International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

# Review on Reversible Data Hiding With Distributed Source Encoding Using Identity Hiding Mechanism for Image and Data Owner

**Sanjyot A. Biranje[1], Dr. D S. Bhosle[2]**

[1]Department of Computer Science and Engineering, AMGOI Vathar

[2]Professor, Department of Computer Science and Engineering, AMGOI Vathar

**Abstract:** ***Using Reversible Data Hiding concept system can provide security, authentication to the information system. Data hiding cannot recover original cover. While Reversible data hiding is a novel concept, which can recover original cover without any loss of image. With Reversible Data Hiding (RDH) the proposed system can perform embedding operation after encryption. In this technology initially image owner creates space for embedding additional data and then encrypts the original image after that data hider module embed additional data in the space created in the encrypted image. At the receiver side, host can extract the data and additional data and recover original message. This concept improves payload & security of the system. This is the basic theme of this concept. Basically this work describes the survey of the reversible data hiding techniques, related methods and procedures that have been developed with the subject.***

**Keywords:** reversible data hiding, watermarking, privacy information, encryption, image security

## 1. Introduction

The protection of data can be done by several mechanisms to secure and achieve authenticity and integrity of data. Data hiding is a technique in which a piece of information can be embedded to cover media data for security reason. So a digital watermarking can be used to protect the copyright of digital products unlike robust watermarking, reversible data hiding (RDH) emphasizes perfect image reconstruction and data extraction, but not robustness against malicious attacks. In such processes it is needed to maintain the original view of the host image as well as protect integrity of data. For evaluating the Data hiding methods performance it must be concentrating on the robustness of watermarked image quality and restored image quality. For this purpose the work proposes a novel scheme of reversible data hiding in encrypted images using distributed source encoding. After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make room for the secret data.

To protect the legal copyright of diverse forms of multimedia, techniques used to embed information are desperately needed. The data hiding techniques focus on how to efficiently embed a piece of information into cover media data to carry out specific missions. Reversible Data Hiding in Encrypted Images with Distributed Source Encoding is useful in protecting the copyright of digital products. The techniques requires visual imperceptibility and robustness against various malicious attacks. To restore an original image, the proposed method can recover the host image under resist multiform attacks, and thus protect the copyright of digital products. On the receiver side, the secret bits can be extracted if the image receiver has the embedding key only. In case the receiver has the encryption key only, he/she can recover the original image approximately with high quality using an image estimation algorithm. If the receiver has both the embedding and encryption keys, he/she can extract the secret data and perfectly recover the original image using the distributed source decoding.

## 2. Problem Statement

Designing a system that hide data using image encryption, data embedding, data extraction and image recovery. Here the sender can encrypts the original image into an encrypted image using a stream cipher and an encryption key. The receiver extracts the secret bits using the embedding key. If he/she has the encryption key, the original image can be approximately reconstructed via image decryption and estimation. Only when both the encryption and embedding keys are available, the receiver can extract the compressed bits, and implement the distributed source decoding using the estimated image as side information to perfectly recover the original image. Two aspects of data security need to be considered:

1) Security of the image content and
2) Security of the additional message.

The content owner does not allow the service provider to access the image content, and the data-hider does not allow adversaries to crack the embedded message.

## 3. Objectives

1) To develop a System that resist malicious attacks to protect the data hidden in image, so only authorized user can retrieve a data.
2) To maintain encrypted image quality so that it is difficult for a hacker to distinguish between the host image and the embedded one.
3) Design a recovery mechanism to recover embedded data even though the image is cropped.

4) To provide an efficient data hiding tech & image encryption in which the data & the image can be retrieved independently.

## 4. Related Work

**Xinpeng Zhang, Member IEEE**
In this paper authors proposed the optimal rule of value modification under a payload-distortion criterion is found by using an iterative procedure, & a practical RDH scheme. The secret data, as well as the auxiliary information used for content recovery, are carried by differences between the original pixel-values & the corresponding values estimated from the neighbours. Here the estimated errors are modified according to the optimal value transfer rule. Also the host image is divided into a number of pixel subsets & auxiliary information of subset is always embedded into the estimation errors in the next subset. A receiver can successfully extract embedded secret data & recover the original content in the subsets with an inverse order.

**Xiaocheng Hu, Weiming Zhang, Xiaolong Li & Nenghai Yu**
In this paper the authors proposed a pixel prediction method based on the minimum rate criterion for RDH, which establishes the consistency between following 2 steps and correspondingly, novel optimized histograms modification scheme is used to approximate the optimal embedding performance on the generated PE (Paired-End) sequences.

1) Sharp prediction error histogram (PEH) is generated by utilizing pixel prediction strategies.
2) Secret messages are reversibly embedded into prediction-errors through expanding & shifting the PE histogram.

**Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang**
In this paper authors proposed RDH method based on PEE for multiple histograms. Here a sequence of histograms are considered & new embedding mechanism based on multiple histograms modification (MHM) is devised .A complexity measurement is computed for each pixel according to its context, to generate a PEH. By varying the complexity to cover the whole image, a sequence of histograms can be generated. Then, two expansion bins are selected in each generated histogram & data embedding is realized based on MHM.Here, expansion bins are adaptively selected considering the image content such that the embedding distortion is minimized.

**Weiming Zhang, Xiaocheng Hu, Xiaolong Li, and Yu Nenghai:-**
In this paper the authors proposed a unified framework of estimating Optimal Transition Probability Matrix (OTPM) for general distortion metrics with which the rate distortion bound of RDH can be calculated for general cases and extend the Recursive Code Construction (RCC) to improve RDH schemes based on any distortion metrics.

**Zhenxing Qian, Member, IEEE, and Xinpeng Zhang, Member, IEEE:-**
In this paper the authors proposed RDH scheme in encrypted images using distributed source coding. After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image make room for the secret data. The selected bit series is Slepian–Wolf encoded using low-density parity check codes. On the receiver side, the secret bits can be extracted if the image receiver has the embedding key only. In case the receiver has the encryption key only, he/she can recover the original image approximately with high quality using an image estimation algorithm. If the receiver has both the embedding and encryption keys, he/she can extract the secret data and perfectly recover the original image using the distributed source decoding.

**Prajakta Jagtap1, Atharva Joshi2, Shamsundar Vyas3 Student, Computer Department, NBN Sinhgad School of Engineering, Pune, India**
In this paper the authors proposed a novel scheme of data hiding in encrypted images based on lossless compression of encrypted data. In encryption phase, the original content is encrypted into images. As majority of the encrypted data is kept unchanged, the quality of the decrypted image is satisfactory. In the receiver phase, the data is extracted from the image with the help of a public key. The receiver can further recover the original plaintext image without any error.

**Xiaochun Cao, Senior Member, IEEE, Ling Du, Xingxing Wei, Dan Meng, Member, IEEE,and Xiaojie Guo, Member, IEEE**
In this paper the authors proposed the patch-level sparse representation when hiding the secret data. The widely used sparse coding technique has demonstrated that a patch can be linearly represented by some atoms in an over-complete dictionary. As the sparse coding is an approximation solution, the leading residual errors are encoded and Self-embedded within the cover image. Furthermore, the learned dictionary is also embedded into the encrypted image. So by using sparse coding, a large vacated room can be achieved, and thus the data hider can embed more secret messages in the encrypted image.

**Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng**
In this paper the authors proposed a lossless, a reversible, and a combined data hiding schemes for cipher text images encrypted by public key crypto systems with probabilistic and holomorphic properties. In the lossless scheme, the cipher text pixels are replaced with new values to embed the additional data into several LSB-planes of cipher text pixels by multi-layer wet paper coding. Then, the embedded data can be directly extracted from the encrypted domain, and the data embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted images for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image can be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the combined technique, a receiver may extract a part of embedded data

before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.

**Image fragmentation**

In the first phase, a image is obtained, which comprises of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The phase incorporates four stages:

1) Fitting the tile images of the secret image into the target blocks of a preselected target image;
2) Changing the color characteristic of every tile image in the secret image to turn that of the corresponding target block in the target image;
3) Pivoting every tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and
4) Implanting required information into the created mosaic image for future recuperation of the secret image.

**Reserve Space**

Here unarability of space is biggest problem and some space created at the time of embedding. So this is also time consuming process. After extracting the data the proposed system cannot achieve the originality. Some distortion exists in the system. So our aim is to remove this type of distortion form the system. There are lots of problems in the existing system. So objective is to recover the problems in future, which are described below:

- The extracted data may contain error.
- Time-consuming process.
- Availability of memory space.
- The key contents are not store of original image.

These entire problem recovered by using the concept of"Reserving Room Before encryption "With the use of this concept with cannot achieve original data after encryption. So that new concept used for achieve this propertyi.e. RRBE. The proposed system extracted data losslessly after encryption.

**Data hiding in encrypted image**

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of A, denoted by *AE* Since *AE* has been rearranged to the top of E.After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following to point out the end position of embedding process and further encrypts according to the data hiding key to formulate marked encrypted image denoted by E'. Anyone who does not possess the data hiding key could not extract the additional data.

**DSC and distributed source decoding**

As the proposed method is based on DSC, the LDPC matrix H to generate the bits that compresses bits into r bits. Here, the ratio β should be determined by correlation statistics between the source and the side information. DSC is shown in Fig. 1, extended block in which X is the source to be encoded, Y is the side information for decoding, and avirtual channel between X and Y is assumed. Since the data-hider has no knowledge of the virtual channel and there is no feedback channel between the data-hider and the receiver.

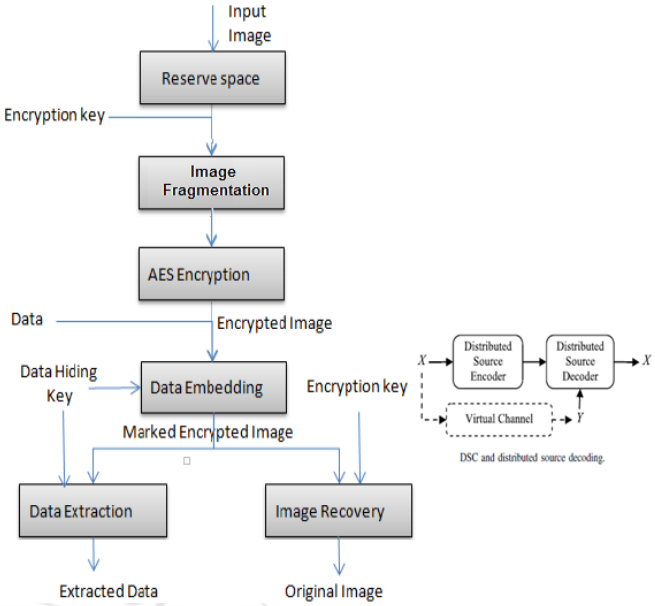


**Figure 1:** Reversible Data Hiding Scheme

**Extracting Data**

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. The order of data extraction before image decryption guarantees the feasibility of this work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating in formation of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

## 5. Conclusion

From the study and analysis different systems to develop crop-resistant encryption method to generate the visual quality of the embedded image and also it is robust against various malicious attacks. System will be used to send important data within the image without affecting any malicious attacks on that image and without worrying about recovering of the hosted data within the image by unauthorized person. So the embedded data within the host image can be recovered by only authorized person.

## References

[1] Z. Erkinet al., "Protection and retrieval of encrypted multimediacontent: When cryptography meets signal processing," EURASIP J. Inf.Secur., vol. 2007, p. 078943, Dec. 2007.
[2] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, andK.Ramchandran, "On compressing encrypted data,"

*IEEE Trans. SignalProcess.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[3] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression ofencryptedgrayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4,pp. 1097–1102, Apr. 2010.

[4] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encryptedimages," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108–3114,Jun. 2012.

[5] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficientbuyer-seller watermarking protocol based on composite signalrepresentation," in *Proc. 11th ACM Workshop Multimedia Secur.*, 2009,pp. 9–18.

[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption andwatermarking in video compression," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[7] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hidingmethod for encrypted images," *Proc. SPIE, Secur., Forensics,Steganogr., Watermarking Multimedia Contents X*, vol. 6819, p. 68191E,Feb. 2008.

[8] X. Zhang, "Reversible data hiding in encrypted image," *IEEE SignalProcess.Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.[9] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible datahiding in encrypted images using side match," *IEEE Signal Process.Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.

[9] X. Zhang, "Separable reversible data hiding in encrypted image,"*IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832,Apr. 2012.

[10] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible datahiding in encrypted images by reserving room before encryption,"*IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562,Mar. 2013.

[11] Z. Qian, X. Han, and X. Zhang, "Separable reversible data hidingin encrypted images by *n*-nary histogram modification," in *Proc. 3rd Int. Conf. Multimedia Technol. (ICMT)*, Guangzhou, China, 2013,pp. 869–876.

[12] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding inencrypted images," *Signal Process.*, vol. 94, pp. 118–127, Jan. 2014.