International Journal of Engineering & Technology, 7 (4.41) (2018) 42-46

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Study of Reversible Data Hiding in Encrypted Images

Pornima Suryawanshi[1]*, Vanita Mane [2], Puja Padiya[3]

[1]Computer Science Deparment, Ramrao Adik Institute of Technology, Navi Mumbai, India.
[2]Computer Science Department, Ramrao Adik Institute of Technology, Navi Mumbai, India.
[3]Computer Science Department, Ramrao Adik Institute of Technology, Navi Mumbai, India.
**E-mail: pornimars11@gmail.com*

Abstract

In our daily life we outsource the multimedia files such as images, videos etc. to the cloud server. So this data need to be stored securely. This security is obtained by using different encryption techniques. The study shows that Reserving Room Before Encryption is much better than the Vacating Room After Encryption. Because Reserving Room Before Encryption gives the better image quality and large payload capacity than Vacating Room After Encryption. But RRBE is having some security isues which is limitation of this method. To overcome this problem Reversible Image Transformation (RIT) based framework is used which is client free framework. In this framework the encrypted image is stored in the form of plaintext. So it will avoid the attention of curious cloud. This paper focuses on different RDH methods.

Keywords: *Data Extraction;Image Encryption;Image Recovery;Reversible Data Hiding;;SVM*

1. Introduction

Internet is boon in today digital world because most of the communication is done through internet. The com-munication may be done by using secure data, important messages, secret data, different images and documents. so it is very important to provide security to this communication. Many encryption techniques are available for security purpose. The term reversible in reversible data hiding in the sense this extract data and image without loss after decryption.

In our daily life we handle so many multimedia files such as images, videos and we outsource this to cloud. this outsourced data needs large storage space. Reversible data hiding in encrypted images are based on following two frameworks [23]:

Framework I vacating room after encryption (VRAE)

Framework II reserving room before encryption (RRBE).

In the framework " vacating room after encryption (VRAE)" [16]. The room can be reserved for embedding bits the Zhang divided the encrypted image into some block. In each block three bits which are LSBs are reserved. This reserved space is used for data embedding which gives maximum entropy. The vacating room after encryption technique useful only for small payload.

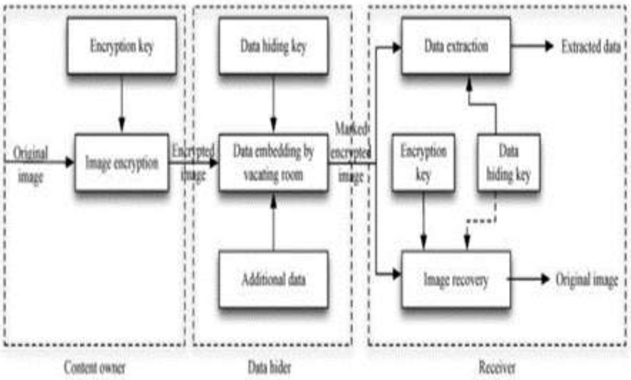

Fig. 1: Framework VRAE [13]

This method recover poor quality image while embeds large data in encrypted image. Fig. 1[13] shows the flow of vacating room after encryption. In this method first original image is encrypted using encryption key. Then room reservation is done in encrypted image for data hiding. In reserved space data hiding is done using data hiding key. In last phase data hiding key is used for data etraction and encryption key gives original image [13].
In the framework" reserving room before encryption (RRBE)" [13], The vacating Room After Encryption in the encrypted images is relatively difficult and sometimes inefficient. To overcome this problem the room is reserved before encryption for data embedding. Fig 2[13] shows the working of reserving Room Before Encryption. In this method first room is reserved from the original image, Then this space reserved image is encrypted using encryption key. This encrypted image is used for data hiding using data hiding key. encryption key is used to recover original image and data extraction is done using data hidi key [13].

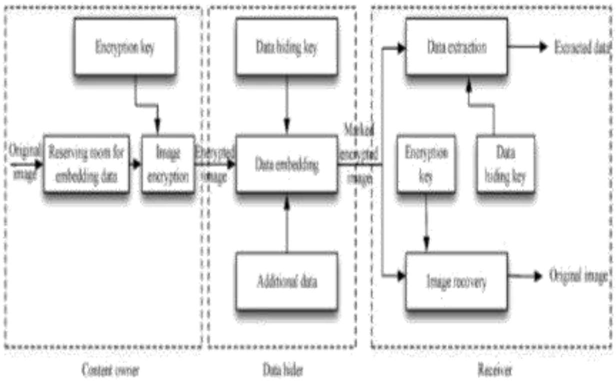

Fig. 2: Framework RRBE [13]

Subsequent sections are organized as follows: In below Section we have done survey about literature. It gives overview of work done in this field. Then Comparative Analysis is given. After that different techniques for Reversible Data Hiding are stated where this hiding is done in encrypted images. Last Section concludes this study.

2. Literature Review

Data hiding is considered as one of the encryption technique. sometimes in data hiding technique after data extraction original image may be damaged. So to avoid this problem Reversible Data Hiding is used which is lossless method.

Literature survey shows that, lot of work is still going on in Reversible Data Hiding using various techniques.

In this paper [13] Reserving Room Before Encryption technique is used. This technique gives better performance than techniques from VRAE framework. Room is re-served from original image before encryption of images. Practically this technique is based on four stages that is generation of encrypted image, data hiding in encrypted image, data extraction and image recovery. This technique is useful for getting better image quality as original without loss after extraction of cover media but it is not useful for large payload.

In this paper[18] Key Modulation technique is used for reversiblee data hiding. In this method the information hiding is done by using public key modulation mechanism. In this technique the secrete encryption key is not needed to embed data into encrypted image. This is RDH method in which powerful two class SVM classifier is used at decoder side to separate encrypted and non-encrypted image patches This is non-separable RDH method because extraction of data and reconstruction of image takes place at a time. Key Modulation technique gives large embedding capacity and also extraction of both data and cover image losslessly. But this is server related technique and encrypted image is in the form of ciphertexts.

Zhenxing Qian, Xinpeng Zhang proposed a technique for Reversible Data Hiding in encrypted images [20] using Distributed Source Encoding. This technique is based on VRAE framework. This method is proposed to get large embedding capacity by MSB estimation together with DSC. This is separable method because separate encryption key and embedding key is needed to reconstruct original image and extract data respectively. Space is reserved for embedding message by compressing some MSB of secrete image is Slepian-Wolf encoded using Low Density Parity Check (LDPC) codes. DSC technique is best for perfectly reconstruct the original image and data using separate keys. but encrypted image is in not in the form of plaintexts.

In this paper [23] the author explained the techniques for RDH using Reversible Image Transformation. Previous techniques are based on RRBE and VRAE framework which gives encrypted image in the form of ciphertext this is not good according to security purpose. Zhang [23] proposed a new framework that is Reversible Image Transformation which gives encrypted image in the form of plaintext. So any traditional RDH algorithm of plaintext image is used to embed data into encrypted image.

3. Comparative Analysis

Different RDH Techniques are used to hide data in the encrypted image. In the below table, I compare the different techniques of RDH techniques and their advantages-disadvantages.

From the above table we conclude that The Reversible Image Transformation technique used for Reversible Data Hiding in encrypted images is better.

Table 1: Comparative Analysis of RDH Techniques

Name of Technique	Year	Pros	Cons
Reserving Room Before Encryption	2013	After decryption original image is captured	This technique is useful for less payload
Key Modulation	2015	Large embedding space is available and Original image is restored	The encrypted image is in the form of ciphertext so it gets attention of curious cloud
Distributed Source Encoding	2015	Good image quality and achieve a better payload capacity with much lower error rates	Encrypted Image is in ciphertext format
Patch-Level Sparse Representation	2016	Large space is available to embed data and image is restored successfully	Ciphertext formed encrypted image may invite Attackers
Reversible Image Transformation	2016	Restore the original image from the encrypted image in a lossless way and embeds large payel because this technique can use any classical method to satisfy needs	Encrypted image has the form of a plaintext image, so avoid the notation of the curious cloud server

4. Different Techniques for Reversible Data Hiding in Encrypted Images

Recently, Research has been going on in the field of Reversible Data Hiding in Encrypted Images. Mostly Data Hiding is done according to two frameworks that is RRBE and VRAE with some more advancement. Different methods used for RDHEI are briefly explained as follows..

4.1.Patch Level Sparse Representation [22]

This technique is based on the Reserving Room Before Encryption framework. In RRBE framework pixel level representation for data embedding is done so it gives less embedding capacity. In HC-SRDHEI technique patch level representation is used for data hiding by using RRBE framework, Therefore large payload is available for data hiding. The below fig shows room preserving process in both pixel level and patch level representation

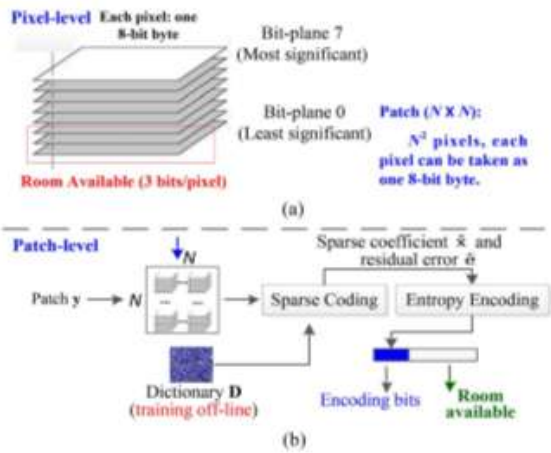
Pixel-level
Each pixel: one 8-bit byte
Bit-plane 7 (Most significant)
Bit-plane 0 (Least significant)
Patch (N X N): N² pixels, each pixel can be taken as one 8-bit byte.
Room Available (3 bits/pixel)
(a)
Patch-level
N
Patch y
N
Sparse coefficient x̂ and residual error ê
Sparse Coding
Entropy Encoding
Dictionary D (training off-line)
Encoding bits
Room available
(b)

Fig. 3: Comparison between pixel-level and patch-level representation for room preserving [22]

In pixel level representation 3 bits are available in each pixel as shown in Fig. 3(a). So small space is available to hide data as compared to patch level representation. Because in patch level representation shown in Fig 3(b) only small number of coefficient and residual error obtained, Therefore large embedding space is available.

Patch Level Sparse Representation is Separable Re-versible Data Hiding tehnique because data extraction and image recovery is not depends on each other that is separate encryption key and embedding key is used for image encryption and data hiding. The fig.4(a) shows that content owner reserves space in training image by using sparse coding and encrypts image usin encryption key. In this encrypted image data hider embeds secrete information using data hiding key in the space where patches are selected using sparse coding. Content owner is not depends on data hider. In fig. 4(b) three cases are given. In case 1 the receiver have only data hiding key so it get only hidden data. In case 2 receiver have both data hiding and encryption key which extract both data and image. In case 3 receiver have encryption key which recover only image. Therefore this technique is separable.

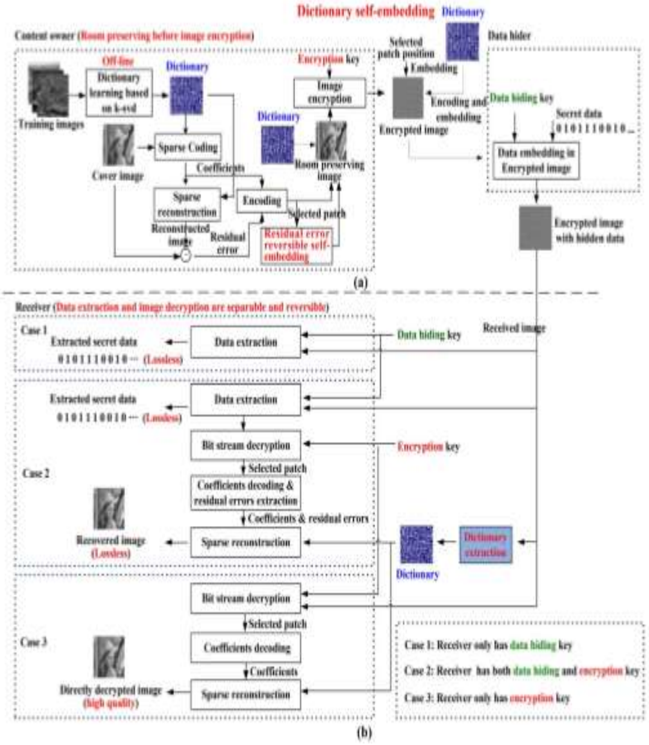
Dictionary self-embedding
Dictionary
Content owner (Room preserving before image encryption)
Data hider
Off-line
Dictionary learning based on k-svd
Dictionary
Training images
Encryption key
Image encryption
Selected patch position
Embedding
Encoding and embedding
Encrypted image
Data hiding key
Secret data
0101110010...
Data embedding in Encrypted image
Sparse Coding
Cover image
Coefficients
Room preserving image
Sparse reconstruction
Encoding
Selected patch
Reconstructed image
Residual error
Residual error reversible self-embedding
Encrypted image with hidden data
(a)
Receiver (Data extraction and image decryption are separable and reversible)
Received image
Case 1
Extracted secret data
0101110010... (Lossless)
Data extraction
Data hiding key
Case 2
Bit stream decryption
Encryption key
Selected patch
Coefficients decoding & residual errors extraction
Coefficients & residual errors
Recovered image (Lossless)
Sparse reconstruction
Dictionary
Dictionary extraction
Case 3
Coefficients decoding
Coefficients
Directly decrypted image (high quality)
Case 1: Receiver only has data hiding key
Case 2: Receiver has both data hiding and encryption key
Case 3: Receiver only has encryption key
(b)

Fig. 4: Flowchart of HC-SRDHEI Method .[22]

4.2. Reversible Image Transformation [23]

The Vacating Room After Encryption (VRAE) and Re-serving Room Before Encryption (RRBE) both frameworks outsourced the encrypted image in the form of ciphertext so it attracts the attention of curious cloud.

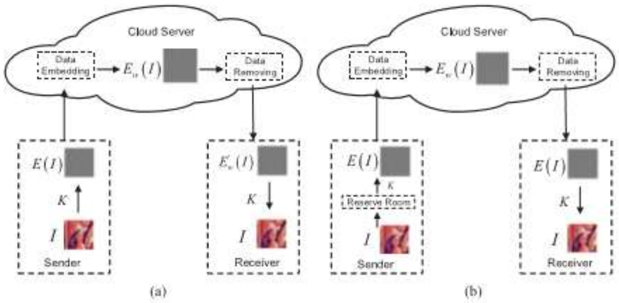

Fig.5:(a) Framework VRAE. (b) Framework RRBE [23]

The Reversible Image Transformation(RIT) based framework[23] store the encrypted image in the form of plaintexts, so it not get the attention of curious cloud. Data embedding is done in this encrypted image by using any RDH algorithm which are applicable for plaintext image. The Reversible Data Hiding used by cloud is not related to both sender and receiver, thus this framework is also called client free scheme. fig.6 [23] shows the working of Reversible Image Transformation based framework.

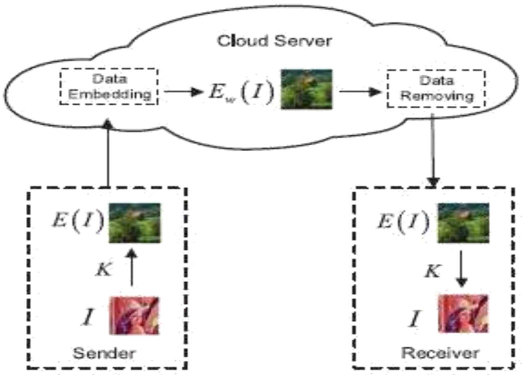

Fig..6: Framework RIT [23]

4.3. Key Modulation [18]

Reversible Data Hiding is also done by using Key Modulation [18] where hiding of data is done in encrypted images. In this technique the data hiding is done by using the public key modulation without access to the encryption key. In the public key modulation dat hiding is done by simple XOR operation.

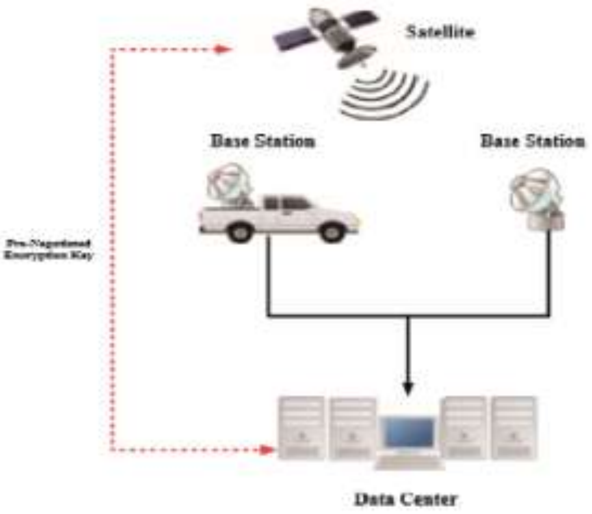

Fig.7: Example of Key Modulation. [18]

In secure remote sensing (fig.7)[18], the satellite images are captured by on-board cameras. After encrypting that captured images sent to the base station(s). Base station then hides some confidential data such as base station ID, Time of Arrival, wind information etc. into that encrypting images. The data center get this encrypted image and do some investigations and stored it. The base station not having any secrete key. All the process done through public network. The data center and satellite only having secrete key [18].

4.4. Distributed Source Encoding [20]

The reserving Room Before Encryption technique [13] for RDH is sometimes impractical because the sender need to do extra RDH before encryption where sender has no idea which data hiding strategy is done by data hider. The sender done space reservation and embedding task, So data hider becomes redundent. To vanish these problemes distributed source coding technique for RDH is used. The Distributed Source Encoding uses MSB bits and Slepian-Wolf Encoding. The data hider embeds data into encrypted image by decomposing image. The decomposing technique is given in followed Fig. 8.

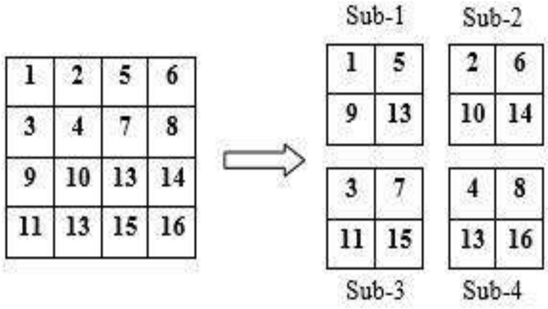

Fig.8: Image Decomposition Technique [20].

The distributed Source Encoding technique[20] is based on three phases as shown in Fig. 9 that is sender pahse, data hider phase and receiver phase. In sender phase sender encrypts the original image using stream cipher and encryption key. The encrypted image is passed to data hider phase. In data hider phase MSB bits are selected for data embedding by using Slepian- Wolf Encoding. The receiver phase contains encrypted image along with secrete data. The DSC technique is consider to be separable reversible data hiding. Because if receiver have only encryption key then approximate image is obtained. If the receiver have both encryption key and embedding key then original image and secrete data is obtained.

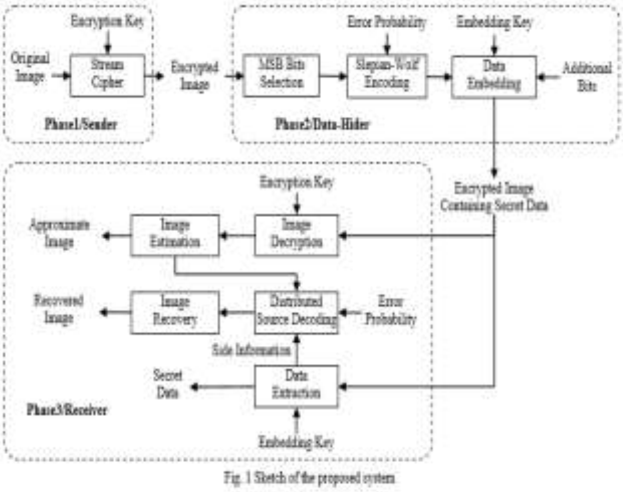

Fig.9: Flowdiagram of Distributed Source Encoding [20]

5. Conclusion

Reversible Data Hiding in encrypted images is a method in which data hiding is done along with lossless extraction of data and cover media. Different techniques are used to satisfy requirement according to embedding capacity and image quality. Reserving Room before Encryption is a technique which gives better image quality after extraction but it gives less embedding capacity. Key Modulation, Distributed Source Encoding and Pitch-level Sparse Rep-resentation are techniques useful for large payload and extraction of image without loss, But encrypted image is in the form of ciphertexts so it gives lack of security. Reversible Image Transformation is a techniques used for Reversible Data Hiding in encrypted images which gives better image quality after extraction and large embedding capacity. RIT gives encrypted image is not in the form of ciphertext, So it avoids the attention of curious cloud which spoils the security. Therefor RIT-based framework is better than other techniques.

References

[1] http://fourier.eng.hmc.edu/e161/lectures/e161ch1.pdf.

[2] Shilpa Sreekumar, Vincy Salam, Advanced Reversible Data Hiding With Encrypted Data, International Journal of Engineering Trends and Technology (IJETT) Volume 13 Number 7 Jul 2014.

[3] https://www.mepits.com/project/337/Project-Ideas/Unified-Data-Embedding-and-Scrambling-Scheme:–Matlab-based-project

[4] http://what-when-how.com/introduction-to-video-and-imageprocessing/point-processing-introduction-to-video-and-imageprocessing- part-4/

[5] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, Reversible watermarking algorithm using sorting and prediction, IEEE Trans. on Circuits and Systems for Video Technology, vol.19, no.7, pp. 989- 999, Jul. 2009.

[6] B.ou, X. Li, Y. Zhao, R. Ni, Y. Shi, Pairwise prediction-error expansion for efficient reversible data hiding, IEEE Trans. on Image Processing, vol. 22, no.12, pp. 5010-5021, Dec. 2013.

[7] Ioan-Catalin Dragoi, Dinu Coltuc, Local-prediction-based difference expansion reversible watermarking, IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014.

[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei, Reversible data hiding, IEEE Trans. on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362, Mar. 2006.

[9] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. on Circuits and Systems for Video Technology, vol. 13, no.8, pp. 890-896, Aug. 2003.

[10] X. Hu, W. Zhang, X. Li, N. Yu, Minimum rate prediction and optimized histograms modification for reversible data hiding, IEEE Trans. on Information Forensics and Security, vol. 10, no. 3, 653-664, Mar. 2015.

[11] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, F. Li, Fast estimation of optimal marked-signal distribution for reversible data hiding, IEEE Trans. on Information Forensics and Security, vol. 8, no. 5, pp. 779-788, May. 2013.

[12] W. Zhang, X. Hu, N. Yu, Optimal transition probability of reversible data hiding for general distortion metrics and its applications, IEEE Trans. on Image Processing, vol. 24, no. 1, pp. 294-304, Jan. 2015.

[13] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. on Information Forensics and Security, vol. 8, no. 3, pp. 553-562, Mar. 2013.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, On compressing encrypted data, IEEE Trans. On Signal Processing, vol. 52, no. 10, pp. 2992-3006, Oct. 2004.

[15] W. Liu, W. Zeng, L. Dong, and Q. Yao, Efficient compression of encrypted grayscale images, IEEE Trans. on Image Processing, vol. 19, no. 4, pp. 1097-1102, Apr. 2010.

[16] X. Zhang, Reversible data hiding in encrypted images, IEEE Signal Processing Letters, vol. 18, no. 4, pp. 255-258, Apr. 2011.

[17] W. Hong, T. Chen, H. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199-202, Apr. 2012.

[18] J. Zhou, W. Sun, L. Dong, et al., Secure reversible image data hiding over encrypted domain via key modulation, IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.

[19] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.

[20] Z. Qian, and X. Zhang, Reversible data hiding in encrypted image with distributed source encoding, IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.

[21] W. Zhang, K. Ma and N. Yu, Reversibility improved data hiding in encrypted images, Signal Processing, vol. 94, pp. 118-127, Jan. 2014.

[22] X. Cao, L. Du, X. Wei, et al., High capacity reversible data hiding in encrypted images by patch-level sparse representation, IEEE Trans. on Cybernetics, vol. 46, no. 5, pp. 1132-1143, May. 2016.

[23] Weiming Zhang, Hui Wang, Dongdong Hou, Nenghai Yu et al., Reversible Data Hiding in Encrypted Images by Reversible Image Transformation, IEEE Trans. on Multimedia, 2016.

[24] B.ou, X. Li, Y. Zhao, R. Ni, Y. Shi, Pairwise prediction-error expansion for efficient reversible data hiding, IEEE Trans. on Image Processing, vol. 22, no.12, pp. 5010-5021, Dec. 2013.

[25] Y. Lee and W. Tsai,A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformation, IEEE Trans. on Circuits and Systems for Video