Severable Recoverable Data Covering In Encrypted Image by Creating Chamber for Data

Prarthana Modak
Professor,
SSPM's College of Engineering,
Mumbai University, Kankavli, India
prarthanamodak@gmail.com

Vijaykumar Pawar
Professor,
A. C. Patil College of Engineering,
Mumbai University, Mumbai, India
vnpawar2000@gmail.com

Abstract: Recent communication technologies are widely using digital images to exchange data over network. In this paper, we are introducing an approach for securing data passed through image. Proposed method provides severable recoverable data covering in scrambled image by creating chamber for data hiding. The proposed work is a kind of separable reversible data hiding in encrypted images. This system uses Rubik's cubic based scrambling to encrypt an image then we are hiding secret data or message into that image. Main characteristic of our system is that at the receiver side we can retrieve hidden data as well as original cover image without any distortion.

Keywords: *Severable, Scrambling, Rubik's cubic, Encryption, Data hiding.*

*****

I. INTRODUCTION

As the use of images over network has increased, more attention is given to reversible data hiding in encrypted images. The characteristic of reversible data hiding is that, at receiver end embedded data is extracted as well as the original cover image can be recovered without any distortion. Other characteristic is shielding the image content's confidentiality. The concept severable data hiding is described as, two separate methods are used to retrieve hidden data & to get decrypt cover image.In this paper we propose a scheme which manages real reversibility by creating chamber for data and encrypting image using Rubik's cubic approach. The proposed method can accomplish real recovery that is data extraction and image extraction without any error.

Reversible data hiding [3], [6] can be defined as an approach where the data is embedded into the host media that may be a cover media. And at the receiving end, the secret data and also the host media will be recovered without any loss. Now a days, a new challenge consist to reversibly hiding the data in encrypted images [1], [6]. Because it recover the original cover after extracting the embedded data. And it also protects the image content's confidentiality.

For data embedding diagonal LSB substitution method is used. This method is a simple approach to embedding message in a cover image. The LSB (i.e. the 8^{th} bit) of selected or all of the bytes of an image is replaced with a bit of the secret message. If a 24-bit image is used, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can embed 3 bits in each pixel. An image of 900 × 600 pixel, can thus be used to keep a total amount of 1,620,000 bits or 202,500 bytes of secret data.

The transmitter side of systems involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be embedded and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data. The recoverability means that not only the embedded secret data but also the encrypted cover image must be recovered at the receiver side. This technique is mainly used for the authentication of data like images, videos, electronic documents. As long as image is concerned the technique could be useful in area of protection and transmission of secret delicate military and medical images.

II. LITERATURE SURVEY

Z. Ni, Y. Shi, N. Ansari, and S. Wei, has proposed a reversible data hiding algorithm [2]. This algorithm can recover the original image without any distortion from the marked image after the hidden data have been extracted. It utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. It can embed more data than many of the existing reversible data hiding algorithms.

A non-separable reversible data hiding method [3] proposed by Xinpeng Zhang, is shown in Figure 1. In this method, the data extraction is not separable from the content decryption. The additional data must be extracted from the decrypted image, so that the principal content of the original image is revealed before data extraction. If some has a data hiding key but not the encryption key, he cannot extract the information from the decrypted image containing additional data.

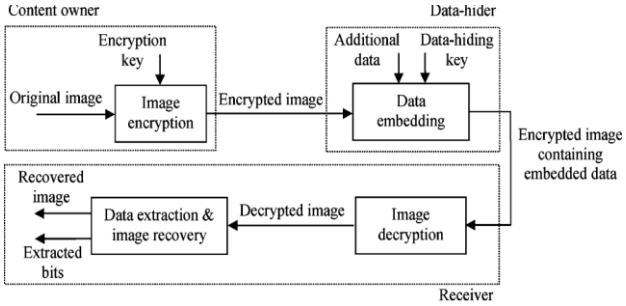

Figure 1. A Non Separable Reversible Data Hiding method.

Xinpeng Zhang has suggested, Separable Reversible Data Hiding in encrypted images [4]. If the receiver has the data

hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the original data. If the receiver has the both the data hiding key and the encryption key, he can extract the additional data and recover the original content.

W. Hong, T. Chen, and H. Wu have proposed, an improved Reversible Data Hiding in Encrypted Images using Side Match[5].The authors work exploit the pixels in calculating the smoothness of each block and consider the pixel correlations in the border of neighboring blocks. These two issues could reduce the correctness of data extraction. This method adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to further decrease the error rate of extracted-bits.

Reversible Data Hiding in encrypted images by Reserving Room before Encryption [1] suggested by Kede Ma, Weiming Zhang, Xianfeng Zhao is shown in Figure 2. The method reserves room before encryption with a traditional RDH algorithm. Hence it is easy for the data hider to reversibly embed data in the encrypted image. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.

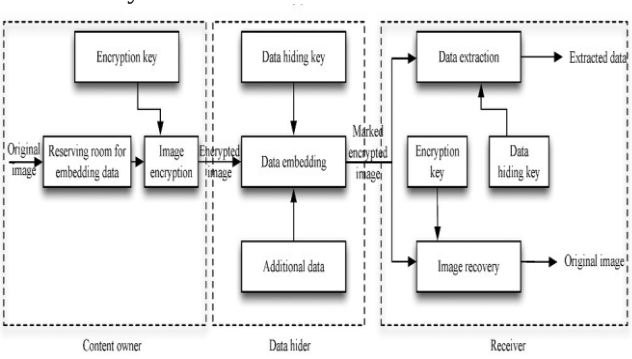

Figure 2. Reversible Data Hiding by Reserving Room before Encryption.

Chang-Lung Tsai, Chun Jung Chen, and Wei-Leih Hsu proposed a data hiding scheme based on the application of Rubik's cubic rotation [7]. They proposed a method which can be combined with any kind of data hiding approaches and encipher system to achieve information protection. The proposed data hiding scheme not only can achieve the benefits of reversible reconstruction of hidden data, but also it possesses good visual quality of the stego-image. Moreover, satisfactory data hiding capacity can be obtained simultaneously. Finally, the proposed data hiding scheme not only can be performed in spatial domain, but also can be performed in the frequency domain or even applied in hybrid domains.

Arnold transformation has been very widely used in literature, so it is unsafe to use the same, Zhenwei Shang et al. proposed a novel image block location scrambling algorithm based on Arnold transformation [8]. The method also makes use of logistic map to generate the sequence. This sequence is used on different blocks in the image after applying Arnold transformation over the blocks. Results show that the proposed method has a good encryption effect, has a large key space and also has key sensitivity.

Kekre et al. proposed an image scrambling algorithm using the concept of relative prime numbers in [9]. One of the main goal of an image scrambling algorithm is that the correlation between any two rows and columns has to be minimum. Considering this aspect, firstly correlation is calculated between the first row and every subsequent prime row, the one having minimum correlation is brought next to the first row, this process is continued till all the rows are placed. Then same process is applied to columns. The method results in good amount of decrease in correlation among rows and columns of the scrambled image when compared to original image. The row prime and column prime would act as a key to descramble the image.

Yang Zou et al. proposed an image scrambling algorithm based on Sudoku puzzle in [10]. The property of a sudoku puzzle is that in any row/column numbers 1 to N appears only once. This concept can be applied and a one to one relationship can be used between two Sudoku puzzles these puzzles can be used to map the original image to a scrambled image. The proposed method scrambles the image at both pixel level and also at bit level so as to provide more security.

III. PROPOSED WORK

The proposed method pools the profits of two different methodologies together. Those are Recoverable Data Hiding and encryption using Rubik's cubic scrambling of a cover image. Severable recoverable data covering in encrypted image by creating chamber for data is shown in figure below.

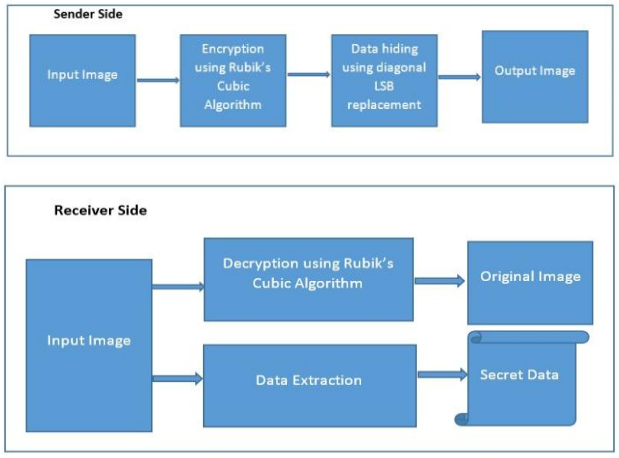

Figure 3. Block Diagram of Proposed Work.

The proposed system will be designed and implemented with the following modules:

a. Image Encryption using Rubik's cubic based algorithm
b. Reserving Room for Data Embedding & Data Hiding
c. Image Decryption & Data Extraction.

3.1 Image Encryption using Rubik's cubic based algorithm

Rubik's cubic was invented in 1974 as a famous wisdom game. In the beginning, it is a cubic with 6 different colors in each side (6 faces) as shown in Figure 4.

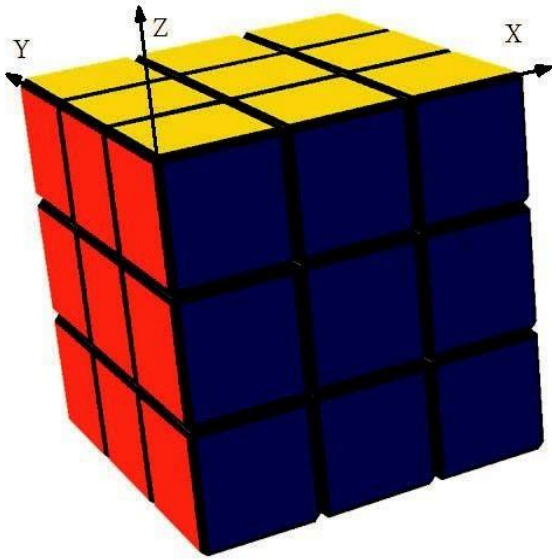

Figure 4. A Rubik's Cubic indexed with direction parameter

Rubik's cubic possesses 6 faces and can be divided into 54 (6 faces×9) elements. In the beginning, an image will be partitioned into different unit block size such as pixel based, 3×3 pixels based, or other n×n pixels based. Then, 54 units will be selected sequentially and transformed into 6 faces according to the six faces of a Rubik's cubic by designated an index number as shown in Figure 5 and Figure 6. Therefore, an image can be partitioned into a lot of different 54 units of blocks and formed a lot of different Rubik's cubic. To apply the Rubik's cubic for image encryption, the basic process unit can be one pixel, small block, or large block (macrocell) is compared to the traditional Rubik's Cubic. For example, an image can be partition by pixels to fit and associated with each of the small cubic of a Rubik's Cubic. Therefore, 54 pixels totally can be fit into the Rubik's Cubic and each pixel represents a small block. An image can also be partitioned based on 3×3, i.e. 9 pixels, as a small block. Thus, 54 3×3 blocks can be fit into the Rubik's Cubic and each 3×3 block represents a small block of the Rubik's Cubic. Each Rubik's cubic can be assigned a different random number for performing rotation to scramble the sequence of original 54 units.

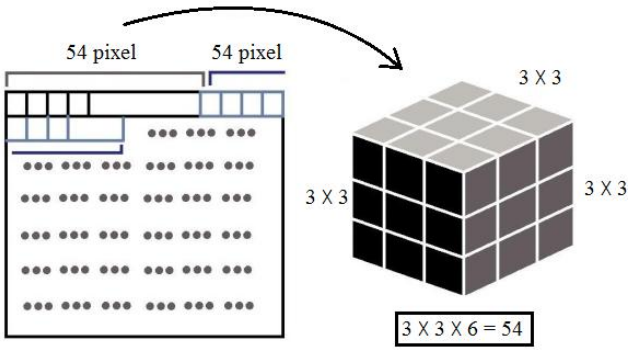

Figure 5. Mapping of Rubik's Cubic and image.

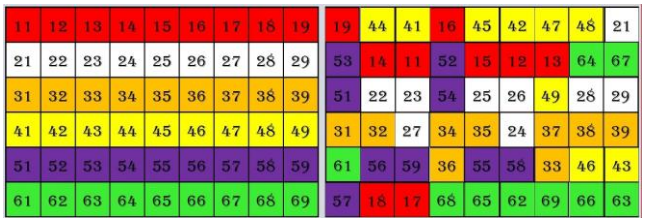

Figure 6. Example of Indexing and block Scrambling.

3.2 Creating Chamber for Data Embedding & Data Hiding

To create chamber for data embedding we are using modified traditional LSB substitution method. Instead of substituting LSB directly we are using diagonal approach.

1. Input to data hinder is an encrypted image and message to embedded.
2. Convert message into binary.
3. Use diagonal approach to create chamber for message embedding.
4. Partition image into number of rectangle/square blocks.
5. Consider pixels on diagonals of each block.
6. By using LSB replacement embed message into image.

3.3 Image Decryption & Data Extraction

As we are using Rubik's cubic scrambling technique to encrypt image we can decrypt it by performing exactly reverse rotations as we have performed for encryption. By using data extraction key we can extract hidden data.

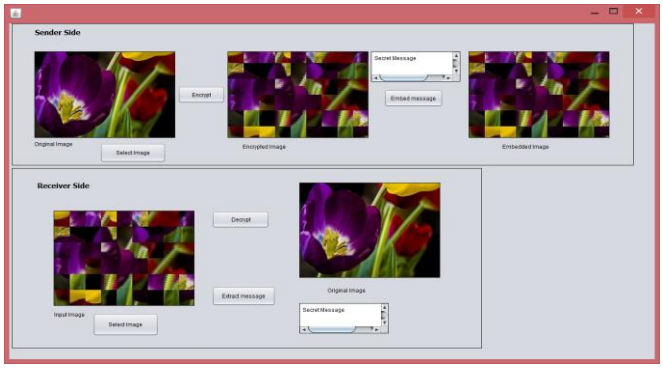

Figure 7. Proposed Work.

IV. CONCLUSION

As we are developing severable recoverable system, it gives following benefits at receiver side. First, if receiver having scrambling key he can decrypt image without knowing about hidden data. Second if receiver having data extraction key, he can extract data without decrypting cover image. Third benefit is that original cover image can retrieved without any distortion of it. If data to be embedded is an image we can use same encryption algorithm to encrypt data.

REFERENCES

[1] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", *IEEE Transactions on Information Forensics and Security, vol. 8, no. 3,* March 2013.

[2] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology, Vol. 16, No. 3,* March 2006.

[3] X. Zhang, "Reversible data hiding in encrypted image", *IEEE Signal Processing Letters, Vol. 18, No.4,* April 2011.

[4] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2,* April 2012.

[5] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match", *IEEE Signal Process, Vol. 19, no. 4,* April 2012.

[6] Weiming Zhang, Kede Ma, Nenghai Yu, "Reversibility improved data hiding in encrypted images", ELSEVIER Signal Process., 94 (2014) 118-127, June 2013.

[7] Chang-Lung Tsai, Chun-Jung Chen, Wei-Leih Hsu, "Multi-morphological Image Data Hiding based on the Application of Rubik's Cubic Algorithm," *IEEE International Conference*, 2012.

[8] Zhenwei Shang, Honge Ren, Jian Zhang. 2008. A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation. *The 9th International Conference for Young Computer Scientists, 978-0-7695- 3398-8/08/$25.00 © IEEE*

[9] H B Kekre, Tanuja Sarode, Pallavi Halarnkar, "Image Scrambling using R-Prime Shuffle," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, August 2013.

[10] Yang Zou, Xiaolin Tian, Shaowei Xia, and Yali Song. "A Novel Image Scrambling Algorithm Based on Sudoku Puzzle," *Proceedings of the Fourth International Congress on Image and Signal Processing, Vol. 2*, October 2011.

[11] Chin-Chen Chang, Yung-Chen Chou, and the Duc Kieu. "An Information Hiding Scheme Using Sudoku," Proceedings of the Third International Conference on Innovative Computing Information and Control, Dalian China, June 2008.

[12] Qi Dongxu, Zou Jianchun, Han Xiaoyou, "A New Class of Scrambling Transformation And Its Application In The Image Information Covering," *J. Science In China Scrics*, 2000.