DISCRETE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BASED ON TWO-DIMENSIONAL HISTOGRAM ADJUSTMENT

V.V. Vinoth
Research Scholar
Department of ECE
Bharath University, Chennai
India
E-mail:vinothvv.velaian@gmail.com

Dr. B. Karthik
Associate Professor
Department of ECE
Bharath University, Chennai,
India
E-mail: karthik.ece@bharathuniv.ac.in

Abstract- **In this paper we proposed method of completely separable reversible data hiding in encrypted images. The cover image is the first partitioned into non overlapping blocks and specific encryption is applied to obtain the encrypted images. Then, the image difference in the encrypted domain can be calculated based on the homomorphic property of the cryptosystem. The data hider, who does not know the original image content, may reversibly embed secret data into image difference based on two-dimensional difference histogram modification. Data extraction is completely separable from image decryption; that is, data extraction can be done either in the encrypted domain or in the decrypted domain, so that it can be applied to different application scenarios. In addition, data extraction and image recovery are free of any error. Experimental results demonstrate the feasibility and efficiency of the proposed scheme.**

Index Terms- **homomorphic, cryptosystem, two-dimensional difference histogram modification, separable reversible data hiding.**

I.INTRODUCTION

With the rapid developments occurring in mobile internet and cloud storage, privacy and security of personal data have gained significant attention nowadays. There are no guarantees that stored data will not be accessed by unauthorized entities, such as the cloud provider itself or malicious attackers.Under these specific circumstances, sensitive images, such as medical and personal images, need to be encrypted before outsourcing for privacy- preserving. In other words, the consumers would like to give the un trusted cloud server only an encrypted version of the data instead of the original content. The cloudservice provider (who stores the data) is not authorized to access the original content (i.e., plaintext). However, in some application scenarios, the cloud servers or database managers need to embed some additional messages, such as authentication or notation data, directly into an encrypted data for tamper detection or ownershipdeclaration purposes.

Over the past few years, number of schemes about data hiding in encrypted images or videos has been detected. Those researchers have been studying the possibility of hiding data directly in the encrypted domain. However, within these schemes, the host image/video is permanently distorted caused by data embedding. In general, the cloudservice provider has no right to introduce permanent distortion. This implies that, for alegal receiver, the original plaintext content should be recovered without any error after image decryption and data extraction. To solve those type of problem, we taking the reversible data hiding (RDH) in theencrypted domain.

RDH is a technique that slightly alters digital media (e.g., images or videos) to embed secret data while the original digital media can be recovered without any error after the hidden messages have been extracted. This data hiding technique is used to some important and sensitive areas and error concealment, where the original media is required to be reconstructed without any distortion. Three major approaches that, lossless compression, histogram modification, and difference expansion, have already been developed for RDHtechnique. RDH techniques are suitable for plaintext instead of cipher text.

RDH in the encrypted domain has emerged as a new and challenging research field. In recent years,

some RDH methods for encrypted images have been proposed. In general, these methods can be divided into three categories, that is, methods by vacating room after encryption (VRAE), methods by reserving room before encryption (RRBE), and methods based on homomorphic encryption. In VRAE framework, the original signal is encrypted directly by the content owner, and the data hider embedsthe additional bits by modifying some bits of the encrypted data. The advantage of this framework is that the operation of the end user is simple and efficient.

However, as the entropy of an encrypted image has been maximized, the embedding capacity is limited. Moreover, the accuracy of data extraction and the quality of restored image are not satisfactory. The advantages of this framework are embedding capacity is relatively large and pure reversibility is achieved. But this framework might be impractical because it requires the content owner to perform an extra preprocessing before content encryption.

In general, the content owner to send only an encrypted image to the manager without extra information. With the additive homomorphic property of Paillier cryptosystem, firstly proposed a homomorphic encryption based RDH approach. Moreover, RDH in the homomorphic encrypted domain has also been investigated. In the additive homomorphic property of modulo operation is utilized to realize the RDH in the encrypted domain. The advantage is that encryption does not cause data expansion.

In this paper, we develop reliable framework for RDH in the encrypted domain. In fact, the proposed method belongs to the third category. Its main contribution is the combination of the modular addition and two-dimensional (2D) histogram modification. Its advantages are mainly manifested in four aspects. First, room for data hiding does not need to be vacated before encryption, which is more reasonable compared with the methods. Secondly, completely separable and completely reversible can be achieved, which is more reliable than the methods. Thirdly, the modular arithmetic addition operation has additive homomorphism, is utilized for image encryption. It does not cause data expansion, unlike the public-key cryptosystems. The rest of the paper is organized as follows. We describe the proposed scheme, which includes image encryption, data embedding in encrypted image, data extraction, and original image recovery.

II. PROPOSED SCHEME

In this proposed scheme, a RDH method in encrypted images is illustrated. It is composed of three parts, that is, generation of the encrypted image, generation of the marked encrypted image, data extraction, and image recovery. First, the content owner encrypts the original image with encryption key to produce an encrypted image. Then, the data hider without knowing the actual content can embed some additional data into the encrypted image. Here, the data hider can be a third party, for example, a database manager or a cloud provider, who is not authorized to access the original content of the signal (i.e., plaintext). At the receiving end, maybe the content owner himself or an authorized third party can extract the hidden data either in encrypted or decrypted image. For illustrative purposes, the framework of the proposed scheme is given in Figure 1.

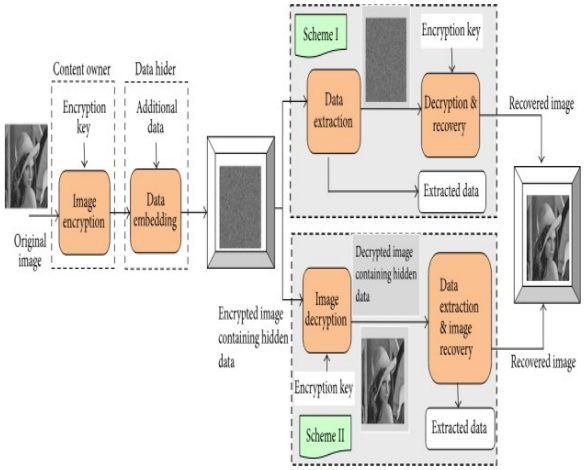


Fig.1 The framework of proposed scheme.

Image Encryption

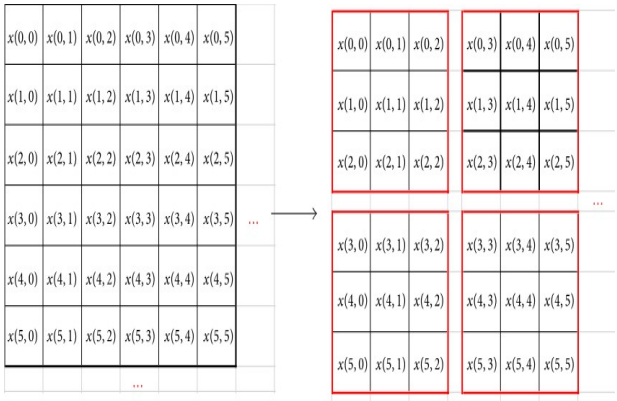


Fig.2 Example of image partition.

Assume the original image X is an 8-bit gray-scale image with size and pixels. As we know, in the plaintext image, the correlation will gradually decrease with the increase of the distance between two pixels. In order to make good use of the correlation among pixels for RDH, the cover image is divided into a number of nonoverlapping blocks of size as shown in Figure 2. If both M and N can be divisible by 3, the number of nonoverlapping blocks is (M/3) × (N/3). If M or N cannot be divisible by 3, the image is divided into [M/3] × [N/3] blocks, including [M/3] × [N/3] blocks of size 3 × 3. Here, [M/3] denotes the smallest integer greater than or equal to M/3, and [M/3] denotes the greatest integer less than or equal to M/3.

Data Embedding in Encrypted Image

After receiving the encrypted image, the data hider can embed some additional information into it for the purpose of media notation or integrity authentication. To achieve reversibility, the idea of histogram shifting is introduced in cipher text based on homomorphic encryption. The process consists of two types, namely, difference histogram generation and difference histogram modification.

According to the above proof, the correlation between the neighboring pixels in the local area of the plaintext image is preserved; that is, the difference remains unchanged even after encryption. All other 3×3 blocks can be processed in the samemanner.

(1) Difference Histogram Generation:

Before performing the data embedding operation, a two-dimensional difference histogram of the encrypted image needs tobe generated. The detailed procedure can be described as follows.

Step1. Divide the encrypted image into nonoverlapping 3 × 3 blocks, which is the same as Figure 2. If the width or height of the image is not a multiple of 3, then the edge block will be ignored during the data embedding process.

Step2. Calculate the difference between the basic pixel and the remaining pixels in each 3 × 3 block.

Step3. Generate the difference histogram using differences in each 3 × 3 block. There is a high degree of correlation between adjacent pixels in a local region of an image. That is, they have similar gray values, or even the same gray value. Thus, the resulting difference histogram has a higher peak than the histogram of the original image. To demonstrate the distribution of the image difference, the histograms of some residual images are shown in Figure 3. It is clearly seen that the distribution is approximately symmetrical.

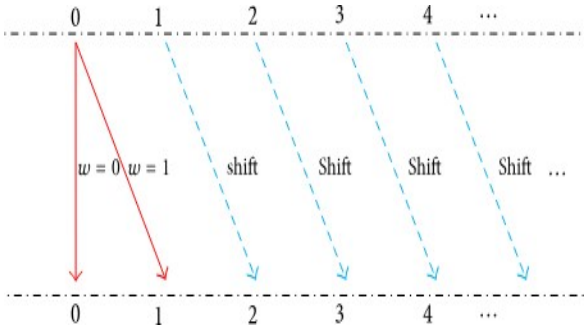
(a) Lena

(b)Tank

Fig. 3 1D histogram of image difference.

(2) Difference Histogram Modification:

When the difference histogram is generated, reversible data hiding can be accomplished by using histogram shifting method.



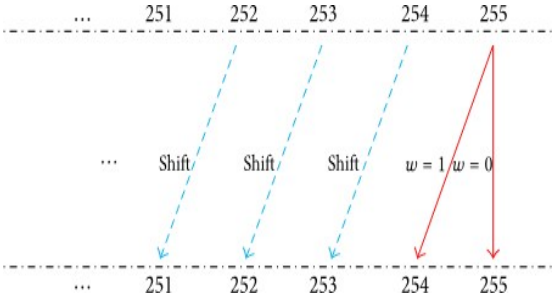


Fig. 4 Illustration of the 1D histogram modification.

For example, histogram modification in Figure 5 is in fact equivalent to the one shown in Figure 6.

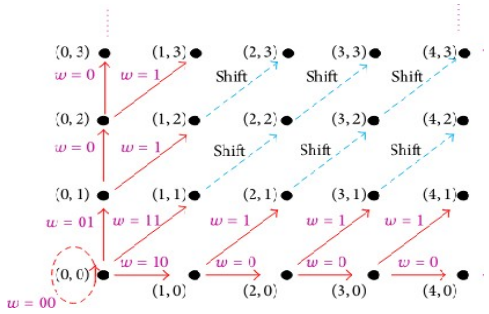


Fig 5. Illustration of the 2D histogram modification.

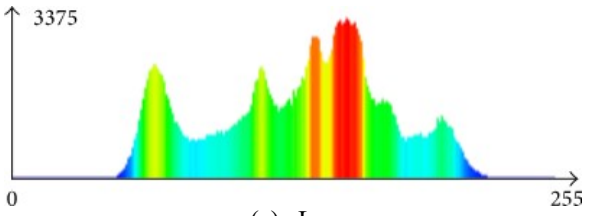
Data Extraction and Original Image Recovery

In this scheme, data extraction and image decryption are completely separable. Inother words, the hidden data can be extracted either in encrypted or in decrypted domain. Our method is also reversible, where the hidden data could be removed to obtain the original image. We will first discuss the extraction in the encrypted domain

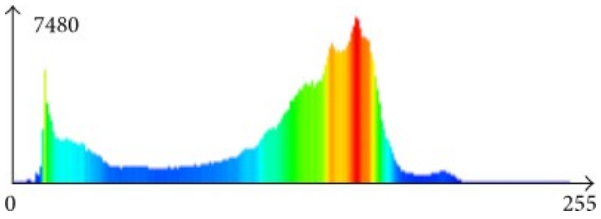
III.EXPERIMENTAL RESULTS

Scrambling Effect and Security Analysis

For an image encryption scheme, the security depends on cryptographic security and perceptual security. Cryptographic security denotes the security against cryptographic attacks, which relies on the underlying cipher. The pseudo-random sequence is used to encrypt image. Figure 8 illustrates the histogram of the original image. The corresponding histogram is shown in Figure . By comparing Figures 6 and 7, it can be observed that the modified distribution appears to be uniform, which suggests that a statistical analysis would not be effective for evaluating the originalcontent.



(a) Lena



(b) Boats

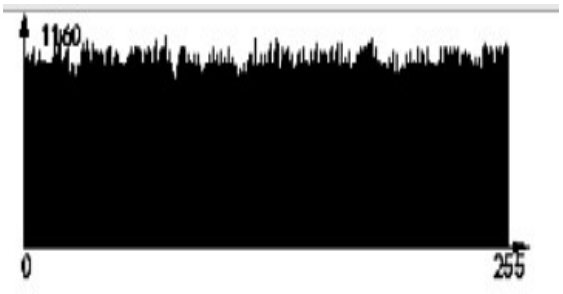


Fig.5 Histogram of the original image

(a) Lena

(b) Boats

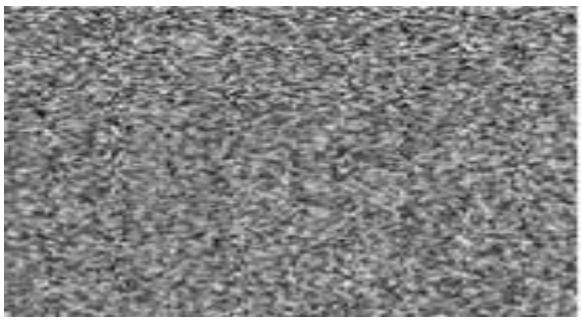
Fig.7 Histogram of the correspondingencrypted image.

The original images are given in Figure 8, and their corresponding encrypted results are shown in Figure 9.

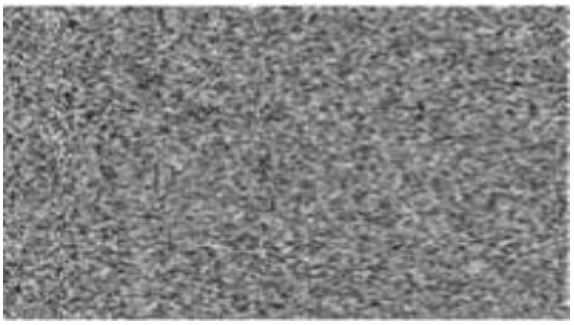
(a) Lena

(b) Boat

Fig. 8 Original images.



(a) Lena (9.53 dB)



(b) Boats (9.11 dB)

Fig.9 The corresponding encryptedimages.

Visual Quality of Marked and Decrypted Image

Since the embedding scheme is reversible, the original cover content can be perfectly recovered after extracting the hidden data. In some scenarios, the encrypted image containing the hidden data provided by the server needs to be decrypted by the authorized user. Therefore, the visual quality of the decrypted image containing the hidden data is also expected to be equivalentor very close to that of the original image. Inother words, the degradation of the image quality should be maintained at an acceptable range, even if the hidden data has not been removed. In the proposed method, since the maximum change in pixel value is 2, the artifacts introduced will not be perceptible. To verify this, a series of tests have been conducted. The original images and their corresponding decrypted versions containing the hidden data are shown in Figures. From our subjective examination, itis concluded that the marked content cannot be visually distinguished from nonmarked content. In addition to subjective observation, PSNR values are also given in Figure 8. In addition to Zelda, PSNR values of the remaining images are all above 47 dB. Generally, it is almost impossible to detect the degradation in image quality caused by data hiding.

(a) Lena (47.29 dB)

(b) Boats (47.27 dB)

Fig.10 Decrypted images containing the hidden data

IV.COMPARISON AND DISCUSSION

Taking Lena and Boats as an example, the performance comparison of different embedding rates is given in Figure 10. Obviously, the proposed method can provide better performance when the embedding capacity exceeds the maximum capacity of one-layer embedding strategy.

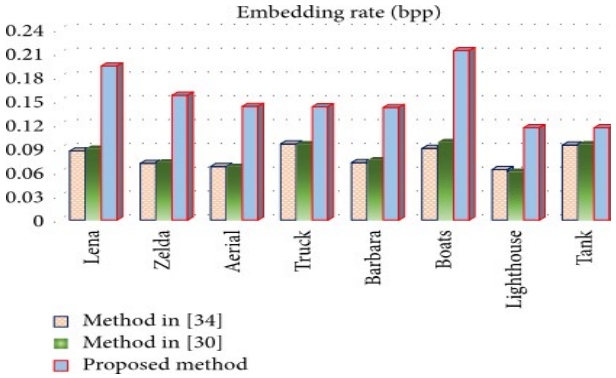
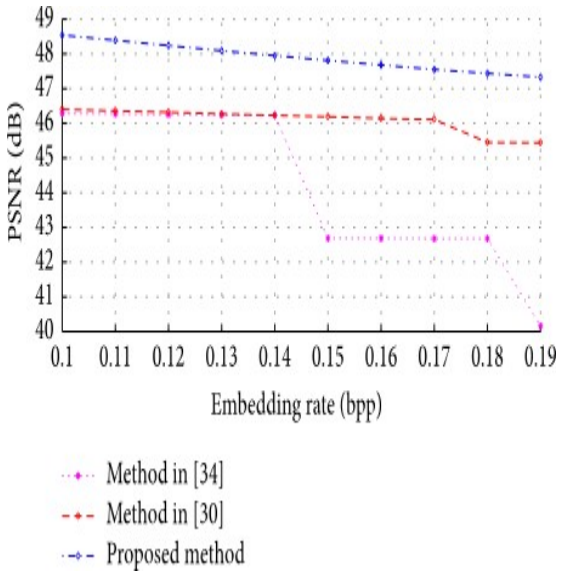
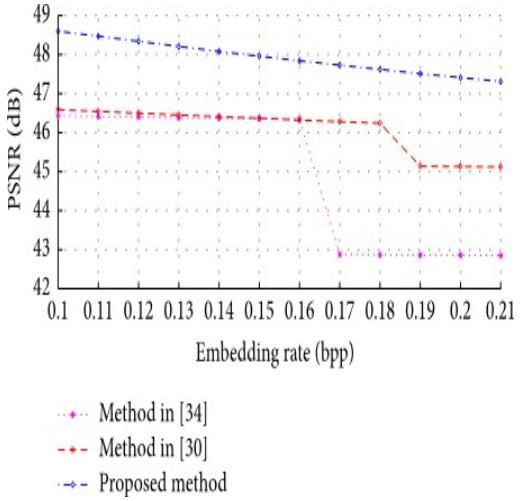


Fig.11 The comparison results ofembedding capacity.



(a) Lena



(b) Boats

Fig.12 The performance comparison of different embedding rates.

V.CONCLUSION

In this paper, an algorithm to reversibly embed secret data in encrypted images ispresented. A specific modulo operation is utilized to encrypt the image, which can preserve some correlation between the neighboring pixels. With the preserved correlation, the data hider can embed thesecret data into the encrypted image by using 2D histogram modification, even though he does not know the original image content. Since the embedding process is done on encrypted data, our scheme preserves the confidentiality of content. Data extraction is separable from image decryption; that is, the additional data can be extracted either in the encrypted domain or in the decrypted domain. Furthermore, this algorithm can achieve real reversibility and high quality of marked and decrypted images. One of the possible applications of this method is image annotation in cloud computing where high image quality and reversibility are greatly desired.

REFERENCES

[1] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016. View at Publisher · View at Google Scholar · View at Scopus

[2] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2594–2608,2016. View at Publisher · View at Google Scholar

[3] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: a review of its benefits and open issues," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 87–96, 2013. View at Publisher · View at Google Scholar · View at Scopus

[4] B. Zhao, W. Kou, H. Li, L. Dang, and J. Zhang, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Information Sciences, vol. 180, no. 23, pp. 4672–4684, 2010. View at Publisher · View at Google Scholar · View at MathSciNet · View at Scopus

[5] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," Journal of Visual Communication and Image Representation, vol. 30, pp. 125–135, 2015. View at Publisher · View at Google Scholar View at Scopus

[6] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000 images," IEEE Transactions on Multimedia, vol. 14, no. 3, pp. 703–716, 2012. View at Publisher · View at Google Scholar · Viewat Scopus

[7] H. Liu, D. Xiao, R. Zhang, Y. Zhang, and S. Bai, "Robust and hierarchical watermarking of encrypted images based on Compressive Sensing," Signal Processing: Image Communication, vol. 45, pp. 41–51, 2016. View at Publisher · View at Google Scholar · View at Scopus

[8] D. Xu, R. Wang, and Y. Q. Shi, "Data hiding in encrypted H.264/AVC video streams by codeword substitution," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 596–606, 2014. View at Publisher · View at Google Scholar View at Scopus

[9] D. Xu and R. Wang, "Context adaptive binary arithmetic coding-based data hiding in partially encrypted H.264/AVC videos," Journal of Electronic Imaging, vol. 24, no. 3,Article ID 033028, 2015. View at Publisher View at Google Scholar · View at Scopus

[10] D. Xu, R. Wang, and Y. Q. Shi, "An improved scheme for data hiding in encrypted H.264/AVC videos," Journal of Visual Communication and Image Representation, 2015. View at Publisher · View at Google Scholar · View at Scopus

[11] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–361, 2006. View at Publisher · View at Google Scholar · View at Scopus

[12] D. Xu, R. Wang, and Y. Q. Shi, "An improved reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," Journal of Visual Communication and Image Representation, vol. 25, no. 2, pp. 410–422, 2014. View at Publisher · View at Google Scholar · View at Scopus

[13] D. Xu and R. Wang, "Two-dimensional reversible data hiding-based approach for intra-frame error concealment in H.264/AVC," Signal Processing: Image Communication, vol. 47, pp. 369–379, 2016. View at Publisher · View at Google Scholar. View at Scopus

[14] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," EURASIP Journal on Applied Signal Processing, vol. 2, pp. 185–196, 2002. View at Google Scholar

[15] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding-new paradigm in digital watermarking," EURASIP Journal on Applied Signal Processing, vol. 2, pp. 185–196, 2002. View at Google Scholar

Publisher · View at Google Scholar · View at MathSciNet View at Scopus

[16] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 890– 896, 2003. View at Publisher · View at Google Scholar · View at Scopus

[17] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," IEEE Access, vol. 4, pp. 3210–3237, 2016. Viewat Publisher · View at Google Scholar · View at Scopus

[18] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Processing Letters, vol. 18, no. 4, pp. 255–258, 2011. View at Publisher · View at Google Scholar View at Scopus

[19] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202, 2012. View at Publisher · View at Google Scholar · View at Scopus

[20] C. Qin and X. Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content," Journal of Visual Communication and Image Representation, vol. 31, pp. 154–164, 2015. View at Publisher · View at Google Scholar ·