of the 2 pixels in each block.
Step 3: All possible difference values are classified into a number of ranges.
Step 4: The calculated d value then replaced by a new value to embed the value of a sub-stream of the secret message.
Step 5: The number of bits which can be embedded in a pixel pair is decided by the width of the range that the difference value belongs to which gray scale range.
Step 6: Assume the gray value (g) of the pixel is in binary forms.
Step 7: Consider value [K] and bits to be inserted on cover image.
Step 8: Now take the gray value **g'** of pixel and check it is in the range or outside therange.
Step 9: After embedding the K-bits of message into the gray value **g** of pixel and new gray value **g'** may go outside the range.
Step 10: To make within the range, K+1 bits of **g'** are changed from 0 to 1 or vice-versa.
Step 11: This process is repeated until **g'** value falls within the range.

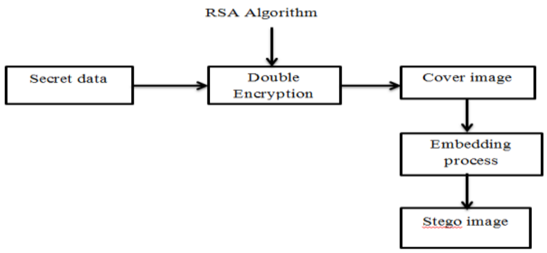

Fig 1: Embedding process

4. Result and Discussion

The simulation procedure is as follows: We selected BMP colourimages as cover image and secret data in text format. By using RSA public key cryptographic algorithm we are performing double encryption on secret data. In embedding process, the cipher text bits obtained from RSA Algorithm are embedded by using OPAP Algorithm. Then the stego image is obtained

.

Fig: 2(a). China wall

Fig: 2 (b). IPod

Fig: 2(c). Ice Age

Fig: 2(d). Spiderman

Peak signal-to-noise ratio (PSNR), Mean square error (MSE) are image quality parameters used to measure the quality of stego image then it is compared to the original image.Mean Square Error (MSE), is computed by averaging the squared intensity of the input image and the output image pixels as in (1).

$$MSE=\frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} e(m,n)^2 \qquad (1)$$

Where e(m, n) is the error difference between the original and the stego images.Peak Signal-to-Noise Ratio (PSNR), Signal–to-noise ratio (SNR) is a mathematical measure of image quality based on the pixel difference between two images PSNR is defined as in (2)

$$PSNR=10\log_{10}\frac{s2}{MSE} \qquad (2)$$

Where s = 255 for an 8-bit image. In receiver end the cipher data is converted back to original secret data by using RSA algorithm and we can extract the secret data from cover image using inverse OPAP algorithm

Table: 1. Evaluation Metrics using Opap Data Hiding Method

Cover image	**Size of Secret Data**	**MSE**	**PSNR**
China wall	1KB	0.32	53.0
Ipod	10KB	34.85	32.7
Ice Age	100KB	34.83	32.71
Spiderman	200KB	7.41	39.42

5. Conclusion

The idea of using steganography &cryptography together is to provide high security & robustness to the original image .we have encrypted the original image before stegno-processing to increase withstanding capacity of the cover image .Data hiding is then done and the resultant is also encrypted to provide additional security to data transmission. Thus our objective of developing a new security system fulfilled. This work can be extended with highly secure encryption algorithms for other stegnographic techniques in the future.

References

[1] Masoud Afrakhteh, Subariah Ibrahim Adaptive steganography scheme Using More Surrounding Pixels, International Conference On Computer Design and Applications (ICCDA 2010), 1, V1225-V1229

[2] Wu. Tsai, A steganographic method for images by pixel-value differencing, 24(9-10), 2003, 1613-1626

[3] A. E. Mustafa, A. M. F. ElGamal, M. E. ElAlmi, Ahmed. B D, A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit, 21, 2011

[4] H. C. Wu, Tsai, Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, IEE Procvis. Image signal process, 152(5), 2005, 611-615

[5] Chi-Kwong Chan, L. M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition Society. Published by Elsevier Ltd. All rights reserved.doi:10.1016/j.patcog.2003.08.007.

[6] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, A Comparative Analysis of Image Steganography, International Journal of Computer Applications (0975 – 8887), 2(3), 2010

[7] Chung - Ming Wang, Nan-I Wu, Chwei - Shyong Tsai, Min-Shiang Hwang, A high quality steganographic method with pixel-value differencing and modulus

[8] A. L. Khade. B. G. Hogde, V B Gaikwad, Secret Communication via Image Hiding In Image by Pixel Value Differencing, ICWET, 2010, 437-438

[9] M. Padmaa, Y. Venkataramani, ZIG-ZAG PVD – A Nontraditional Approach, International Journal of Computer Applications (0975 –8887),5(7), 2010

[10] J. K. Mandal 1, Debashis Das, Steganography using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow, The second International Conference on Computer Science, engineering and applications (CCSEA-2012), 2012

[11] J. K. Mandal, Debashis Das, Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain, International Journal of Information Sciences and Techniques (IJIST), 2(4), 2012, 83-93139

[12] Rajyaguru, M. H., Combination of Cryptography and Steganography With Rapidly Changing Keys, International Journal of Emerging Technology and Advanced Engineering, 2(10), 2012, 329-332.

[13] Manoj, I. V. S., Cryptography and Steganography. International Journal of Computer Applications (0975–8887), 1(12), 2010, 63-68

[14] Proposed System for Data Hiding Using Cryptography And Setganography International Journal of Computer Applications (0975 – 8887), 8(9), 2010

[15] N. Hopper, L. von Ahn, J. Langford, Provably Secure Steganography, Computers, IEEE Transactions on, 58(5), 662-676, 2009

.