
Reversible Data Hiding Practices: An Exhaustive Study

(IJSNT) International Journal of
Communication Systems and Network
Technologies

ISSN Number: 2053-6283

Volume 7, Issue No. 1, 1–7

©The Author(s) 2018

<https://journals.mirlabs.in/index.php/ijcsnt>

DOI-10.18486/ijcsnt/7.1.087



Deepika Bahal¹, Manish Dixit²

Abstract

A phenomena of hiding any information are known as data hiding. For hiding data a number of techniques are used. Hiding of data can be done within audio, video, text and image. Inserting data in other data are a way of steganography. Mainly, in a digital image we hide data. It is equally mandatory to provide security with data hiding because data are transmitted over the network. There are many robust methods for encryption of images as per requirement. This paper provides a detailed survey of various techniques available for RDH.

Keywords

Image Steganography, Reversible Data Hiding, LSB, Histogram, Region of Interest, SMVQ

Received: 24 December 2017; **Revised:** 30 March 2018; **Accepted:** 23 April 2018;

Published: 30 April 2018;

¹Department of CSE & IT, Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh India.

²Department of CSE & IT, Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh, India.

Corresponding author:

Email: deepikabahal20@gmail.com



© 2018 by **Deepika Bahal and Manish Dixit** Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license, (<http://creativecommons.org/licenses/by/4.0/>).

This work is licensed under a Creative Commons Attribution 4.0 International License

Introduction

Steganography, which accurately means “coverwriting” and is coined from Greek terms *Steganós* (Covered), and *Graptos* (Writing). Usually, invisible communication is identified as steganography. In different forms, there is hiding of data, such as audio, video, image, communication. As people regularly convey email in which there are mainly digital images or sharing of these images is done through internet communication applications modern. Multimedia objects like images, audio, video, etc. as a cover image system which is used is known as steganography. A message which contains actual content protecting is essential. In the modern world, other information data can be hidden. Steganography deals with the art of a hiding information with an interesting property of hiding the mere existence of the secret information. Cover image, secret image and stego-image is the key modules of steganographic prototype. Where we mask our clandestine information is known as a cover image. The bit stream is converted into a secret image which is hidden and it uses stego-key, the insertion procedure is performed. For safe communication without compromising the quality of cover media after mining the message.

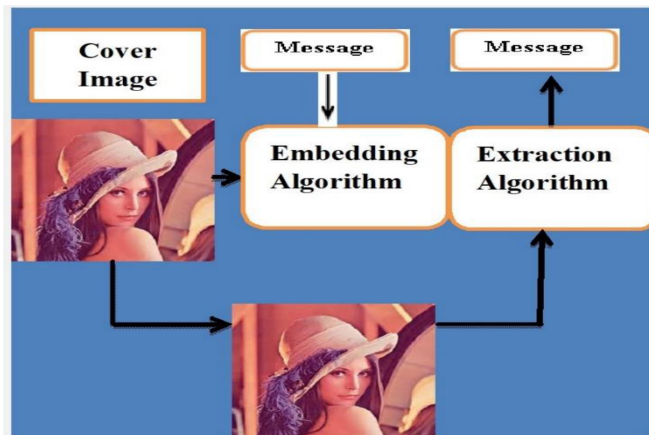


Figure 1. Image Steganography

A method “Reversible Data Hiding” is used to conceal covert information. In current time various RDH techniques have developed like histogram modification and the difference expansion technique. Being lossless makes this technique suitable for medical and military applications. This technique received more attention over the years because of its high efficiency and simplicity.

Related Work

This paper is based on the recent innovation made in the field of data embedding and using image steganography.

Weiming Zhang et.al^[1] have used a novel framework which is created for reversible image transformation (RIT) for RDH. The semantics of the previous image to the semantics of other image are through RDH-EI and original image is protected. The original image can be converted to a randomly

selected target image of the same size by means of RIT and the original image can be restored from the encrypted image in a lossless mode.

Pulkit Khandelwal and Neha Bisht^[2] have used dynamic programming to estimate the cost of the image and further random traversal is used to choose the pixels in which data is to be inserted. The authors have embedded each of the selected pixels in a predefined manner where information is in the form of bits. In terms of payload capacity, robustness, fidelity and the metrics calculated show a remarkable improvement over these existing methods.

Zhenxing Qian et.al^[3] have used a method which is grounded on progressive recovery of reversible data hiding in encrypted images (RDH-EI). There exists a framework in which three parties are included they are content-owner, the data-hider. Encryption of an original image by means of a stream cipher process. The encrypted image into three channels to create a marked encrypted image and extra data which is mined from the marked encrypted image and the original image can be retrieved which does not include any fault on the recipient side this entire procedure is completed on server side by data hider. It verifies that it is better than a separable RDH-EI method to accomplish an improved embedding rate.

Vaishali Sharma and Rupali Bhardwaj in^[4] have implemented a method in which complemented message is secreted by creating an outline of the cover image, by means of the inverted bit LSB technique. Where simulation is completed in MATLAB 14 they have used predictable on the basis of PSNR and MSE. As the cover image to cover images of dimension 512 X 512 is used which is a group of 8-bit grayscale and the gray image of size 128 X 128 to develop the stego image. Instead of hiding the message bits absolutely in cover image pixels the three levels of security, are generated randomly by authors provided through the pseudo-random number generator.

Zhenxing Qian and Xinpeng Xiang in^[5] have exhausted distributed source coding an innovative scheme for data concealment of reversible data hiding (RDH). The new image is scrambled with a stream cipher by the sender. The original image is retrieved of great quality and with the embedding key all the hidden data can be extracted. To enhanced embedding payload in the encrypted image recommended method adds to the VRE category.

Tajo Mathew in^[6] has employed the approach of reserving a sufficient area for the added data before encrypting the cover image. Firstly, it classifies the suitable blocks of hiding data from various parts of the image. After encrypting the image, those LSB-planes are used to hide additional data. It accomplishes the state-of-the-art methods in the encrypted image in the projected scheme experimentally.

Ying-Hui XIA and Hao-Tian WU^[7] have recommended a method to distinct the background and foreground the basic grayscale values which is identified as the utmost inter-class square error so that segmented background can be recognizable. A novel technique is used to acquire the foreground contour in order to raise the contrast of ROI in the medical image. There are three approaches used by authors for data hiding, i.e. Background segmentation, pre-processing and data embedding. By using the methods, the original image can be retrieved whenever required.

Dongdong Hou et.al^[8] have firstly processed the original image by means of a classic image processing method to develop the desired target image. According to the transition probability matrix the original image can be processed. The Author has used reversible image processing (RIP) technique. To accomplish the original image author used the two methods histogram equalization and gamma transform. The original copy of the processed image without loss can be returned by these methods. Similar histograms of the original and processed image can be obtained by using these two techniques.

Zhuo Zhang and Weiming Zhang^[9] have utilized used reversibility and moderate detectability methods to hide data. Created on histogram shifting method for prediction error (PE) the authors have offered a reversible steganographic method. Data hiding methods require multimedia-based covert storage. The concept of “Reversible steganography” came to meet the covert storage needs. This is an instance of which has reversed and moderate undetectability.

Tanwi Biswas et.al^[10] have recommended an innovative technique that is created by compressed gray level histogram shifting of reversible data hiding which offer an extreme ability of data hiding and also preserve high-quality image. For achieving lower distortion and improved capacity authors have used a histogram shifting created by data hiding technique.

Hamad A AL-Korbi et.al^[11] have used Haar Wavelet transform to offer a great capability and effective stenography method so that in a sole cover at the same time binary image, color images, and large text files can be all hidden. The user can conceal multiple types of private data (i.e. B&W and color images and text files) with a stego-image of a unified size of 512 X 512 pixels. By make use of recommended procedure, along with low mean square error (MSE) and high power signal-to-noise ratio (PSNR), a high capacity of about 99% is being accomplished.

Lingfei Wang et.al^[12] offered a unique method reversible data hiding scheme which utilizes enhanced Side-match vector quantization (SMVQ) for color images. In SMVQ method authors done the first column and row blocks are encrypted by convectional vector quantization and the residual blocks are encoded in a raster scanning order. Using a smaller sub codebook (SC). SMVQ technique can be simply designed by designing shifting and embedding functions. Embedding capacity and image quality can be enhanced.

Panda et.al^[13] presented a secure method to cover image in image steganography, by altering within the neighboring pixels the cover image. This technique makes the image more steady and unchanging.

Khodaei et.al^[14] presented a method by means of pixel value differencing and LSB substitution for data hiding. Here an image is fragmented into two blocks. The difference of two pixels is calculated and as per the difference, the number of embedding bits into LSBs of two pixels will be predictable.

Zhicheng Ni et.al^[15] offered a technique that explains reversible separate original image from the data which is hidden removed without any loss. By utilizing a data hiding key, add data to the scrambled image which is encoded by means of encryption keys. Extraction of the message is only done by the person who use up the data hiding key, without having knowledge of the original image. Extraction of the novel and hidden data is possible if both the keys are known. There is no loss of original image is done with embedded data and it is recovered by any distortion. For this the author used the method which is known as histogram of an image to locate its apex and zero positions and data is embedded by vaguely change transformation of values.

Xinpeng Zhang et.al^[16] proposed a technique in which encryption key is used by the sender to encrypt an uncompressed image. Data administrator will hide the data of the encoded image by utilizing of an encryption key. But previously by compressing Least Significant Bits of encrypted image by consuming another key an encoded image can be compressed. This makes gap for data embedding. Decryption is done by the hider but not the original image. At the recipient-end, original image is obtained without any distortion. This method provides the advantage of lossless compression of data.

Gupta et.al^[17] put forward a new method for image security, combining cryptography, stenography and watermarking techniques. It provides improved outcomes for MSE, PSNR and embedding power even after noise attacks and also hides the information. It also offers security for video.

Bajwa et.al^[18] implemented two methods for color image steganography. A hashing approach for secure data hiding is proceeded by the authors. Using gray scale a secure image is transmitted at high speed. This technique also supports a data of different file format such as BMP, JPEG,GIF with secured transmission.

Vipul Sharma and Sunny Kumar^[19] suggested a novel method which increases the capacity of storage by concealing message in an image. Compression of data which to be embedded is done by a compression algorithm.Only for bmp images,this technique is helpful.

Yang et.al^[20] offered a method for data hiding in the imageby using adaptive LSB substitution. This method takes care of noise sensitive area for embedding,in order to achieve better visual quality of stego-image.Normal texture and edges area of embedding is taken as an advantages. To calculate the number of k-bit LSB, this technique examines the edges, brightness and texture masking of the cover image for secret data embedding. For superior stego-image visual quality done by an LSB substitution method,that is pixel adjustment method is also utilized. This whole effect displays an extreme concealed capability.

Table: Comparion Between Related Works

Reference	Method	PSNR (dB)	Complexity	Domain
Zhenxing Qian ^[3]	RDH	Not Mentioned	Not Mentioned	Spatial
Vaishali Sharma et al. ^[4]	LSB	59.72	More	Spatial
Zhenxing Qian ^[5]	RDH	63.1	Not Mentioned	Spatial
Tojo Mathew ^[6]	Histogram	55.43	Not Mentioned	Spatial
Ying-Hui Xia et al. ^[7]	Histogram	35.16	Low	Spatial
Dongdong Hou et al. ^[8]	Histogram	56.98	More	Spatial

Conclusion and Future Work

The scope encoded this paper the chiefly emphasiset concise explanation of the numerous methods used in reversible data hiding and associationamong them.Ahuge amount of data can be embedded by certain methods, whereas some other embed smallquantity of data. Misrepresentation of the original imageand embedded image, take place in some methods.Due to distortion they havea very bad effect on image and data.But each work has its positive and negative. Different levels of application are completed with separate methods. To provide better security and efficient work it is necessary to develop a robust system and regaining the original data without lacking several alterations. Aninclusivegroupingof image which contain data encryption with security of huge extremehas to be recommended in upcomingeffort.

References

- [1] Zhang W, Wang H, Hou D et al. Reversible data hiding in encrypted image by reversible image transformation. In *Proceedings of the IEEE Transactions on Multimedia*. pp. 1–11.
- [2] Khandelwal P, Bisht N and Thanikaiselvan V. Randomly hiding secret data using dynamic programming for image steganography. In *Proceedings of the International Conference on Computing and Network Communications*. pp. 777–783.
- [3] Qian Z, Zhang X and Feng G. Reversible data hiding in encrypted images based on progressive recovery. In *Proceedings of the IEEE Signal Processing Letters*. pp. 1–5.
- [4] Sharma V and Bhardwaj R. A lossless data hiding method based on inverted lsb technique. In *Proceedings of the Third International Conference on Image Information Processing*. pp. 486–490.
- [5] Qian Z and Xhang X. Reversible data hiding in encrypted image with distributed source encoding. In *Proceedings of the IEEE Transactions on Circuits and Systems for Video Technology*. pp. 1–13.
- [6] Mathew T and Johnpaul CI. Reversible data hiding in encrypted images using interpolation-based distributed space reservation. In *Proceedings of the IEEE International Conference on Advanced Computing and Communication System*. Coimbatore, India.
- [7] XIA YH and WU HT. Reversible data hiding in medical image for contrast enhancement of roi. In *Proceedings of the IEEE 12th International Conference on Computational Intelligence and Security*. pp. 633–637.
- [8] Hou D, Zhang, Zhan Z et al. Reversible image processing via reversible data hiding. In *Proceedings of the IEEE*. pp. 427–431.
- [9] Zhang Z and Zhang W. Reversible steganography: Data hiding for covert storage. In *Proceedings of the APSIPA Annual Summit and Conference*. pp. 753–756.
- [10] Biswas T, Hasan MM and Debnath T. A new method of reversible data hiding based on compressed gray level histogram shifting. In *Proceedings of the IEEE*.
- [11] Al-Korbi HA, Al-Ataby A, Al-Tae MA et al. High-capacity image steganography based on haar dwf for hiding miscellaneous data. In *Proceedings of the IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*.
- [12] Wang L, Pan Z and Zhu R. Efficient reversible data hiding scheme based on improved smvq index for color image. In *Proceedings of School of Electronic and Information Engineering, Xi'an Jiaotong University, P.R. China*. pp. 1–6.
- [13] Panda SS. A secure approach to spatial image steganography. *VIT University, Vellore, India* 2016; 8(2): 13384–13400.
- [14] Khodaei M. Adaptive data hiding, using pixel-value differencing and lsb substitution. *Institute for Advanced Studies in Basic Science (IASBS), Zanjan, Iran* 2016; : 1–12.

-
- [15] Ni Z, Sh Y, Ansari N et al. Reversible data hiding. *IEEE Transactions on Information Forensics and Security* 2012; .
 - [16] Zhang X. Separable reversible data hiding in encrypted image. *IEEE Transactions on Information Forensics and Security* 2012; 7(2): 826–832.
 - [17] Gupta R. New proposed practice for secure image combining cryptography steganography and watermarking based on various parameters. In *Proceedings of the International Conference on Contemporary Computing and Informatics*. pp. 475–479.
 - [18] Bajwa IS. A new perfect hashing based approach for secure stenograph. In *Proceedings of the 6th International Conference on Digital Information Management*. pp. 174–178.
 - [19] Sharma V and Kumar S. A new approach to hide text in images using steganography. *International Journal of Advanced Research in Computer Science and Software Engineering* 2013; .
 - [20] Yang H, Sun X and Sun G. A high capacity image data hiding scheme using adaptive lsb substitution. *Radioengineering* 2009; .