Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 9, September 2019

A REVIEW PAPER ON DATA HIDING IN ENCRYPTED IMAGE USING LOCATION MAP

T R Mahesh
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id- t.mahesh@jainuniversity.ac.in

Abstract

In recent decades, researchers have attracted considerable attention to the visual privacy of digital data, especially in cloud-based services. It is not possible to disregard the usefulness of Reversible Data Hiding in Encrypted Images (RDHEI) as it satisfies visual privacy and data security requirements. It typically comprises the content creator, data hider, and receiver of three distinct stakeholders. Using the encryption function, the original image is encrypted by the content owner. There is still a chance for the data hider/cloud owner to embed the additional data in it after encryption. The embedded data and the original image are retrieved losslessly at the receiver end. In our suggested RDHEI method, the room is reserved by the content owner for the data concealed before image encryption.

Keywords: *Data Hiding, Encryption, Location Map, Number of Pixel Change Rate (NPCR), Vacating Room.*

I.INTRODUCTION

For clandestine communication, data hiding has attracted considerable analysis. It tries to conceal covert information in a covered media so that the opponent does not have any idea of its presence. In general, data hiding infuses the cover media with perpetual noise, and after the embedded data has been removed, the cover media cannot be reconstructed[1]. Reversible Data Hiding (RDH) is such a technique that the cover can be retrieved losslessly even after removing the embedded data[2], [3].

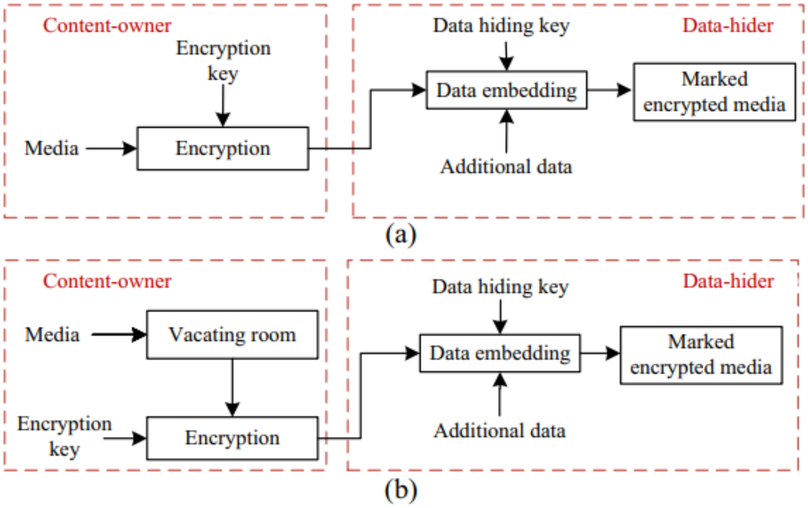

Fig. 1: Illustrates the double room emptying situations in RDHEI schemes for embedding: (a) Vacating room after Encryption (b) Vacating room before Encryption.

Figure 1 illustrates the double room emptying situations in RDHEI schemes for embedding: (a) Vacating room after Encryption (b) Vacating room before Encryption. Using the following formulas, the relationship analysis of the images is carried out. Correlation plays a key role in assessing the resemblance between the two neighboring pixels of the plain image as well as the cypher image. By applying the formulas below, the correlation coefficient of the images can be determined.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$$

$$cov\,(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\ (y_i - E(y))$$

$$r_{xy} = \frac{cov\,(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$\sqrt{D(x)} \neq 0, \sqrt{D(y)} \neq 0$$

In order to lose the image data during the transmission through the communication channel, there are some parameters that ensure the vulnerability of the different image formats against the strikers' various attacks. The Number of Pixel Change Rate (NPCR) and Unified Average Changed Intensity (UACI). The formulas for calculating the NPCR and UACI for an image is given below[4], [5].

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\ \%$$

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{255} \right] \times \frac{100\%}{M \times N}$$

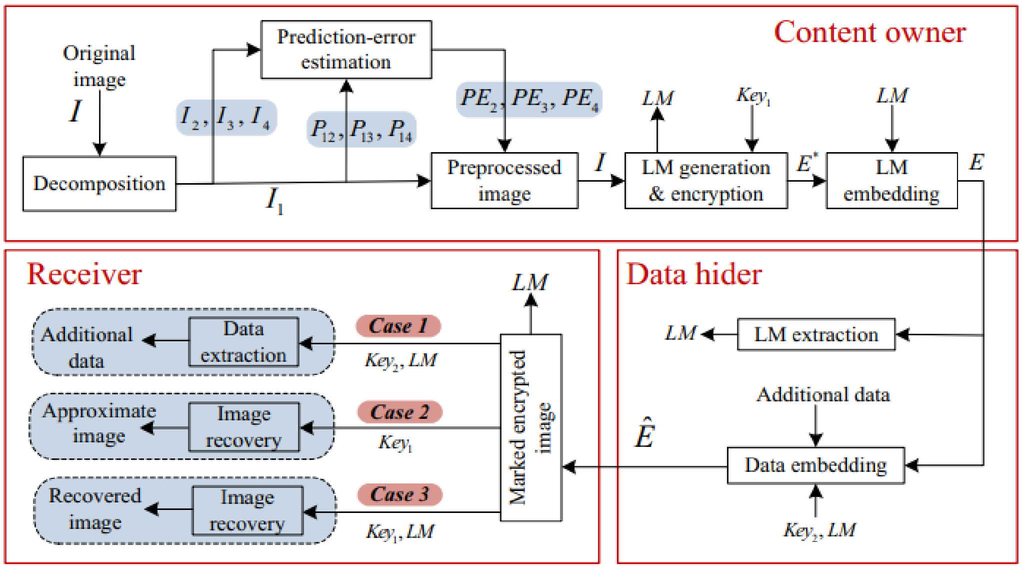

Fig. 2: Illustrates the procedure of the data hiding.

II.LITERATURE REVIEW

An analysis on a new DNA-based colour image encryption algorithm and spatial chaotic map was carried out by Liu et al. A colour image encryption algorithm based on DNA encoding is proposed in this paper, together with a logistic map and spatial map. Firstly, the algorithm performs logistic map scrambling for channels R, G, B. XOR is then run between the pixel channels and the spatial map-controlled sequence matrix. After that, the addition of R, G, B by DNA addition after DNA encoding is realized and the complement process is carried out using the spatial map-controlled DNA sequence matrix. What's more, after DNA decoding, R G B canal images are obtained. Finally, by reconstructing the components R, G, B, you get the encrypted R, G, B photos.

III.CONCLUSION

The authors give a detailed analysis of reversible data hiding strategies for encrypted images in this paper. First, the original picture is preprocessed and the corresponding map of the location is produced. In addition, using the standard stream cypher, we encrypt the preprocessed image and send it to the hider data along with the embedded location map. Secondly, by applying MSB substitution, the data hider embeds the additional data into the encrypted image at assigned locations. Finally, the receiver acquires the marked encrypted image containing the additional information. In extracting both the additional data and the lossless image recovery separately, position maps are required. In addition to the position map, the data hiding key is important for the extraction of additional data. And, an encryption key is necessary for lossless image recovery. The third case is approximate picture recovery, where we only need the encryption key.

IV.REFERENCES

[1] E. N. Kumar and E. S. Kumar, “A Simple and Robust EVH Algorithm for Modern Mobile Heterogeneous Networks- A MATLAB Approach,” 2013.

[2] S. Kumar, A. Gupta, and A. Arya, Triple Frequency S-Shaped Circularly Polarized Microstrip Antenna with Small Frequency-Ratio. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)/ISSN(Online): 2320-9801, 2016.

[3] X. Wu, J. Weng, and W. Q. Yan, “Adopting secret sharing for reversible data hiding in encrypted images,” Signal Processing, 2018, doi: 10.1016/j.sigpro.2017.09.017.

[4] J. Gupta, P. Gupta, and S. C. Gupta, “Reversible data hiding technique using histogram shifting,” 2015.

[5] Z. Yin, A. Abel, J. Tang, X. Zhang, and B. Luo, “Reversible data hiding in encrypted images based on multi-level encryption and block histogram modification,” Multimed. Tools Appl., 2017, doi: 10.1007/s11042-016-4049-z.