An Efficient technique in Cryptography based on RGB Color Preserving method

Anchal.A [1], Dr. S. A. Ladhake [2]
[1](Dept. of CSE, Sipna College of Engineering & Technology, Amravati, India)
[2](Professor, Dept. of CSE, Sipna College of Engineering & Technology, Amravati, India)

Abstract— *To maintaining the secrecy and confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves hiding the data using data hiding algorithm to maintain the images secrecy.A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key.*

Keywords— Cover image, data hiding, data extraction, Image encryption, Image decryption, Data recovery.

1. Introduction

Cryptography is a technique for securing the secret information. Sender encrypts the message using the secret key and then sends it to the receiver. The receiver decrypts the message to get the secret information. Cryptography focuses on keeping the content of the message secret where as data hiding concentrates on keeping the existence of the message secret [1]. Data hiding is the other technique for secured communication. Data hiding involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information [2]. Data hiding is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly.

The strength of data hiding gets amplified if it combines with cryptography. The terminologies used in data hiding are cover-image, hidden 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 hidden 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 [2]. The embedding algorithm is the way, which is used to embed the secret information in the cover image.

The security of the transformation of hidden data can be obtained by two ways: encryption and data hiding. A combination of the two techniques can be used to increase the data security. In encryption, the message is changed in such a way so that no data can be disclosed if it is received by an attacker. Whereas in Data hiding, the secret message is embedded into an image often called cover image, and then sent to the receiver who extracts the secret message from the cover message. When the secret message is embedded into cover image then it is called a hidden image [6]. The visibility of this image should not be distinguishable from the cover image, so that it almost becomes impossible for the attacker to discover any embedded message.

2. Literature Review

Fridrich et al. (2001) [3], proposed the reversible data embedding method for the authentication purpose so the embedding capacity of this method is low. To separate the data extraction from image decryption, Zhang emptied out space for data embedding in the idea of compressing encrypted images [4], [5].

An encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes, a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed in [4]. W. Liu, W. Zeng, the lossy compression method presented in [5], an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied X. Zhang [8].

W. Liu, W. Zeng proposed, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource, a lossless compression method for encrypted gray image using progressive decompose and rate compatible turbo codes is developed in [5].

The method in [6] compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiver side is the spatial correlation of decrypted images.

A novel method for RDH in encrypted images, for which we do not “vacate room after encryption” as done in [7], but “reserve room before encryption”. In that, we first empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. In methods of [6]–[7], the encrypted 8-bit gray-scale images are generated by encrypting every bit-planes with a stream cipher.

2.1 **Problem Analysis**

Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. There was another problem if either of data hiding key or encryption key is leaked then the intruder can extract or decrypt the image through data hiding key or decrypt the image through encryption key.

Another problem found is that, the secret key use for encrypting the image and data hiding is same. So the user who knows the secret key use for encryption can access the embedded data and original data. The original image can be retrieved from encrypted image after extraction or removing the data hidden in the image. The content owner and data hider share the same encryption key for encryption of image and data hiding.

In previous work , there are no provision of choosing the key and more encode-decode time consumption. There are lots of data hiding programs available. A few of them are excellent in every respect; unfortunately, most of them lack usable interfaces, or contain too many bugs, or unavailability of a program for other operating systems.

3. Proposed Methodology

Data hiding provides easy way of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely. This system would be mainly concerned with the algorithm ensuring the secure data transfer between the source and destination. For that we first used encryption and then data hiding and vice-versa. In data hiding we will use cover image for security purpose. The medium in which information is to be hidden, is called as cover image.

The secret key use for encrypting the image and data hiding is same. To resolve that problem we will use one secret key for encrypting the image and another secret key for data hiding. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. Thus, if the both keys are different then there are lot of security in data transmission.

RGB shares are generated from the original secret image and by sticking together with encrypted image reveal the secret. If we are creating one or more shares and some or all of them

sticked together for getting the real secret unreveal. This process of securing data is called as secret sharing. This is one of the secure process in secure data transmission. This improves the overall quality of an image.

Proposed system has four main phases:

1. Image Encryption
2. Data Hiding
3. Image Decryption
4. Data extraction and image recovery

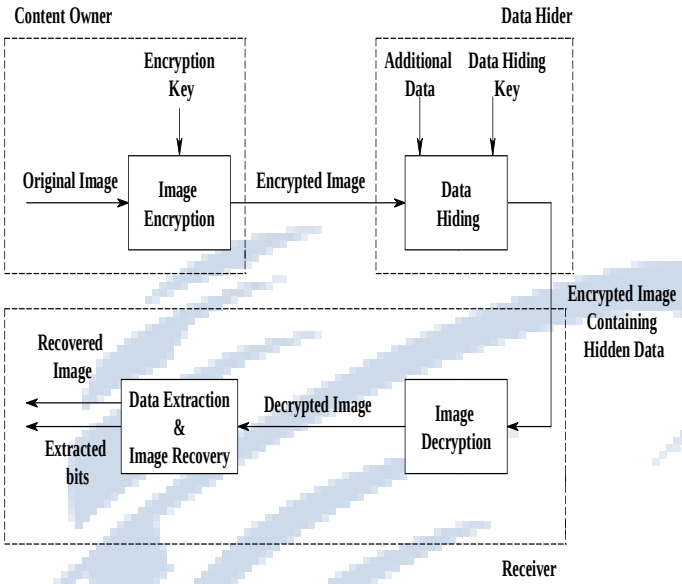

Figure 3.1 Proposed Data Hiding scheme

(Sender Side)

1. Select Image
2. Encrypt Image using Encryption key
3. Hide an encrypted image into cover image using data hiding
4. Display result of hidden image.

(Receiver side)

1. Select Hidden Image
2. Extract Hidden encrypted Image.
3. Decrypt Image
4. Extract data
5. Generate Original Image.
6. Display Result

In the proposed scheme, the original image is encrypted using an encryption key and the additional data are hidden into the encrypted image using data-hiding key. With an encrypted image containing additional data, if the receiver has only the data hiding key, he can extract the additional data though receiver does not know the image content. If receiver has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the hidden data.

3.1 Image Encryption

Proposed Image Encryption algorithm

1. ***Select an Image.***
2. ***Split Image Pixels Componants.***
3. ***XOR higher (Red,Green & Blue) Pixels componants with lower componant.***
4. ***Set (XOR result + Lower LSB)to encrypted pixel.***
5. ***Repeate step 2 to 4 until all pixels are XORed.***
6. ***Stop***

In a proposed methodology, an RGB Image encryption scheme work as follows

1. An Image with RGB format can be represented as

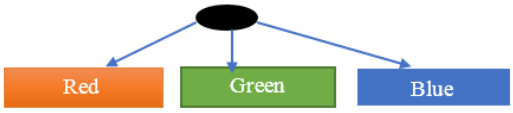

Figure3.1.1 RGB formated Image Pixel

2. Each componant of an image pixel is of 8 bits represented with

Figure3.1.2 an Image Pixel Componant

3. An Image encryption is a process where image is converted into unreadable format(Applicable for each componenats).

	Result bits	

4. Set result Bits with an each componant of pixel.so an encrypted image pixel becomes

MSB							LSB
MSB							LSB
MSB							LSB

5. Lets Consider an Example, a Pixels represented with

24 bits value as 111010100110111011000110. It's RGB Componenabts becomes

1	1	1	0	1	0	1	0
0	1	1	0	1	1	1	0
1	1	0	0	0	1	1	0

XOR for Red Componant

1 1 1 0

xor

1 0 1 1

=

1 0 1 0

So resultant red pixel componant

1 0 1 0 1 0 1 0

Same for all Green and Blue Pixels componants

3.2 LSB Image Stegnography

Proposed LSB Data hiding algorithm

1. ***Select an Image***
2. ***Split Image Pixels Componants.***
3. ***Replace LSB of Pixel componants with data Bits.***
4. ***Bind All componants(Red,green and Blue) to single pixel.***
5. ***Repeate step 2 to 4 until all data bits are hidden.***
6. ***Stop***

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:

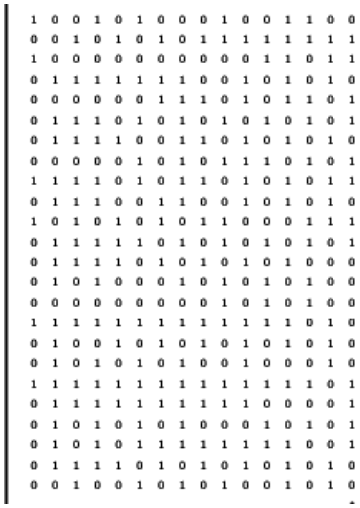

Figure3.2.1 Input Image Pixels

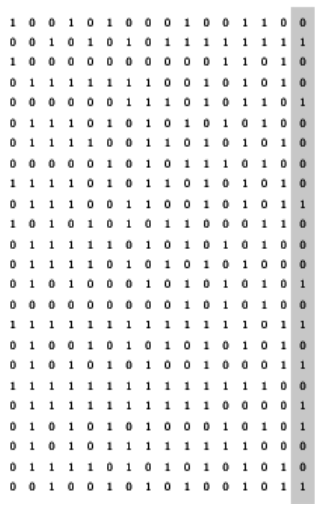

Figure3.2.2 Stego Image Pixels

Total data hiding capacity of an Image can be represented with

$Hc = (H\ x\ W\ x\ 3)/24$ ..... Eq……..3.2.1

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage : As the number of used LSBs during LSB coding increases or, equivalently, depth of the modified LSB layer becomes larger, probability of making the embedded message statistically detectable increases and perceptual transparency of stego objects is decreased. Low Bit Encoding is therefore an undesirable method, mainly due to its failure to meet the Steganography requirement of being undetectable.

4. Result Analysis

Quantization error	
Method	***Error***
LSB	-1 to + 1

3rd LSB	-8 to + 8
4th LSB	-16 to + 16
5th LSB	-32 to + 32
6th LSB	-64 to +64

Table 4.1 Quantization error Result

Sr.No	Image Size	Data bits	Data Hided	Result Image Size	PSNR
1	100 X 100	500	√	100 X 100	70.57
2	150 X 150	500	√	150 X 150	75.2143
3	200 X 200	500	√	200 X 200	80.237
4	250 X 250	500	√	250 X 250	67.2382
5	300 X 300	500	√	300 X 300	76.2342

Table 4.2 Constant data bits Result

Sr.No	Image Size	Data bits	Data Hided	Result Image Size	PSNR
1	100 X 100	500	√	100 X 100	65.57
2	150 X 150	1000	√	150 X 150	71.234
3	200 X 200	1500	√	200 X 200	79.1231
4	250 X 250	2000	√	250 X 250	61.2342
5	300 X 300	2500	√	300 X 300	72.345

Table4.3 Varying data bits Result

Sr.No	Image Size	Encrypted Image Size	PSNR
1	100 X 100	100 X 100	10.57
2	150 X 150	150 X 150	5.2143
3	200 X 200	200 X 200	6.237
4	250 X 250	250 X 250	2.2382
5	300 X 300	300 X 300	7.2342

Table 4.4 Image Encryption result

5. Implication

Following are the applications for data hiding of image

1. Secret communication,
2. Copyright protection,
3. Document authentication,

5.1 Secret communication

Secret communication does not advertise a covert communication by using data hiding. Therefore, it can avoid scrutiny of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people.

5.2 Copyright protection

Copyright protection can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the data. Data hiding are used for copyright protection by embedding the hidden data secretly which can be read only through the secret key held by the owner.

5.3 Document authentication

Document authentication is one of the best application of secure data transmission**.** In Document authentication data will be sent securely from sender to receiver.

Conclusion

We presented a reduced distortion algorithm for LSB image steganography and cryptography. The key idea of the algorithm is data hiding bit embedding that causes minimal embedding distortion of the host image. visualisation tests showed that described algorithm succeeds in increasing the depth of the embedding layer from 1 th to 5 LSB layer without affecting the perceptual transparency of the data hided image signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well,because there is a significant cryptography provided for data security.

References

[1] Lini Abraham, Neenu Daniel ," Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research volume 2, issue 4, April 2013, PP-186-189.

[2] Mohanraj Arumugam and Rabindra Kumar Singh,"Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013, PP-1-5.

[3] Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G., 2008. A novel difference expansion transform for reversible data embedding. IEEE Transaction Information Forensics and Security 3 (3), 456–465.

[4] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. SignalProcess.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans.*

Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[6] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1,pp. 53–58, Feb. 2011.

[7] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[8] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[9] Chang, C.C., Lu, T.C., 2006." A difference expansion oriented data hiding scheme for restoring the original host images" Journal of Systems and Software 79 (12), 1754–1766.

[10] W. Puech" Image Encryption and Compression for Medical Image Security" PROCEEDING OF IEEE Image Processing Theory, Tools & Applications.

[11] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images" Author manuscript, published in "IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".

[12] Saurabh Singh and Gaurav Agarwal,"Hiding image to video: A new approach of LSB replacement",International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003

[13] Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-14244-7432-5.