A Secure and Privacy-Preserving Technique Based on Contrast-Enhancement Reversible Data Hiding and Plaintext Encryption for Medical Images

Yang Yang, Xingxing Xiao, Xue Cai, and Weiming Zhang

***Abstract*—Protection of medical data has become a prerequisite in medical imaging clouds due to the semi-trusted cloud. Aiming at preserving patients' privacy and increasing the security of medical images in the cloud, this letter proposes a secure and privacy-preserving technique which provides a new security mechanism for medical data. In this technique, a novel reversible data hiding (RDH) based on adaptive texture classification is proposed to embed privacy data into medical images for preserving patients' privacy and improving image quality, and plaintext encryption is proposed to encrypt the marked medical image into the similar image of target image for increasing image security. Extensive experiments have shown that the proposed RDH is better than other RDH methods. Plaintext encryption can reduce the attacker's attention and increase the security of medical images well.**

***Index Terms*—Reversible data hiding, plaintext encryption, contrast enhancement, security, preserve privacy, medical images.**

I. Introduction

MEDICAL imaging clouds are significant in medical industry [1]. Due to semi-trusted clouds, there are security problems of medical data. Medical records and medical images contain sensitive patients' medical privacy and they are facing threats of data security. Hence, a secure and privacy-preserving technique is needed urgently.

Reversible data hiding (RDH) [2]–[4] is a data hiding technique which is the perfect recovery of the cover image and the hidden data. There are already classical RDH algorithms in [5]–[14]. For improving the quality of images, RDH methods with contrast enhancement (RDH-CE) [15]–[18] are proposed later. Wu *et al.* [16] selected two highest bins of image's gray histogram to embed data. On Wu's basis, Gao *et al.* [17] added the wavelet domain to embed data. Yang *et al.* [18] proposed that data was embedded into region of interest (ROI) and region of non-interest (NROI) respectively. The flaw of these methods is that the contrast of images is not obvious at the low embedding rate. RDH with obvious contrast enhancement is required whether at the low or high embedding rate. For the sake of image security and data protection, RDH combined with encryption [19]–[23] is proposed. At present, the scheme of RDH in the encrypted image is the way of RDH after encryption. Different from natural images, the data embedded into a medical image is not limited to information about owner and authentication, but also contains patient's medical records. What's more, it involves a great deal of privacy and is easier to be leaked. Hence, data should be first embedded into medical image to preserve patients' privacy, which can avoid mismatches and save storage space. In this letter, a secure and privacy-preserving technique based on RDH-CE and plaintext encryption is proposed for medical images. There are three main contributions: (1) propose a novel RDH-CE based on adaptive texture classification for privacy preserving and medical image quality improvement; (2) propose a new idea: plaintext encryption for increasing medical image security; (3) propose a new framework which provides a secure and privacy-preserving mechanism for medical data.

The rest of letter is organized as follows. Section II introduces the proposed technique. Section III shows experiments. And Section IV describes the conclusion.

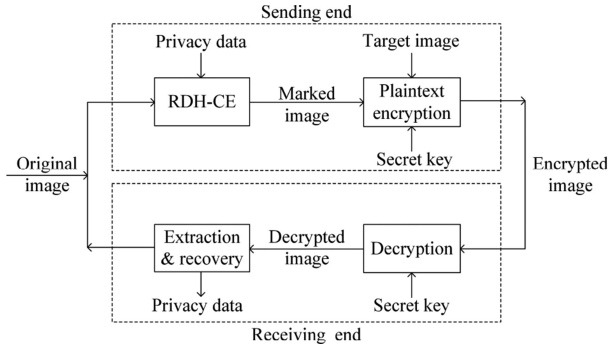

Fig. 1. The framework of the proposed technique.

II. Proposed Method

In order to preserve patients' privacy and increase the security of medical images, the letter proposes a secure and privacy-preserving technique. The proposed technique consists of four stages in Fig. 1: RDH-CE based on adaptive texture classification, plaintext encryption, decryption, extraction and recovery.

A. RDH-CE Based on Adaptive Texture Classification

In medical images, the lesion is important diagnostic bases and it is so obvious mutations that the structure and density

Manuscript received November 17, 2019; revised January 6, 2020; accepted January 7, 2020. Date of publication January 10, 2020; date of current version February 12, 2020. This work was supported in part by the Natural Science Foundation of China under Grant 61502007 and Grant 61572452 and in part by the Natural Science Research Project of Anhui province under Grant 1608085MF125. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Roberto Caldelli. *(Corresponding author: Yang Yang.)*

Y. Yang, X. Xiao, and X. Cai are with Anhui University, Hefei 230601, China (e-mail: sky_yang@ahu.edu.cn; xiaoxingxingaabb@163.com; cedartsia@163.com).

W. Zhang is with the University of Science and Technology of China, Hefei 230027, China (e-mail: zhangwm@ustc.edu.cn).

Digital Object Identifier 10.1109/LSP.2020.2965826

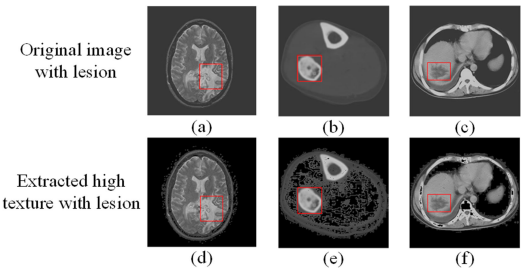

Fig. 2. Original images and extracted high texture with lesion.

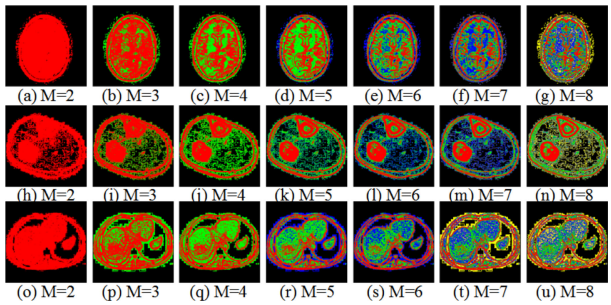

Fig. 3. Texture classification.

of lesions are significantly different from the normal region. In other word, the texture of the lesion is significantly higher. As shown in Fig. 2, the lesion region belongs to high texture region. With contrast enhancement of the high texture region, the visual quality of medical image is improved. To improve medical image quality and satisfy the higher embedding rate for medical images, RDH-CE based adaptive texture classification is proposed to embed data into the empty bins of the high texture region's stretched histogram and into low texture region by one-direction histogram shifting (HS) from left to right.

1) Texture Classification: Inspired by complexity measurement [9], we class pixels into different texture grades by complexity measurement. Because texture grade M affects image texture classification. The bigger M is, the more precise texture classification is, but the larger capacity of the location map is for recording classification's status. It is worth noting that the location map needs to be embedded as auxiliary information for recovery. Hence, we propose adaptive texture classification method to decide the optimal M. The range of M is 2 to 8 and the optimal M is introduced in Section III-A. To reduce auxiliary information, we class M texture grades into the high texture and the low texture further by Eq. (1).

$$\begin{cases} h_{high}(n) = \begin{cases} \left\{1 \le k \le N : n_k \ge \frac{M}{2}\right\}, & \text{if } M \bmod 2 = 0 \\ \left\{1 \le k \le N : n_k \ge \frac{M-1}{2}\right\}, & \text{if } M \bmod 2 = 1 \end{cases} \\ h_{low}(n) = \begin{cases} \left\{1 \le k \le N : n_k < \frac{M}{2}\right\}, & \text{if } M \bmod 2 = 0 \\ \left\{1 \le k \le N : n_k < \frac{M-1}{2}\right\}, & \text{if } M \bmod 2 = 1 \end{cases} \end{cases} \tag{1}$$

In which $h_{high}(n)$ and $h_{low}(n)$ are sets of pixels in the high and low texture region respectively, N is the number of image's pixel, k is the k-th pixel, n_k is the k-th pixel's complexity. As shown in Fig. 3, the image is classed into the high and low texture region by an operation of texture classification. Black pixels denote the low texture, and colorful pixels denote the high texture.

2) Embedding Data Into the High Texture Region: The contrast enhancement by [16]–[18] is not obvious at low embedding rate. To enhance contrast, the entire image is first stretched to achieve obvious contrast enhancement whether at low or high embedding rate. Data is sequentially embedded into the empty bins of the stretched histogram as the descending order of texture, which can avoid overflow problems. The histogram achieves an uniform distribution by embedding data into the highest bins and the contrast of marked image is enhanced further, which is similar to histogram equalization for contrast enhancement.

① The original pixel I_o will be stretched to I by Eq. (2).

$$I = round\left[(L_{\max} - L_{\min}) * \frac{I_o - I_{\min}}{I_{\max} - I_{\min}}\right] \tag{2}$$

In which $L_{\min} = 0$ and $L_{\max} = 255$ generally. As a result, $[I_{\max}, I_{\min}]$ in the original image are stretched to $[L_{\max}, L_{\min}]$.

② The modified pixel I'_h in high texture region is modified by Eq. (3).

$$\mathrm{I}'_h = \begin{cases} I_h + b_i, & \text{if } I_h = I_{hm} \&\& 0 \le I_h \\ & \quad \le 126 \&\& h(I_h + 1) = 0 \\ I_h - b_i, & \text{if } I_h = I_{hm} \&\& 129 \le I_h \\ & \quad \le 255 \&\& h(I_h - 1) = 0 \\ I_h, & \text{if } I_h \ne I_m \end{cases} \tag{3}$$

In which I_{hm} is pixel value of peak bin in the high texture region's histogram. $b_i \in \{0, 1\}$ is the secret data to be embedded. $h(I_h)$is the number of pixel I_h in the gray histogram.

③ Repeat step ② until there is no empty bin to embed or all data is embedded into the high texture region. I_{hm} in each round is embedded as a part of data in the next round. And I_{hm} in the last round is regarded as the auxiliary information.

3) Embedding Data Into the Low Texture Region: To increase the embedding rate, the rest of data is embedded into the low texture region by one-direction HS from left to right.

① Preprocess: $I_i = I_{io} - L_{\min}$, where I_{io} denotes the unmarked pixel and I_i denotes preprocessed pixel, in the low texture region.

② Data is embedded by Eq. (4) repeatedly until all data is embedded into image. The marked pixel I'_i in low texture region is calculated via

$$I'_i = \begin{cases} I_i + 1, & \text{if } I_i > I_{im} \\ I_i + b_i, & \text{if } I_i = I_{im} \\ I_i, & \text{others} \end{cases} \tag{4}$$

Where I_{im} denotes pixel value of peak bin in the low texture region's histogram.

To achieve reversibility, the auxiliary information, such as M, $I_{\max}$, $I_{\min}$, $L_{\max}$, $L_{\min}$, I_{hm} and I_{im} in the last round, and the location maps, is first compressed by [24]. Then, compressed information is embedded into the four sides of image without first 16 pixels, as the embedding process of low texture region. The peak bin's pixel value in the last round and embedding round number l are instead of the least significant bits (LSBs) of the first 16 pixels which have been embedded into image.

B. Plaintext Encryption

Traditional encryption methods [19]–[23] transform original images into unreadable code to protect image content. Protecting image's content is achieved but the intention to conceal the content has been exposed, which easily attracts the attacker's curiosity and attention. For reducing attackers' attention and

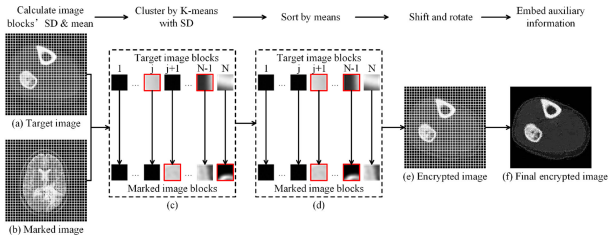

Fig. 4. Flow diagram of plaintext encryption.

increasing the security of images, this letter proposes plaintext encryption to transform an image into another image with visual meaning. Different from traditional encryption methods, the characteristic of plaintext encryption is that the encrypted image is still visually meaningful and reduces attackers' attention. Fig. 4 shows plaintext encryption's flow diagram.

1) Calculate the Mean and Standard Deviation (SD) Divide the Marked and Target Image Into N Blocks Respectively. Calculate Each Block's u and σ: $u = \frac{1}{m*n}\sum_{i=1}^{n*m} p_i$, $\sigma = \sqrt{\frac{1}{m*n}\sum_{i}^{n*m}(p_i - u^2)}$ *Where the Size of Image Block is $m*n$, and p_i is i-th Pixel.:*

2) Cluster: We adopt K-means [25] which is a non-uniform clustering algorithm to cluster image block according to standard deviation. As a result, marked blocks and target blocks are clustered into K classes respectively, and marked blocks and target blocks are matched one by one in each class as Fig. 4(c).

3) Sort: It's worth noting that, for some smooth or complex blocks, their SDs are close, but their means are far. As shown in Fig. 4(c), the target block and marked block are matched in the j-th column. To be close to target block, pixels in marked block need to be shifted and shifted values need to be embedded as auxiliary information. Due to the large mean difference between marked block and target block, the auxiliary information increases. To reduce auxiliary information, we further sort blocks which are in the same class according to mean value. As shown in Fig. 4(d), matched blocks have not only similar SD but also similar mean value. The auxiliary information has reduced.

4) Shift and Rotate: To approach the target block, marked pixel p_i needs to shift to obtain encrypted pixel by $p_i'' = p_i + \Delta u$, where the value of shifting $\Delta u = round(u' - u)$, u' and u are the means of target and marked blocks respectively. Note that the encrypted pixel p'' should be an integer at the range from 0 to 255. To avoid the overflow or underflow problem, we modify Δu by reducing the maximum overflow or underflow value. Next, we quantize Δu by Eq. (5) to reduce bits. Finally, we use $\Delta u'' = \frac{|\Delta u'|}{4}$ to record for reducing bits further.

$$\Delta u' = \begin{cases} 8 * round\left(\frac{\Delta u}{8}\right), & \text{if } \Delta u > 0 \\ 8 * floor\left(\frac{\Delta u}{8}\right) + 4, & \text{if } \Delta u < 0 \end{cases} \tag{5}$$

To make the encrypted image more similar to the target image, rotate each marked block into one of the four directions 0°, 90°, 180° or 270° and choose the optimal direction which makes the minimum root mean square error [26] between the rotate version and the corresponding target block.

5) Embed Auxiliary Information: To decrypt perfectly, auxiliary information, such as N, K, the matching index, values of shifting and rotating, is embedded into images. It's worth noting that auxiliary information should be first compressed by [24], then encrypted by advanced encryption standard into the secret sequence with the secret key before embedded.

C. Decryption

The third party with right, such as doctors and patient, can read images' content with the secret key after downloading images. Decryption is the inverse process of encryption as:

① Extract the secret sequence as [11]'s extracting process.
② Decrypt the secret sequence with the secret key.
③ Decompress to obtain the auxiliary information, such as N, K the matching index, the values of rotating and $\Delta u''$, recover $\Delta u'$ from $\Delta u''$.
④ Divide the encrypted image into N blocks, rotate and shift inversely.
⑤ Restore the image blocks to generate the marked image according to the matching index.

D. Extraction and Recovery

When doctors want to know about patient's previous medical history or patient wants to know the diagnostic results, they can extract data from medical image and recover image. The steps of extraction and recovery are as follows:

① Read LSBs of first 16 pixels in four sides of image to obtain the peak bin's pixel value in the last round and l. Extract data by Eq. (6) and recover pixels in four sides of image by Eq. (7) and (8). Decompress extracted data to obtain auxiliary information. The image is divided into the high and low texture region through the location map of texture classification.

$$b_i = \begin{cases} 1, & \text{if } I_i' = I_{im} + 1 \\ 0, & \text{if } I_i' = I_{im} \end{cases} \tag{6}$$

$$I_i = \begin{cases} I_i' - 1, & \text{if } I_i' > I_{im} \\ I_i', & \text{others} \end{cases} \tag{7}$$

$$I_{io} = I_i + L_{\min} \tag{8}$$

② In the low texture region, data is extracted by Eq. (6). Pixels of low texture region are recovered by Eq. (7) and (8).
③ In the high texture region, data is extracted by Eq. (9) and pixels of high texture region are recovered by Eq. (10).

$$b_i = \begin{cases} 1, & \text{if } 0 \le I_h' \le 126 \&\& I_h' = I_{hm} + 1 \\ 1, & \text{if } 129 \le I_h' \le 255 \&\& I_h' = I_{hm} - 1 \\ 0, & \text{others} \end{cases} \tag{9}$$

$$I_h = \begin{cases} I_h' - 1, & \text{if } 0 \le I_h' \le 126 \&\& I_h' = I_{hm} + 1 \\ I_h' + 1, & \text{if } 129 \le I_h' \le 255 \&\& I_h' = I_{hm} - 1 \\ I_h', & \text{others} \end{cases} \tag{10}$$

④ I_o is restored from I by

$$I_o = round\left[\frac{I}{L_{\max} - L_{\min}} * (I_{\max} - I_{\min}) + I_{\min}\right] \tag{11}$$

III. Experimental Results

Extensive experiments have done on medical images from [27]. Due to the space limitation, we choose 3 groups of medical images which represent lesions in different body parts, such as brain, abdomen and femur. And each group chooses 6 images randomly to show the experimental results.

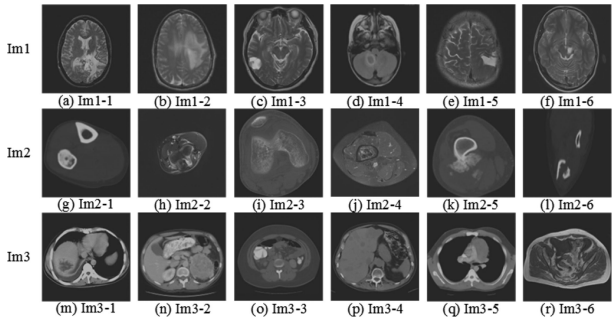

Fig. 5. Original images.

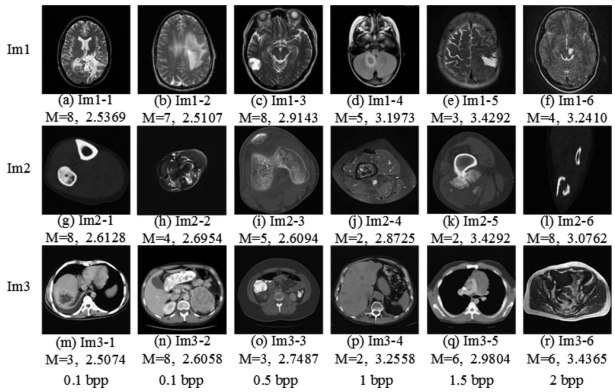

Fig. 6. Marked images at different embedding rates.

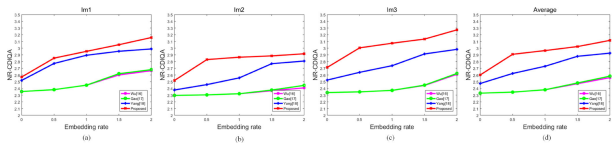

Fig. 7. The average NR-CDIQA when comparing the proposed RDH-CE with other RDH-CE methods.

A. Experimental Results of RDH-CE

We use no-reference contrast distortion image quality assessment (NR-CDIQA) [28] as image quality assessment. This section discusses the optimal value of M, marked images, and compares the proposed RDH with Wu [16], Gao [17] and Yang [18]'s methods which also are RDH-CE at different embedding rates respectively. NR-CDIQA [28] is a no-reference image quality assessment method for contrast enhancement and it was proposed based on the principle of natural scene statistics. The higher NR-CDIQA is, the better quality of images is. In addition, due to the calculation of NR-CDIQA value is related to the texture, this method takes NR-CDIQA as the standard to decide the optimal M value. Calculate NR-CDIQA value of each marked image from $M = 2$ to $M = 8$ and select the marked image with the highest NR-CDIQA. As a result, M that makes NR-CDIQA value highest is the optimal M. Fig. 6 shows marked images with the optimal M and NR-CDIQA at different embedding rates. Compared with original images (Fig. 5), the quality of marked images is obviously improved. Fig. 7 shows the average NR-CDIQA value of each group and all testing images by different methods. It shows that contrast enhancement of the proposed RDH-CE is better than that of other methods whether at high or low embedding rate.

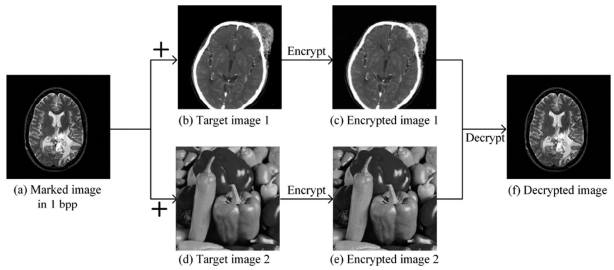

Fig. 8. Images by plaintext encryption.

TABLE I
THE AVERAGE VALUE OF PSNR AND $|\rho_{xy}|$ BY PLAINTEXT ENCRYPTION

Image group	Encrypted image	PSNR		$\|\rho_{xy}\|$	
		Marked	Target	Marked	Target
Im1	Encrypted 1	12.1834	28.1173	0.3399	0.9440
	Encrypted 2	8.5721	26.0815	0.2152	0.9569
Im2	Encrypted 1	9.9121	27.3402	0.3865	0.9811
	Encrypted 2	8.4103	27.7438	0.2057	0.9564
Im3	Encrypted 1	10.4269	26.5289	0.3352	0.9614
	Encrypted 2	7.8314	27.0110	0.1217	0.9508
All	Encrypted 1	10.8408	27.3288	0.3539	0.9622
	Encrypted 2	8.2713	26.9454	0.1809	0.9547

B. Experimental Results of Plaintext Encryption

To verify the performance of plaintext encryption, we discuss the subjective visual effect and objective data respectively. It is noticing that image block's size is $4 * 4$ and image blocks are clustered into 10 classes in experiments. For marked images in Fig. 6, we choose 18 medical images and 18 natural images randomly as target images in plaintext encryption. As shown in Fig. 8, the encrypted image is similar to the target image and conceals the original content completely. Attackers think that visually meaningful encrypted images are common images with no secret, so reduce the attention to these encrypted images. We use PSNR and correlation coefficient ρ_{xy} [23] to display experimental results from objective data. We calculate 36 pairs images' PSNR and ρ_{xy} value. Table I shows the average PSNR and $|\rho_{xy}|$ value of each group and all images respectively. The column of "marked" donates comparison of encrypted image with marked image and the column of "target" donates comparison of encrypted image with target image. We can summarize that the encrypted image is quite different from the marked image and there is no correlation between the encrypted and marked image.

IV. CONCLUSION

In this letter, we propose a secure and privacy-preserving technique for medical images. RDH-CE based on adaptive texture classification first embeds privacy data into medical images reversibly to preserve privacy and improve image quality. Different from traditional encryption methods, plaintext encryption encrypts the marked image into the other image to reduce attackers attention and increase image security. Experiments have shown that the proposed RDH-CE is superior to other methods. Plaintext encryption can reduce the attacker's attention and increase medical image security effectively.

REFERENCES

[1] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, to be published, [Online]. Available: https://doi.org/10.1016/j.ins.2019.01.070.

[2] Y. Shi, X. Li, X. Zhang, H. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[3] H. Chen, J. Ni, W. Hong, and T.-S. Chen, "High-fidelity reversible data hiding using directionally enclosed prediction," *IEEE Signal Process. Lett.*, vol. 24, no. 5, pp. 574–578, May 2017.

[4] J. Qin and F. Huang, "Reversible data hiding based on multiple two-dimensional histograms modification," *IEEE Signal Process. Lett.*, vol. 26, no. 6, pp. 843–847, Jun. 2019.

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

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

[7] B. Ou, X. Li, W. Zhang, and Y. Zhao, "Improving pairwise PEE via hybrid-dimensional histogram generation and adaptive mapping selection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 7, pp. 2176–2190, Jul. 2019.

[8] S. Kim, R. Lussi, X. Qu, F. Huang, and H. J. Kim, "Reversible data hiding with automatic brightness preserving contrast enhancement," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 8, pp. 2271–2284, Aug. 2019.

[9] X. Li, W. Zhang, and X. Gui, "Efficient reversible data hiding based on multiple histograms modification," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 2016–2027, Sep. 2015.

[10] J.Wang, J. Ni, X. Zhang, and Y. Q. Shi, "Rate and distortion optimization for reversible data hiding using multiple histogram shifting," *IEEE Trans. Cybernet.*, vol. 47, no. 2, pp. 315–326, Feb. 2017.

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

[12] R. M. Rad, K. Wong, and J.-M. Guo, "Reversible data hiding by adaptive group modification on histogram of prediction errors," *Signal Process.*, vol. 125, pp. 315–328, 2016.

[13] Y. Yang, W. Zhang, X. Hu, and N. Yu, "Improving visual quality of reversible data hiding by twice sorting," *Multimedia Tools Appl.*, vol. 75, pp. 13663–13678, 2016.

[14] W. He, G. Xiong, S. Weng, Z. Cai, and Y. Wang, "Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion," *Inf. Sci.*, vol. 467, pp. 784–799, 2018.

[15] Y. Yang, W. Zhang, D. Liang, and N. Yu, "Reversible data hiding in medical images with enhanced contrast in texture area," *Digit. Signal Process.*, vol. 52, pp. 13–24, 2016.

[16] H.-T. Wu, J.-L. Dugelay, Y.-Q. Shi, "Reversible image data hiding with contrast enhancement," *IEEE Signal Process. Lett.*, vol. 22, no. 1, pp. 81–85, Jan. 2015.

[17] G. Gao and Y.-Q. Shi, "Reversible data hiding using controlled contrast enhancement and integer wavelet transform," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 2078–2082, Nov. 2015.

[18] Y. Yang, W. Zhang, D. Liang, and N. Yu, "A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18043–18065, 2018.

[19] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[20] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 7, pp. 553–562, Mar. 2013.

[21] S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Trans. Multimedia*, vol. 21, no. 1, pp. 51–64, Jan. 2019.

[22] H. Ge, Y. Chen, Z. Qian, and J. Wang, "A high capacity multi-level approach for reversible data hiding in encrypted images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 8, pp. 2285–2295, Aug. 2019.

[23] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

[24] P. G. Howard, F. Kossentini, and B. Martins, "The emerging JBIG2 standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8, no. 7, pp. 838–848, Nov. 1998.

[25] K. Krishna and M. N. Murty, "Genetic K-means algorithm," *IEEE Trans. Cybernet.*, vol. 28, no. 3, pp. 433–439, Jun. 1999.

[26] Y. L. Lee and W. H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 4, pp. 695–703, Apr. 2014.

[27] Open Access National Imaging Archive [Online]. Available: https://imaging.nci.nih.gov

[28] Y. Fang, K. Ma, Z. Wang, W. Lin, Z. Fang, and G. Zhai, "No-reference quality assessment of contrast-distorted images based on natural scene statistics," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 838–842, Jul. 2015.