A Review On RGB Color Preserving Cryptography For Secure Data Transmission

Anchal A. Solio, Dr. S. A. Ladhake

***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. We present a new concept for RGB image based data hiding. It introduces the concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits. It offers very high capacity for cover media compared to other. In secure transformation of data in encrypted image is to provide high network security for data transformation.

***Index Terms*— Cover image, Data hiding, Data extraction, Data recovery. Image encryption, Image decryption .**

I. 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]. Cryptography is a technique for keeping message secure and free from attacks. Cryptography provides encryption techniques for a secure communication. In cryptography secret message is scrambled.

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. The embedding algorithm is the way, which is used to embed the secret information in the cover image [2].

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. Currently, Internet and digital media are getting more and more popular. So, requirement of secure transmission of data also increased. Various good techniques are proposed and already taken into practice.

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 will improves the overall quality of an image.

When using a 24 bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden.

***Anchal A. Solio**, Computer Science & Engineering, SGBAU, Sipna C.O.E.T. Amravati., Amravati, India, 9405423936*
***Dr. S.A. Ladhake**, , Computer Science & Engineering, SGBAU, Sipna C.O.E.T. Amravati., Amravati, India, 9422156682.,*

ISSN: 2278 – 1323

While using a 24 bit image gives a relatively large amount of space to hide messages, it is also possible to use a 8 bit image as a cover source. Because of the smaller space and different properties, 8 bit images require a more careful approach. Where 24 bit images use three bytes to represent a pixel, an 8 bit image uses only one. Changing the LSB of that byte will result in a visible change of color which is neglible and not easily detected with necked eyes, as another color in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in grayscale, as the human eye will not detect the difference between different gray values as easy as with different colors.

II. LITERATURE REVIEW AND RELATED WORK

Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G. [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. 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, L. Dong, and Q. Yao [5], proposed the lossy compression method, in that 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.

W. Liu, W. Zeng [5] 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.

X. Zhang [6], proposed method of 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.

X. Zhang [7], proposed a novel method for RDH in encrypted images, for which we do not “vacate room after encryption” as done, but “reserve room before encryption”. In that, they 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 [7]–[8], the encrypted 8-bit gray-scale images are generated by encrypting every bit-planes with a stream cipher.

Chang, C.C., Lu, T.C [9], proposed cryptographic methods do not hide the very existence of the secret data. Alternatively, confidential data can be protected by using information hiding techniques. Information hiding embeds secret information into cover objects such as written texts, digital images, audios, and videos. For more secure, cryptographic techniques can be applied to an information hiding scheme to encrypt the secret data prior to embedding.

III. ANALYSIS OF PROBLEM

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.

IV. PROPOSED WORK AND OBJECTIVES

Proposed system has four main phases:

A. Image Encryption

B. Data Hiding

C. Image Decryption

D. Data extraction and image recovery

ISSN: 2278 – 1323

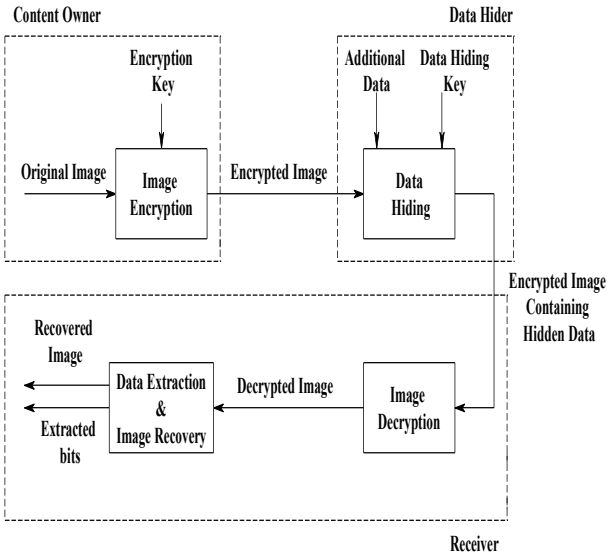

Figure:- Proposed Data Hiding scheme

(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.

V. IMPLICATION

In secure transformation of data in encrypted image is to provide high network security for data transformation. Extract the hidden data and recover the original content without any error in natural image if the amount of data is not too large. The proposed scheme of reversible data hiding technique is achieved through color image instead of gray scale image to improving the capacity of hidden data. To considering gray scale image the amount of additional data is small.

When using a color image instead of gray, each bit of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. It gives a relatively large amount of space to hide data. The image based data hiding technique is tried to improve the capacity of hidden data since, there is a limitation on how much information can be hidden into an image. To overcome the capacity problem we provide high security separate key should be used for encryption and decryption.

VI. APPLICATIONS

Following are the applications for data hiding of image :-

I. Secret communication,
II. Copyright protection,
III. Document authentication,

I. 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.

II. 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.

III. 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.

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.

ISSN: 2278 – 1323

[4] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, 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".

AUTHORS INFORMATION

Ms. Anchal A. Solio did her B.E. in Information Technology from Amravati University. She is also pursuing her M.E. in Department of Computer Science and Engineering from Sipna College of Engineering & Technology, Amravati. She is currently working as a Assistant professor in Department of Computer Science and Engineering, from the same institute since 2013.Her areas of interest is Digital Image Processing.

Dr. Siddharth A. Ladhake did his B. E. in Electrical Engineering from Nagpur University, M. E. and Ph.D. in Electronics Engineering from Amravati University. He is the Principal of Sipna College of Engineering & Technology, Amravati. He has more than 20 years of Teaching Experience. He has published many research papers and 10 scholars are pursuing Ph.D. under him. He is a member of fellow of many National and International organizations.

ISSN: 2278 – 1323