Secure Reversible Data Hiding in Scrambled Pictures by Reserving Room before Encryption

Ms. Jayamala K. Hipparkar*, Ms. Prajakta P. Solankar

Department of Computer Science, Karmayogi Engineering College, Shelve, Pandharpur
Solapur University, India.

*Corresponding author
doi: https://doi.org/10.21467/proceedings.118.51

ABSTRACT

Today reversible information stowing away in encoded pictures by holding room before encryption is a very significant method is use in different utilization of safety. Where information security is essential vital. These instruments are essential use in inelegancy organization. At some point when we manage an information and that information is noticed ob outsider client and that circumstance you need to shroud information specifically component that time we can utilize this reversible information covering up in scrambled pictures by holding room before encryption strategy. In this paper, we propose a novel technique by holding room before encryption with a conventional RDH calculation, and in this manner it is simple for the information hider to reversibly install information in the scrambled picture. The proposed technique can accomplish genuine reversibility, that is, information extraction and picture recuperation are liberated from any blunder. Analyses show that this novel technique can insert more than 10 times as enormous payloads for a similar picture quality as the past techniques, for example, for PSNR dB.

Keywords: Reversible data hiding, image encryption, privacy protection, histogram shift.

1 Introduction

This is technique which can use to recover original image without any data loss. we can put cover on original image and extract this cover ant get a original data. Now we can introduce about the system. This is a technique in which we can recover original image after the embedded message is extracted. This is use in clinical symbolism, military symbolism also, law legal sciences, where no twisting of the first cover is permitted. Since rest introduced, RDH has attracted considerable research interest. Thus, technique of reversible data coloring is on encrypted data is preferred. Suppose a medical image database is stored In a data center, and a server in the data center can embed notations into an encrypted version of a medical image through a RDH technique. With the notations, the server can manage the image or verify its integrity without having the information on the first substance, and hence the patient's security is ensured.

In this Current Framework, since losslessly clearing room from the scrambled pictures is moderately troublesome and at times wasteful, for what reason would we say we are still so fixated to discover novel RDH methods turning out straightforwardly for Scrambled Pictures? The method in 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 also the spatial correlation of decrypted images. All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encoded pictures has been maximized, these techniques can only achieve small payloads generate marked image with poor quality huge payload and every one of them are dependent upon some blunder rates on information extraction and additionally picture rebuilding.

Proceedings DOI: 10.21467/proceedings.118; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-6-4

Disadvantage

1 Low error rate

2 Data extraction and image restoration problem

3 Required time to extract data

4 Its lengthy process

2 Related Work

In hypothetical angle, Kalker and Willems set up a rate-contortion model for RDH, through which they demonstrated the rate-bending limits of RDH for memoryless covers and favorable to represented a recursive code development which, be that as it may, doesn't move toward the bound. Zhang *et al.* worked on the repeat sive code development for paired covers and demonstrated that this development can accomplish the rate-bending bound as long as the pressure calculation comes to entropy, which sets up strategies referenced above depend on spatial relationship of unique picture to remove information. That is, the encoded picture ought to be unscrambled first before information extraction.

To isolate the information extraction from picture decoding, Zhang exhausted out space for information inserting following the thought of packing encoded pictures Pressure of scrambled information can be planned as source coding with side data at the decoder [14], in which the regular strategy is to produce the compacted information in lossless way by ex-ploiting the conditions of equality check lattice of channel codes. The technique in packed the scrambled LSBs to abandon space for extra information by discovering conditions of an equality check network, and the side data utilized at the beneficiary side is additionally the spatial relationship of decoded pictures.

Every one of the three strategies attempt to clear room from the encoded pictures straightforwardly. In any case, since the entropy of scrambled pictures has been expanded, these methods can just accomplish little payloads or create stamped picture with poor quality for huge payload and every one of them are dependent upon some mistake rates on information extraction as well as picture rebuilding. Al-however the strategies in can dispense with blunders by mistake remedying codes, the unadulterated payloads will be additionally burned-through. Hong *et al.* decreased the mistake pace of Zhang's strategy by completely abusing the pixels in computing the perfection of each square and utilizing side match. The extraction and recuperation of squares are performed by the sliding request of the supreme perfection contrast between two up-and-comer impedes and recuperated squares can additionally be utilized to assess the smooth-ness of unrecovered blocks, which is alluded to as side match.

3 Proposed Technique

Proposed technique is very simple method of reversible data hiding and extracting original data. In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH assignments in encoded pictures would be more normal and a lot simpler which drives us to the novel framework, “reserving room before encryption (RRBE)”.

Advantage

Not only does the proposed method separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- Real reversibility is realized, that is, data extraction and image recovery are free of any error.

Proceedings DOI: 10.21467/proceedings.118
ISBN: 978-81-947843-6-4

Series: AIJR Proceedings
ISSN: 2582-3922

- For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

3.1 Modules

1. Encrypted Image Generation
    a) IMAGE PARTITION
    b) SELF REVERSIBLE EMBEDDING
2. Data Hiding in Encrypted Image
3. Data Extraction and Image Recovery
4. Data Extraction and Image Restoration

3.2 Modules Description

Encrypted Image Generation

In this module, to construct the encrypted image, the first stage can be divided into three steps:

a) IMAGE PARTITION,
b) SELF REVERSIBLE EMBEDDING followed by image encryption.

Toward the start, picture parcel step isolates unique picture into two sections and afterward, the LSBs of are reversibly inserted into with a standard RDH calculation so LSBs of can be utilized for obliging messages; finally, encode the modified picture to create its last form.

Image Partition

The administrator here for reserving room before encryption is a standard RDH method, so the objective of picture segment.

Self-Reversible Embedding

The objective of self-reversible installing is to implant the LSB-planes of into by utilizing conventional RDH calculations. We work on the technique in to exhibit the cycle of self-inserting.

3.3 Data Hiding in Encrypted Image

In this module, a content owner encodes the original image utilizing a standard code with an encryption key. In the wake of creating the encoded picture, the content owner gives up it to an data hider (e.g., a data set administrator) and the data hider can insert some helper information into the scrambled picture by losslessly clearing some room as per a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

3.4 Data Extraction and Image Recovery

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. At the point when the information base supervisor gets the information concealing key, he can unscramble and separate the extra information by straightforwardly perusing the decoded form. While mentioning for refreshing data of encoded pictures, the data set chief, then, at that point, refreshes data through LSB substitution and scrambles up dated data as indicated by the information concealing key once more. As the entire cycle is altogether worked on scrambled area, it evades the spillage of unique substance.

3.5 Data Extraction and Image Restoration

In this module, in the wake of producing the checked unscrambled picture, the content owner can additionally extricate the information and recuperate original image.

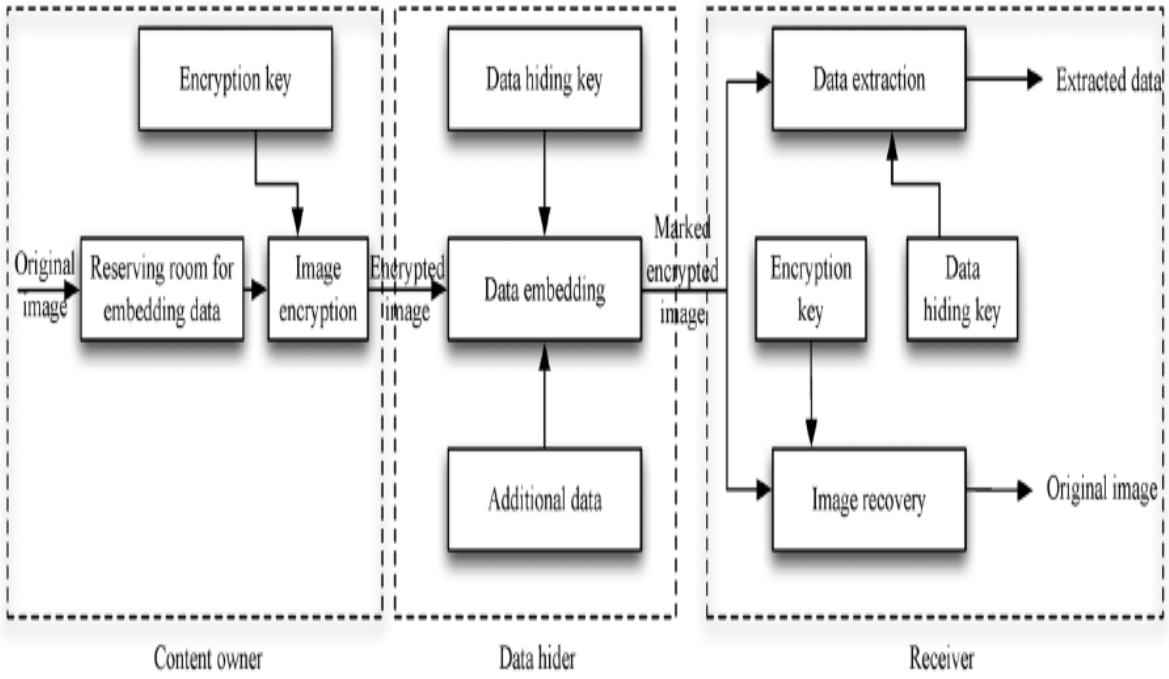

Figure 1: *System Architecture*

4 Implementation of RRBE

The figure 2 gives the data user room before encryption process in this stage the user will provide the information the image and encrypted key to the RRBE. The RRBE will process the user input will complete the encryption process these things can observe in the figure 3. The figure 4 and 5 will gives after RRBE of the user data, the user should register to the service provider, the service provider will hides the data by applying the service provider data hiding algorithms or also called as service provider encryption process.

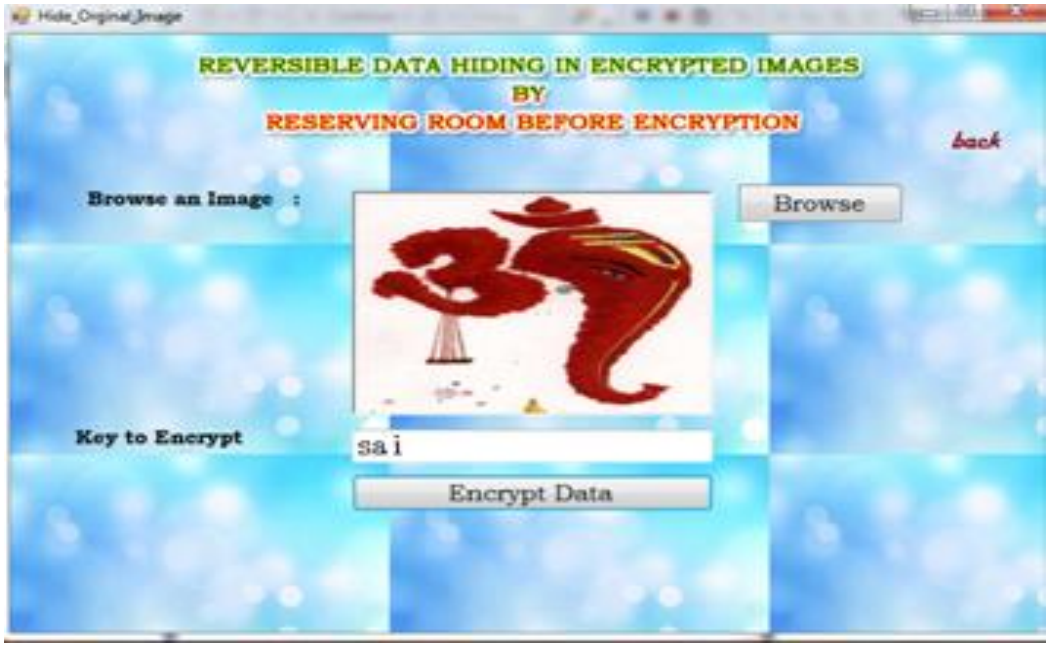

Figure 2: *User Data Input Provider*

Proceedings DOI: 10.21467/proceedings.118
ISBN: 978-81-947843-6-4

Series: AIJR Proceedings
ISSN: 2582-3922

Figure 3: *Create Encryption Key*

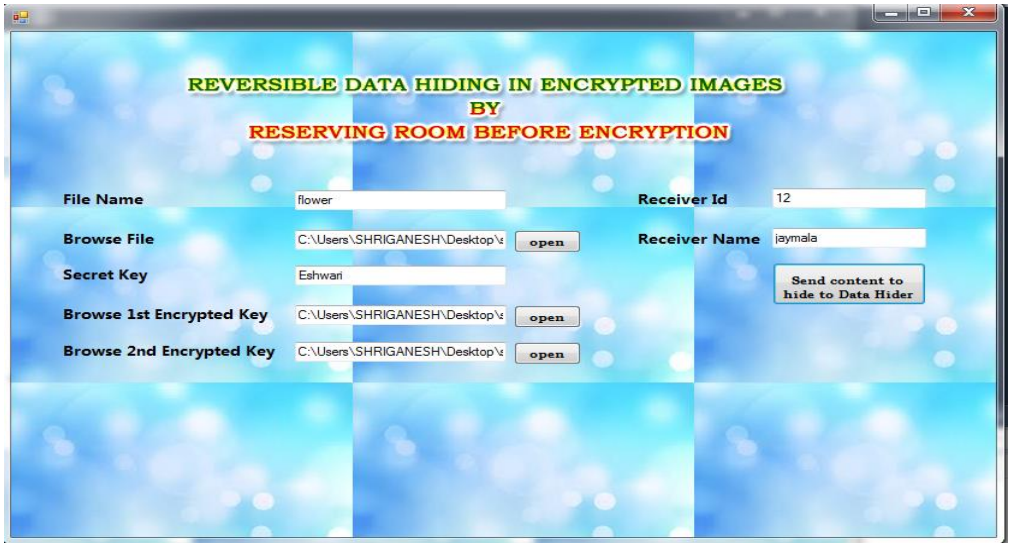

Figure 4: *Send Content to Data Hider*

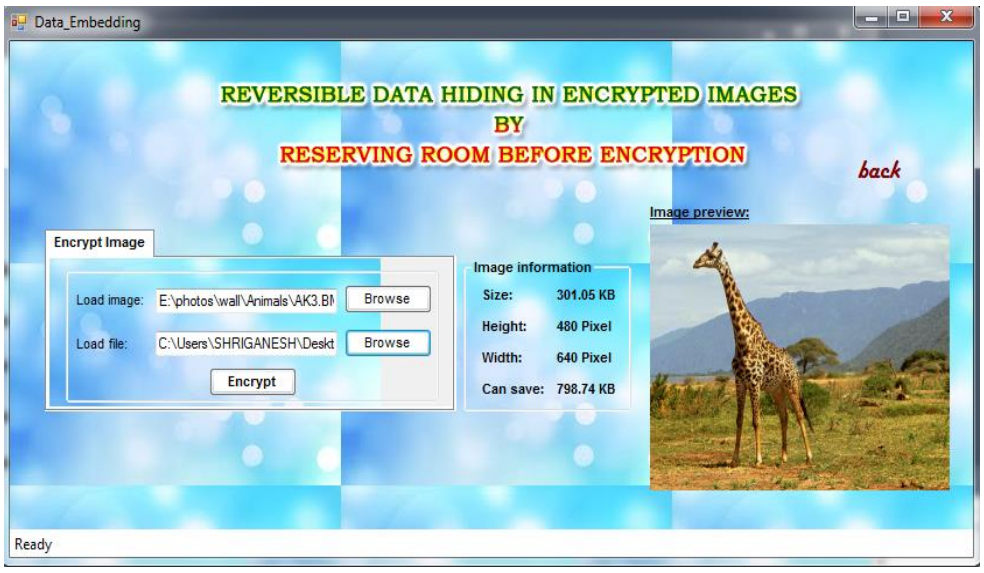

Figure 5: *Data Hiding Success by Service Provider*.

5 Conclusion

In reversible data hiding method we can learn that data can be recover lossless if you can use a right technique. Data is a very important and integral part of any field and the secrecy of that is also very important in a medical and government and military operation. So, this approach provides a very important approach to hide and get data with easily anywhere without loss. The proposed strategy can exploit all customary RDH procedures for plain pictures and accomplish phenomenal performance without loss of amazing mystery.

References

[1] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc. Photonics West Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[2] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[3] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[4] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding," in *Proc. 14th IntConf. Digital Signal Processing (DSP2002)*, 2002, pp. 71–76.

[5] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in *Proc 13th Information Hiding (IH'2011), LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.

[6] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[7] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[8] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec.2011.

[9] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, 2009.

[10] L. Luo *et al.*, "Reversible imagewatermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[12] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC, 1996.

[13] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[14] 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.

Proceedings DOI: 10.21467/proceedings.118
ISBN: 978-81-947843-6-4

Series: AIJR Proceedings
ISSN: 2582-3922