A Secure and High Visual-Quality Framework for Medical Images by Contrast-Enhancement Reversible Data Hiding and Homomorphic Encryption

YANG YANG\(^1\), XINGXING XIAO\(^1\), XUE CAI\(^1\), AND WEIMING ZHANG\(^2\)

\(^1\)School of Electronics and Information Engineering, Anhui University, Hefei 230601, China
\(^2\)School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China

Corresponding author: Yang Yang (sky_yang@ahu.edu.cn)

This work was supported in part by the Natural Science Foundation of China under Grant 61502007 and Grant 61572452, in part by the Natural Science Research Project of Anhui province under Grant 1608085MF125, in part by the Backbone Teacher Training Program of Anhui University, and in part by the Doctoral Scientific Research Foundation of Anhui University under Grant J01001319.

ABSTRACT
Medical data security is facing great challenges in medical applications due to the open internet and the semi-trusted cloud. For the sake of privacy protection and the security of medical images, this paper proposes a secure and high visual-quality framework for medical images. In this framework, a novel reversible data hiding (RDH) based on lesion extraction embeds privacy data into medical images for privacy protection and image quality improvement, homomorphic encryption based on chaotic map encrypts images for medical image security. The experiments have shown that the proposed framework increases the security of medical data and improves the visual quality of medical images significantly. The proposed RDH in this framework outperforms the other RDH methods with contrast enhancement and the proposed encryption scheme increases image security well.

INDEX TERMS
Reversible data hiding, homomorphic encryption, contrast enhancement, security, medical images.

I. INTRODUCTION
Nowadays, medical imaging clouds, telemedicine and telematics services play a significant responsibility in the growth of the medical industry. These medical applications bring great benefits to people. However, there are great challenges for medical data security in medical applications simultaneously. Due to the semi-trusted cloud and the open internet, medical data including of medical records and images is constantly threatened by illegal activities. These data containing sensitive patients’ information is easy to become the target of attackers, resulting in medical data leakage. What is more, malicious attacks for medical images may interfere with doctors’ diagnosis. The security of medical data is seriously threatened. Therefore, a secure scheme for medical data is desired in medical applications extremely.

Reversible data hiding (RDH) is a data hiding technique that can recover the original image without any distortion after the embedded data is extracted from the marked image. At present, there are already many classic algorithms, such as lossless compression [1], difference expansion [2], [3] and histogram shifting [4], [5]. For improving the quality of images, RDH methods with contrast enhancement are proposed later. This important technique is applied to images with high quality, such as the medical image. Wu et al. [7] expanded the peak-pairs of gray histogram to embed data to enhance image’s contrast, and they improved image preprocessing to achieve the high payload later [8]. On the basis of histogram shifting, Gao et al. [9] added wavelet domain to embed data. Yang et al. [10] prioritized to embed data into the texture region by prediction errors histogram. For medical images, there are existing RDH methods based on region of interest (ROI) segmentation, such as adaptive threshold detector (ATD) and Otsu. Gao et al. [11] adopted histogram shifting to embed data into ROI which was segmented.
by Otsu. Yang et al. [12] adopted histogram shifting to embed data respectively into region of interest and region of non-interest (NROI) which were segmented by ATD. In fact, RDH based on ROI used threshold segmentation methods to segment an image into foreground and background. However, the lesion area is an important basis for doctors to make a diagnosis. So, RDH methods based on lesion extraction and with obvious contrast enhancement are desired for medical images.

Inspired by the need of image security and data protection, reversible data hiding combined with encryption [13]–[15] emerged. Reversible data hiding combined with encryption not only protects the hidden data, but also ensures the security of cover images, which achieves data protection and image security. As shown in Fig.1, the traditional framework is a way of RDH after encryption, which applies to natural images which will be uploaded into the cloud. The user is unwilling to expose their sensitive data or private information of the image to untrusted channels or cloud. Hence, the image is encrypted into unintelligible ciphertext data by encryption. On the cloud, some additional data is need to be embedded into images for cover authentication or content integrity verification. At present, the scheme of reversible data hiding in encrypted image has two frameworks [16]: one is vacating room before encryption (VRBE), and the other is vacating room after encryption (VRAE). In the framework of VRBE, the image is first preprocessed to vacate room. Then, image is encrypted and data is embedded into the room which has been vacated. Ma et al. [17] first emptied out room by embedding LSBs of some pixels into other pixels with histogram shifting of prediction errors. Then, data is embedded into the vacating room after encryption. Zhang et al. [18] proposed that the original image was divided into the encryption region and the embedding region firstly. Then the embedding process and the encryption process were performed separately. Cao et al. [19] vacated room to embed data by representation of sparse coding before encryption. In the framework of VRAE, the image is first encrypted, then data is embedded into encrypted domain. Zhang et al. [20] embedded data into the vacating room which was vacated by flipping least significant bits (LSBs) of pixels in each encrypted block. Hong et al. [21] ameliorated Zhang’s method at the decoder side by using a different estimation equation and side match technique. Zhang et al. [22] embedded data into the encrypted image by using cipher-text compression. Puteaux et al. [23] proposed a RDH method based on most significant bit (MSB) prediction to embed data into encrypted images. Wu et al. [24] proposed RDH based on difference expansion and histogram shifting to embed data into the encrypted domain.

The traditional framework of RDH after encryption (Fig.1) solves the problem about image security and data protection effectively. Different from natural images, the data embedded into a medical image is not limited to information about owner and authentication, and also includes patient’s records consisting of diagnostic reports, vital signs, and other information. Besides, the data related to patients also needs to be transmitted or stored as a file. What is more, it involves a great deal of privacy and is easier to be leaked. Hence, we propose a new framework of RDH before encryption as shown in Fig.2. Data should be first embedded into the correspondent medical images to protect patients’ privacy and match its medical image, which also can save space in storage and transmission. In addition, the visual quality of medical images can be improved well by contrast-enhancement RDH. Then, marked medical images are encrypted to ensure the security of image content before they are uploaded or transmitted. If users refuse to upload an medical image or privacy data into the cloud, just do the first step of the proposed framework: embed privacy data into the medical image to prevent privacy leaks. Meanwhile, the quality of marked image is improved for observing. In a word, the proposed framework is more suitable for medical images to increase the security of medical data and improve visual quality of medical images in medical applications, such as picture archiving and communicating system, hospital information system, telemedicine, medical imaging clouds, telematics medical services and so on. The main contributions of this framework include two aspects:

- Propose a secure and high visual-quality framework for medical images. Different from the traditional framework of RDH in encrypted images, the proposed framework is a way of RDH before encryption for privacy protection and image security in medical applications.
- Propose RDH based on lesion extraction and homomorphic encryption based on chaotic map in the framework. The proposed RDH not only enhances contrast for the lesion area but also increases the embedding rate. The proposed encryption scheme protects images from attacks. Experiments have shown that the proposed RDH is better than other contrast-enhancement RDH methods.
in the lesion area and the proposed encryption scheme can increase image security well.

The rest of this paper is organized as follows. Section II describes the details of the proposed framework. Experimental results and analysis are shown in Section III. Finally, conclusion is presented in Section IV.

II. PROPOSED METHOD

Aim at increasing the security of medical data and improving the visual quality of medical images, this paper proposes a secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. Fig. 3 illustrates the diagram of the proposed framework.

The proposed framework consists of four stages as Fig. 3: RDH based on lesion extraction, image encryption, image decryption, extraction and recovery. At the sending end, privacy data is first embedded into the image by RDH based on lesion extraction to protect patient’s privacy and improve image quality. And, the marked medical image is encrypted by encryption to increase security of medical images. Then encrypted medical images are uploaded or transmitted safely. At the receiving end, the encrypted image can be decrypted with secret key to obtain marked images with contrast enhancement. Finally, privacy data can be extracted completely and the medical image can be recovered losslessly by the third party with right.

A. REVERSIBLE DATA HIDING BASED ON LESION EXTRACTION AND WITH CONTRAST ENHANCEMENT

To protect patients’ privacy and improve the visual quality of medical images, RDH based on lesion extraction and with contrast enhancement is proposed in this framework. This section introduces the proposed RDH in detail.

In medical images, the lesion area is an important basis of diagnosis and requires high image quality for diagnosis. The non-lesion area does not contain the key information and the pixel range of non-lesion area is so monocular that it can embed high-capacity data. Thus, we use different RDH methods to embed privacy data into the lesion and non-lesion area respectively for privacy protection after lesion extraction, which achieves not only image quality improvement but also high embedding capacity. Fig. 4 illustrates the diagram of the proposed RDH. Firstly, the lesion area is extracted by distance regularized level set evolution (DRLSE) and the rest area is the non-lesion area. Secondly, privacy data is embedded into the lesion area preferentially by improved histogram shifting method to enhance the contrast of medial image’s lesion area. Lastly, the rest of data is embedded into the non-lesion area by the high-capacity embedding method to achieve the higher payload.

1) LESION EXTRACTION

At present, there are existing RDH methods based on ROI segmentation, such as ATD and Otsu, for medical images.
Let $I$ be a medical image and $I(x, y)$ be a pixel located at the coordinate $(x, y)$ on $I$. A binary image $I_b(x, y)$ is generated by

$$I_b(x, y) = \begin{cases} 1, & I(x, y) \in L \\ 0, & \text{others} \end{cases}$$

where $L$ is the lesion area. “1” in $I_b$ denotes the lesion area. “0” in $I_b$ denotes the non-lesion area. We can extract lesion from $I$ in accordance with $I_b$.

2) DATA EMBEDDING
To protect patients’ privacy, privacy data is embedded into medical images. For improve visual quality of medical images, data is embedded into the lesion area preferentially to enhance contrast. The rest of data is embedded into the non-lesion area to achieve the higher payload. To achieve reversibility, the auxiliary information needs to be embedded into the image. This section details the process of data embedding.

a: EMBEDDING IN THE LESION AREA
Medical images’ lesion area is the important basis for doctors to make a diagnosis. We aim at enhancing the contrast of lesion area for improving the quality of medical images and achieving RDH meanwhile. To enhance contrast, the lesion area is stretched firstly. As a result, there are empty bins in the gray histogram. Data is sequentially embedded into the empty bins of the stretched histogram. And the contrast of lesion area is enhanced further, which is similar to the effect of histogram equalization. The embedding steps in the lesion area are detailed as follows:

(1) The value of pixel in the lesion area is stretched firstly. The original value $I_o$ will be stretched to $I_1$, when the value is stretched from $[I_{\text{max}}, I_{\text{min}}]$ into $[I_{\text{max}}-I_{\text{min}}]$ as follow:

$$I_1 = \text{round} \left( \frac{I_o - I_{\text{min}}}{I_{\text{max}} - I_{\text{min}}} \right)$$

(2) To avoid the overflow problem and the underflow problem, data is embedded by shifting histogram from left to right if the pixel $I_1$ is in $[0, 126]$, or data is embedded by shifting histogram from right to left if the pixel $I_1$ is in $[129, 255]$. Calculate the gray histogram of lesion area. The marked pixel $I'_1$ is modified by

$$I'_1 = \begin{cases} I_1 + b_i, & \text{if } I_1 = I_m \& \& 0 \leq I_1 \leq 126 \\
& \& \& h(I_1 + 1) = 0 \\
I_1 - b_i, & \text{if } I_1 = I_m \& \& 129 \leq I_1 \leq 255 \\
& \& \& h(I_1 - 1) = 0 \\
I_1, & \text{if } I_1 \neq I_m \end{cases}$$

In which $I_1$ is the unmodified pixel in the lesion area. $I_m$ is the pixel value of peak bin in the gray histogram. $b_i$ is the data to be embedded. $h(I_1)$ is the frequency of pixel $I_1$ in the gray histogram of lesion area.
(3) Repeat step (2) until there is no empty bin to be embedded or all data is embedded into the lesion area. The pixel value of peak bin in each round is embedded as the part of privacy data into the next round.

b: EMBEDDING IN THE NON-LESION AREA

To achieve the higher embedding rate, the rest data is embedded into the non-lesion area when there is no empty bin to embed data in the lesion area. We adopts a high-capacity RDH method [26] that can achieve the high embedding rate. The embedding steps in the non-lesion area are detailed as follows:

(1) Select one of four prediction modes in [27] and calculate the prediction error $e_{i,j}$ by

$$e_{i,j} = I_{i,j} - p_{i,j}$$ (4)

In which the prediction value $p_{i,j}$ is predicted by its neighbors simply using the interpolation technique in [28].

(2) Calculate the value of smoothness $\sigma$ which measures whether the pixel $I_{i,j}$ is smooth or complex by standard deviation of $I_{i,j}$ and its eight surrounding neighbors.

$$\sigma = \sqrt{\frac{\sum_{k \in [-1,0,1]} (I_{i,k,j} - \mu)^2}{8}}$$ (5)

In which $\mu$ is the mean of $I_{i,j}$ and its eight surrounding neighbors.

(3) The expanded prediction error $e'_{i,j}$ is calculate by Eq.(6) if $\sigma < T_v$.

$$e'_{i,j} = \begin{cases} e_{i,j} \times 4 + b_i, & \text{if } -T_p \leq e_{i,j} < T_p \\ e_{i,j} - 3 \times T_p, & \text{if } e_{i,j} \leq -T_p - 1 \\ e_{i,j} + 3 \times T_p, & \text{if } e_{i,j} \geq T_p \end{cases}$$ (6)

In which $b_i \in \{0, 1, 2, 3\}$, $T_v$ and $T_p$ are thresholds detailed in [26]. $e'_{i,j}$ is calculate by Eq.(7) if $\sigma \geq T_v$.

$$e'_{i,j} = \begin{cases} e_{i,j} \times 2 + b_i, & \text{if } -T_p \leq e_{i,j} < T_p \\ e_{i,j} - T_p, & \text{if } e_{i,j} \leq -T_p - 1 \\ e_{i,j} + T_p, & \text{if } e_{i,j} \geq T_p \end{cases}$$ (7)

In which $b_i \in \{0, 1\}$.

(4) The marked pixel $I'_{i,j}$ is got by

$$I'_{i,j} = p_{i,j} + e'_{i,j}$$ (8)

In which $I'_{i,j}$ should be in [0,255]. If an overflow or underflow problem occurs, we need the location map to record the overflow or underflow situation.

Step (1)-(4) are the process of a layer embedding. If a layer embedding does not meet the required embedding rate, repeat step (1)-(4) until all data is embedded into the image.

c: EMBEDDING OF THE AUXILIARY INFORMATION

In order to extract data completely and recover image losslessly, the auxiliary information, such as the edge of lesion area, the value of peak bin $I_m$ in the last embedding round of lesion area, the threshold $T_v$ and $T_p$, the number of embedding layer, the end of symbol and the compressed location map in the non-lesion area, needs to be embedded into image. The four sides of medical image do not contain critical information, so they are used to embed the auxiliary information. As shown in Fig.6, the size of the image is $X \times Y$, $h$ rows and $h$ columns of the image’s sides without first $M$ pixels are the place to embed the auxiliary information by replacing least significant bit (LSB). It is worth noting that $h$ rows and $h$ columns of the image’s sides are segmented firstly and they do not participate in the embedding process of lesion or non-lesion area. $h$ (2 bits), the number of LSB plane (2 bits) and the end of symbol ($log_2X + log_2Y$ bits) are put in the first $M$ ($M = 2 + 2 + log_2X + log_2Y$) pixels’ LSB. Original LSBs of $h$ rows and $h$ columns in image’s four sides are embedded into the non-lesion area to vacate room which is used to embed the auxiliary information after all data is embedded into image.

B. HOMOMORPHIC ENCRYPTION BASED ON CHAOTIC MAP

To prevent image content from being maliciously read or leak, the marked image is transformed into unintelligible ciphertext data by additive homomorphism algorithm to increase security. Only with the secret key, can the image be decrypted. To increase image security further, the Piecewise Linear Chaotic Map is used to generate the secret key which is hard to break. As shown in Fig.7, homomorphic encryption based on chaotic map encrypts the marked image $M$ into the encrypted image $C$.

The secure performance of encryption is related to the secret key closely. Since chaotic systems can generate pseudo-random sequences with randomness, non-correlation and complexity. And they are particularly sensitive to initial values and parameters. Thus, the proposed encryption scheme uses a chaotic generator based on the Piecewise Linear Chaotic Map [29] to generate the secret key. In addition, the advantage of the secret key via chaotic generator...
is that its space is large, the randomness is strong, and the distribution of key is simple and convenient. The generation of secret key is shown in Fig.7. Firstly, input the initial value $x_0$ and the parameter $c$, and the chaotic generator generates a pseudo-random sequence $R$ which is in $[0, 1]$. Secondly, quantize $R$ into random integral sequence $S$ which is in $[0,255]$ by Eq.(9) to adapt to image encryption. Finally, the secret sequence are generated and $K = (c, x_0)$ is regarded as the ultimate secret key.

Homomorphic encryption is special among encryption algorithms, because the encrypted domain can be directly operated without the original image content. In other words, the encrypted image is not required to be decrypted firstly, then recalculated, and finally encrypted. Homomorphic encryption simplifies the process of operation and ensures the security of image. Therefore, the proposed encryption scheme adopts the additive homomorphism as Eq.(10). The calculation of the propose algorithms is simple, and no data expansion is generated. What is more, the encrypted domain can be directly calculated as $E(M1 + M2, S1 + S2) = (C1 + C2) \mod 256 = C1 \oplus C2$ where $\oplus$ is the modular $N$ addition. It can achieve the authentication and retrieval of encrypted images and so on. The arithmetic addition of plaintext is equal to the modular addition of ciphertext. If $M2$ is plaintext, that is, $K2$ is 0, the modular addition of ciphertext is as $C1 \oplus C2 = E(M1 + M2, S1)$. When $M2$ is the medical authentication or retrieval data, the modular addition of ciphertext is equal to the arithmetic addition of plaintext, which means that ciphertext authentication or retrieval succeeds.

$$E(M, S) = (M + S) \mod N \quad (10)$$

In which $M$ represents the set of the plaintexts, $C$ represents the set of the ciphertexts, $E()$ represents the operation of encryption, $S$ denotes the secret sequences, and $N$ is 256. The steps of encryption are described as follows:

1. Input $K$ to obtain the random sequences $R$
2. Quantize the random sequence $R$ into the integral sequence $S$ by Eq.(9).
3. Encrypt image by Eq.(10).

C. IMAGE DECRYPTION

To read image content, the encrypted image can be decrypted to obtain the marked image with the secret key. Otherwise, the encrypted image cannot be decrypted without the correct key. The steps of decryption are described as follows:

1. Input $K$ to obtain the random sequences $R$
2. Quantize the random sequence $R$ into the integral sequence $S$ by Eq.(9).
3. Decrypt image by Eq.(11)

$$D(C, S) = (C - S) \mod N \quad (11)$$

where $D()$ represents the operation of encryption.

D. DATA EXTRACTION AND IMAGE RECOVERY

The marked images with contrast enhancement are obtained after decryption. If doctors want to learn about information related patients or patient himself wants to know diagnostic records and results, data can be extracted and the medical image can be recovered completely with authorization. This section details the process of data extraction and image recovery.

1. Extract first $M$ pixels’ LSB in four sides of image to obtain $h$, the number of LSB plane and the end of symbol.
2. Extract all auxiliary information from four sides of image except for the first $M$ pixels, such as the edge of lesion area, the value of peak bin $I_m$ in the last embedding round of lesion area, the threshold $T_v$ and $T_p$, the number of embedding layer, the end of symbol and the compressed location map in the non-lesion area. And decompress the location map of non-lesion area.
3. Extract the lesion area and the rest of image is the non-lesion area according to the edge of lesion area.
4. In the non-lesion area, if $\sigma < T_v$, data $b_i$ and the prediction error $e_{i,j}$ are calculated by Eq.(12) and Eq.(13) respectively.

$$b_i = e_{i,j} - 4 \left\lfloor \frac{e_{i,j}}{4} \right\rfloor \quad (12)$$

where $b_i \in \{0, 1, 2, 3\}$.

$$e_{i,j} = \begin{cases} e_{i,j} + 3 \ast T_p, & \text{if} \ e_{i,j} \leq -4T_p - 1 \\ e_{i,j} - 3 \ast T_p, & \text{if} \ e_{i,j} \geq 4T_p \\ \left\lfloor e_{i,j}/4 \right\rfloor, & \text{if} \ -4T_p \leq e_{i,j} \leq 4T_p - 1 \end{cases} \quad (13)$$

If $\sigma \geq T_v$, data $b_i$ and the prediction error $e_{i,j}$ are calculated by Eq.(14) and Eq.(15) respectively.

$$b_i = e_{i,j} - 2 \left\lfloor \frac{e_{i,j}}{2} \right\rfloor \quad (14)$$

where $b_i \in \{0, 1\}$.

$$e_{i,j} = \begin{cases} e_{i,j} + T_p, & \text{if} \ e_{i,j} \leq -2T_p - 1 \\ e_{i,j} - T_p, & \text{if} \ e_{i,j} \geq 2T_p \\ \left\lfloor e_{i,j}/2 \right\rfloor, & \text{if} \ -2T_p \leq e_{i,j} \leq 2T_p - 1 \end{cases} \quad (15)$$

The original pixel $I_{i,j}$ in the non-lesion area is recovered by

$$I_{i,j} = p_{i,j} + e_{i,j} \quad (16)$$

Repeat the process of extraction and recovery in the non-lesion area until all embedded data of the non-lesion area is extracted.
(5) Obtain LSBs of image’s four sides from data which just has been extracted from the non-lesion area to recover four sides of image.

(6) In the lesion area, data extraction and image recovery are as follows:

$$b_i = \begin{cases} 
0, & \text{if } 0 \leq I'_l \leq 126 \&\& I_l = I_m + 1 \\
1, & \text{if } 129 \leq I'_l \leq 255 \&\& I_l = I_m - 1 \\
others
\end{cases}$$  \hspace{1cm} (17)

$$I_l = \begin{cases} 
I'_l - 1, & \text{if } 0 \leq I'_l \leq 126 \&\& I_l = I_m + 1 \\
I'_l + 1, & \text{if } 129 \leq I'_l \leq 255 \&\& I_l = I_m - 1 \\
others
\end{cases}$$  \hspace{1cm} (18)

(7) The pixel $I_l$ in the lesion area is recovered to $I_o$ which is the pixel before stretched.

$$I_o = \text{round} \left[ \frac{I_l}{L_{\max} - L_{\min}} \ast (I_{\max} - I_{\min}) + I_{\min} \right]$$  \hspace{1cm} (19)

III. EXPERIMENTS

We discuss the performance of RDH and encryption respectively to show the characteristic of proposed framework through lots of experiments. The experiments are tested by coding the algorithm in MATLAB 2016 running on Window 10 and run on a 64-bit PC with Intel (R) Core (TM) CPU @3.90 GHz and 4G RAM. We choose three different kinds which are often made to examine body in hospital to show the experiment results: CT mainly examines bone, joint, organ in thorax etc. through X-ray; MRI mainly examines brain, soft tissue of the whole body etc. through electromagnetic wave; USI mainly examines abdomen, blood vessel etc. through ultrasound. And, we choose 24 medical images [30] in Fig.8 randomly due to space limit. In particular, there are 8 medical images with different lesion in each type medical images respectively. In this section, the experimental results and analysis are introduced in detail.

A. EXPERIMENTS OF RDH

To illustrate the performance of the proposed RDH scheme, we do two series of experiments: discuss the experiment results in the lesion area, and compare the contrast performance of the proposed method in the lesion area with that of other methods which are Yang [10], Wu [8], Gao [11] and Yang [12]’s RDH with contrast enhancement at different embedding rate.

We first compare the method of lesion extraction in the proposed scheme with Gao [11] and Yang’s [12] methods due to Yang [10] and Wu’s [8] methods without segmentation. ROI methods based on threshold segmentation divide images into foreground and background. Foreground is regarded as ROI in which doctors are interested and background is regarded as NROI which do not contain the key information. Here, “CT1”, “MRI1” and “USI1” are taken as examples in Fig.9. Fig.9 (b), (f) and (j) belong to ROI by Otsu [11]. In particular, (j) ignores the important place which is the lesion area by Otsu. Fig.9 (c), (g) and (k) belong to ROI through ATD [12]. Fig.9 (d), (h) and (l) are the lesion area by the way of lesion extraction. We can conclude that ROI is just the place which is sweeping, and it is not intuitive to observe. The lesion area is the doctor’s focus and used as the basis for clinical diagnosis. The way of lesion extraction is performed for targeting the lesion area, and the effect of segmentation is clear and intuitive to observe. So the proposed scheme has an advantage over other segmentation methods for the lesion area.

From the subjective visual and objective data, we discuss the performance of contrast enhancement and the maximum embedding bits in the lesion area. In Fig.10, “CT1”, “MRI1” and “USI1” are taken as examples. The contrast of lesion area in three different types of medical images is enhanced obviously in 0.1 bpp, 0.6 bpp, 0.8 bpp and 1 bpp respectively. Because data is embedded into empty
bins in the lesion area, there is the maximum embedding bits. As shown in Table 1, there are 99488 bits, 132437 bits and 52438 bits in the lesion area of three medical images respectively, the corresponding value of no-reference contrast distortion image quality assessment (NR-CDIQA) [31] is 2.9039, 2.5891 and 2.8980 respectively, and the corresponding value of no-reference improved contrast distortion image quality assessment (NR-ICDIQA) [32] is 2.9894, 2.9784 and 2.9806 respectively. Here, NR-CDIQA and NR-ICDIQA methods can effectively assess the quality of contrast-enhancement images. The higher the scores of NR-CDIQA and NR-ICDIQA are, the better the quality of images is.

We discuss the contrast enhancement performance of proposed method in the lesion area and make comparisons with Yang [10], Wu [8], Gao [11] and Yang’s [12] methods which are also RDH with contrast enhancement at different embedding rates. As shown in Table 2-7, we also calculate peak signal to noise ratio (PSNR) and structural similarity index measurement (SSIM). It is worth noting that PSNR and SSIM are traditional methods of image quality assessment. PSNR is based on the error between the marked image and the original image. It is an image quality assessment for error sensitive image. But it does not take the human visual characteristics into account. SSIM is a full-reference image quality assessment which reflects the structural characteristics of the image, but it ignores the underlying visual characteristics of the human visual system. Therefore, PSNR and SSIM do not evaluate the image with contrast enhancement well. We use NR-CDIQA and NR-ICDIQA methods to assess the quality of marked images. In this paper, we take “CT1”, “MRI1” and “USI1” as examples of three types of medical images in Table 2, 4 and 6. NR-CDIQA and NR-ICDIQA value of three medical images by the proposed RDH in lesion area RDH are higher than those of other RDH methods in 0.1 bpp, 0.6 bpp, 0.8 bpp and 1 bpp respectively. We also calculate the average values of assessment parameters for three types of medical images in Table 3, 5 and 7. The average NR-CDIQA and NR-ICDIQA value of three types of marked images by the proposed RDH in lesion area RDH are higher than those of other RDH methods in 0.1 bpp, 0.6 bpp, 0.8 bpp and 1 bpp respectively. Experimental results show that the contrast of marked images in the lesion area is enhanced obviously and the proposed method is better than other contrast-enhancement RDH methods for lesion area at different embedding rates.

Next, we analyze the reasons why the proposed method is better than Yang [10], Wu [8], Gao [11] and Yang’s [12] methods. Yang’s [10] method prioritizes to embed data into the texture region by prediction error histogram. Lesion is

---

**TABLE 1.** The value of NR-CDIQA, NR-ICDIQA and the maximum embedding bits in the lesion area.

| Image(size)   | NR-CDIQA | NR-ICDIQA | Maximum Embedding Bits |
|--------------|----------|-----------|------------------------|
| CTI (351 x 220) | 2.9039   | 2.9894    | 99488                  |
| MRI (340 x 180) | 2.5891   | 2.9784    | 132437                 |
| USI (199 x 203) | 2.8980   | 2.9806    | 52438                  |

**TABLE 2.** The value of assessment parameters by the proposed method compared with other methods in an image “CT1”.

| Embedding rate | Method | PSNR | SSIM | NR-CDIQA | NR-ICDIQA |
|---------------|--------|------|------|----------|-----------|
| 0.1 bpp       | Yang [10] | 53.1104 | 0.9985 | 2.5971   | 1.9335    |
|               | Wu [8]   | 53.6797 | 0.9516 | 2.0817   | 1.8499    |
|               | Gao [11] | 54.0908 | 0.9919 | 2.3295   | 2.3428    |
|               | Yang [12] | 56.0929 | 0.8710 | 2.1858   | 2.3789    |
|               | Proposed | 24.3437 | 0.9717 | 2.4717   | 2.4123    |
| 0.6 bpp       | Yang [10] | 63.6259 | 0.9879 | 2.1021   | 1.9415    |
|               | Wu [8]   | 65.0208 | 0.9314 | 2.1518   | 2.0796    |
|               | Gao [11] | 64.4119 | 0.8423 | 2.2422   | 2.4450    |
|               | Yang [12] | 64.9959 | 0.7508 | 2.2618   | 2.4265    |
|               | Proposed | 24.3510 | 0.9717 | 2.4918   | 2.4508    |
| 0.8 bpp       | Yang [10] | 48.9711 | 0.9869 | 2.1030   | 1.9464    |
|               | Wu [8]   | 49.8474 | 0.8632 | 2.1709   | 1.9435    |
|               | Gao [11] | 50.9501 | 0.7505 | 2.3727   | 2.8487    |
|               | Yang [12] | 50.0343 | 0.7515 | 2.3070   | 2.7505    |
|               | Proposed | 24.4258 | 0.9717 | 2.8614   | 2.9644    |
| 1 bpp         | Yang [10] | 45.9315 | 0.9866 | 2.1031   | 1.9508    |
|               | Wu [8]   | 49.1354 | 0.8588 | 2.2652   | 2.2997    |
|               | Gao [11] | 48.4462 | 0.6734 | 2.7941   | 2.6869    |
|               | Yang [12] | 50.0624 | 0.7548 | 2.8457   | 2.9111    |
|               | Proposed | 24.4329 | 0.9717 | 2.9010   | 2.9880    |
not the texture region necessarily. So, Yang's method does not enhance the contrast of lesion area effectively. Wu's [8] method embeds data into images by histogram shifting. It first chooses the highest two bins, and keeps the bins between the two peaks unchanged and shifts the other bins outwards.

**TABLE 4.** The value of assessment parameters by the proposed method compared with other methods in an image "MRI1".

| Embedding rate | Method       | PSNR     | SSIM     | NR-CDQA  | NR-ICDQA |
|---------------|--------------|----------|----------|----------|----------|
| 0.1 bpp       | Yang [10]    | 53.0278  | 0.9997   | 2.3574   | 2.2937   |
|               | Wu [8]       | 20.1972  | 0.9920   | 2.3412   | 2.2937   |
|               | Gao [11]     | 14.3419  | 0.9935   | 2.3351   | 2.2937   |
|               | Yang [12]    | 21.7007  | 0.9128   | 2.1172   | 2.1993   |
|               | Proposed     | 29.8458  | 0.9634   | 2.5266   | 2.6554   |
| 0.6 bpp       | Yang [10]    | 46.4100  | 0.9914   | 2.1462   | 2.1536   |
|               | Wu [8]       | 20.2512  | 0.9903   | 2.0116   | 2.0272   |
|               | Gao [11]     | 16.5450  | 0.9501   | 1.9010   | 1.9297   |
|               | Yang [12]    | 24.8914  | 0.9483   | 2.5665   | 2.9755   |
|               | Proposed     | 31.0188  | 0.9666   | 2.8880   | 2.9765   |
| 0.8 bpp       | Yang [10]    | 46.2300  | 0.9911   | 2.1463   | 2.1539   |
|               | Wu [8]       | 20.2117  | 0.9910   | 2.1161   | 2.0286   |
|               | Gao [11]     | 18.3465  | 0.7160   | 1.5255   | 2.3334   |
|               | Yang [12]    | 24.8919  | 0.9483   | 2.5872   | 2.9758   |
|               | Proposed     | 31.0188  | 0.9666   | 2.8880   | 2.9765   |
| 1 bpp         | Yang [10]    | 46.2300  | 0.9911   | 2.1463   | 2.1539   |
|               | Wu [8]       | 20.2117  | 0.9910   | 2.1161   | 2.0286   |
|               | Gao [11]     | 16.6156  | 0.6424   | 2.0507   | 2.8072   |
|               | Yang [12]    | 24.8929  | 0.9483   | 2.5843   | 2.9765   |

The contrast of image is not obviously enhanced at the low embedding rate. Gao [11] and Yang's [12] methods first segmented medical image into ROI and NROI, then embedded data into ROI preferentially. However, ROI is not the exact lesion area, they can not directly improve the contrast of the lesion area. The proposed method adopts DRLSE to extract lesion. In the lesion area, pixels are stretched to enhance contrast. Data is first embedded into empty bins of stretched histogram to enhance contrast further. The contrast of lesion area is obviously enhanced at the low embedding rate. In addition, it can avoid the overflow and underflow problems. In the non-lesion area, the rest of data is embedded by the high-capacity embedding way to achieve the higher payload. Through a lot of experiments, the quality of marked images in the lesion area is obviously better than other RDH methods with contrast enhancement.

**B. EXPERIMENTS OF ENCRYPTION**

To verify the security of the proposed encryption, we use different metrics: key pace, histogram of marked images and

| Embedding rate | Method       | PSNR     | SSIM     | NR-CDQA  | NR-ICDQA |
|---------------|--------------|----------|----------|----------|----------|
| 0.1 bpp       | Yang [10]    | 46.4100  | 0.9914   | 2.1462   | 2.1536   |
|               | Wu [8]       | 20.2512  | 0.9903   | 2.0116   | 2.0272   |
|               | Gao [11]     | 16.5450  | 0.9501   | 1.9010   | 1.9297   |
|               | Yang [12]    | 24.8914  | 0.9483   | 2.5665   | 2.9755   |
|               | Proposed     | 31.0188  | 0.9666   | 2.8880   | 2.9765   |
| 0.6 bpp       | Yang [10]    | 46.2300  | 0.9911   | 2.1463   | 2.1539   |
|               | Wu [8]       | 20.2117  | 0.9910   | 2.1161   | 2.0286   |
|               | Gao [11]     | 18.3465  | 0.7160   | 1.5255   | 2.3334   |
|               | Yang [12]    | 24.8919  | 0.9483   | 2.5872   | 2.9758   |
|               | Proposed     | 31.0188  | 0.9666   | 2.8880   | 2.9765   |
| 0.8 bpp       | Yang [10]    | 46.2300  | 0.9911   | 2.1463   | 2.1539   |
|               | Wu [8]       | 20.2117  | 0.9910   | 2.1161   | 2.0286   |
|               | Gao [11]     | 16.6156  | 0.6424   | 2.0507   | 2.8072   |
|               | Yang [12]    | 24.8929  | 0.9483   | 2.5843   | 2.9765   |
|               | Proposed     | 31.0188  | 0.9666   | 2.8880   | 2.9765   |
| 1 bpp         | Yang [10]    | 46.2300  | 0.9911   | 2.1463   | 2.1539   |
|               | Wu [8]       | 20.2117  | 0.9910   | 2.1161   | 2.0286   |
|               | Gao [11]     | 16.6156  | 0.6424   | 2.0507   | 2.8072   |
|               | Yang [12]    | 24.8929  | 0.9483   | 2.5843   | 2.9765   |
|               | Proposed     | 31.0188  | 0.9666   | 2.8880   | 2.9765   |
TABLE 8. The value of absolute correlation coefficient of adjacent pixels, $H$ and $|\rho_{MC}|$ in three medical images respectively.

| Image | Horizontal | Vertical | Diagonal | $H$ | $|\rho_{MC}|$ |
|-------|------------|----------|----------|-----|-------------|
| CT1   | Marked     | 0.9858   | 0.9927   | 0.9807 | 6.6280      |
|       | Encrypted  | 0.0112   | 0.0031   | 0.0028 | 7.9901      |
| MRI1  | Marked     | 0.9681   | 0.9281   | 0.9099 | 5.6159      |
|       | Encrypted  | 0.0081   | 0.0136   | 0.0301 | 7.9898      |
| USI1  | Marked     | 0.9958   | 0.9955   | 0.9927 | 6.5521      |
|       | Encrypted  | 0.0072   | 0.0179   | 0.0144 | 7.9968      |

FIGURE 11. The marked image, encrypted and decrypted image.

We first analyze the key space. The secret key plays an important role in an encryption scheme. The secret key should have large size to resist the brute-force attack. The calculation accuracy of key parameters is $10^{-14}$, the key space of the proposed encryption is $10^{14} \times 10^{14}$ and it is so large that the proposed encryption can resist brute-force attacks.

As we can see in Fig.11, “CT1”, “MRI1” and “USI1” are as examples of three types of medical images. Fig.11 (a), (d) and (g) are marked images, Fig.11 (b), (e) and (h) are encrypted images which are unable to read the original content, Fig.11 (c), (f) and (i) are decrypted images with right key. Image histogram reflects the distribution of pixels. The more uniform distribution of encrypted pixels is, the better the proposed encryption is. Histograms of encrypted images are uniform compared with marked images’ histogram in Fig.12. The correlation of adjacent pixels in the encrypted images is very high. We calculate the correlation of horizontal, vertical and diagonal adjacent pixels by choosing 5000 pixel pairs randomly respectively. “CT1” is as an example in Fig.13, there is no correlation between adjacent pixels in encrypted images. So, attackers can’t obtain any useful information about the original images from their pixel distributions and pixel correlation. The proposed encryption can resist statistical attacks.

We calculate absolute correlation coefficient of horizontal, vertical and diagonal adjacent pixels in the encrypted image, absolute correlation coefficient between the marked and encrypted image, and shannon entropy respectively in Table 8 and 9. Correlation coefficient of horizontal, vertical and diagonal adjacent pixels show a quantity analysis of pixel distribution in the encrypted image. Shannon entropy is a measure of the unpredictability of information content. The higher the entropy, the more uniform the pixel distribution, and the more difficult it is to obtain useful information about the original image from its distribution.
The average value of absolute correlation coefficient of adjacent
image in "CT1".

TABLE 9. The average value of absolute correlation coefficient of adjacent
pixels, \( H \) and \( |\text{MCE}| \) in three types of medical images respectively.

|        | Horizontal | Vertical | Diagonal | \( H \) | \( |\text{MCE}| \) |
|--------|------------|----------|----------|--------|------------|
| CT     | Marked image: 0.9757 | 0.9819 | 0.9613 | 6.2770 | 0.0060 |
|        | Encrypted image: 0.0111 | 0.0088 | 0.0202 | 7.9812 | 0.0060 |
| MRI    | Marked image: 0.9689 | 0.9712 | 0.9485 | 4.9551 |          |
|        | Encrypted image: 0.0101 | 0.0137 | 0.0144 | 7.9829 | 0.0043 |
| US1    | Marked image: 0.9761 | 0.9543 | 0.9390 | 6.2165 |          |
|        | Encrypted image: 0.0135 | 0.0126 | 0.0099 | 7.9830 | 0.0057 |

correlation. The absolute value of correlation coefficient of
adjacent pixels is closer to 0, the pixel correlation is weaker,
and the encrypted image is harder to break. Correlation
coefficient between marked and encrypted image symbolizes
the difference between the marked and encrypted image.
The smaller correlation coefficient is, the larger difference
between the marked and encrypted image is, the better
the proposed encryption is. The pixels of a encrypted image
are expected to randomly distribute to resist various security
attacks. Shannon entropy provides a strict description to
the randomness of image pixels. Shannon entropy of
encrypted images is closer to 8, the randomness of ciphertext
images is so stronger that it is hard to decrypt without key.
Table 8 shows the value of assessment parameters in “CT1”,
“MRI1” and “USI1” respectively, and Table 9 shows the
average value of assessment parameters in three types medical
images respectively. They show that the correlation of
encrypted image is very weak, and the randomness of the
encrypted image is large. Hence, we can conclude that the
proposed encryption can resist statistical attacks by analyzing
histogram, correlation and shannon entropy. As a result,
the proposed encryption scheme can increase image security
well.

IV. CONCLUSION

In this paper, we propose a secure and high visual-quality
framework for medical images by contrast-enhancement
RDH and homomorphic encryption. In this framework, RDH
based on lesion extraction achieves privacy protection and
medical images’ visual quality improvement, and homomor-
phic encryption based on chaotic map protects image from
attacks. Through a lot of experiments, the proposed RDH
scheme has an advantage over other segmentation meth-
ods for lesion area. NR-CDIQA and NR-ICDIQA value of
marked images by the proposed RDH are higher than those of
other RDH methods with contrast enhancement in the
lesion area, which indicates that the contrast enhancement
performance of proposed RDH is better than that of other
RDH methods with contrast enhancement for lesion area.
The correlation of encrypted images and marked images is
very weak and the randomness of encrypted images is large,
which show that the proposed encryption scheme can protect
image content and increase image security. And the proposed
encryption scheme can increases security of medical images
well. In conclusion, the proposed framework can increase
the security of medial data and improve the visual quality of
medical images effectively. In the future, the method of adap-
tive lesion extraction, such as machine learning, reversible
data hiding for improving the quality of medical images and
cryption for increasing the security of medical images will
be researched further.

REFERENCES

[1] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless
generalized-LSB data embedding,” IEEE Trans. Image Process., vol. 14,
no. 2, pp. 253–266, Feb. 2005.
[2] J. Tian, “Reversible data embedding using a difference expansion,” IEEE
Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
[3] D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for
reversible watermarking,” IEEE Trans. Image Process., vol. 16, no. 3,
pp. 721–730, Mar. 2007.
[4] 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.
[5] J. Wang, J. Ni, X. Zhang, and Y.-Q. Shi, “Rate and distortion optimization
for reversible data hiding using multiple histogram shifting,” IEEE Trans. Cybern.,
vol. 47, no. 2, pp. 315–326, Feb. 2017.
[6] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, “Hiding clinical
information in medical images: A new high capacity and reversible data
hiding technique,” J. Biomed. Inf., vol. 66, pp. 214–230, Feb. 2017.
[7] H.-T. Wu, J.-L. Dugelay, and Y.-Q. Shi, “Reversible image data hiding
with contrast enhancement,” IEEE Signal Process. Lett., vol. 22, no. 1,
pp. 81–85, Jan. 2015.
[8] H. Wu, S. Tang, J. Huang, and Y. Shi, “A novel reversible data hiding
method with image contrast enhancement,” Signal Process., Image Comm.,
vol. 62, pp. 64–73, Mar. 2018.
[9] 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.
[10] Y. Yang, W. Zhang, D. Liang, and N. Yu, “A ROI-based high capacity
reversible watermarking,” IEEE Trans. Image Process., vol. 66, no. 2,
p. 253–266, Feb. 2017.
[11] 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, 2017.
[12] C. Yu, X. Zhang, Z. Tang, and X. Xie, “Separable and error-free reversible
data hiding in encrypted image based on two-layer pixel errors,” IEEE
Access, vol. 6, pp. 76956–76969, 2018.
[13] L. Xiong, D. Dong, Z. Xia, and X. Chen, “High-capacity reversible
data hiding for encrypted multimedia data with somewhat homomorphic
encryption,” IEEE Access, vol. 6, pp. 60635–60644, 2018.
[14] H.-Y. Wang, H.-J. Lin, X.-Y. Gao, W.-H. Cheng, and Y.-Y. Chen,
“Reversible AMBTC-based data hiding with security improvement by
chaotic encryption,” IEEE Access, vol. 7, pp. 38337–38347, 2019.
[15] 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.
Y. Yang et al.: Secure and High Visual-Quality Framework for Medical Images

[17] 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 Security, vol. 8, no. 3, pp. 553–562, Feb. 2013.

[18] W. Zhang, K. Ma, and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Process., vol. 94, pp. 118–127, Jan. 2014.

[19] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” IEEE Trans. Cybern., vol. 46, no. 5, pp. 1132–1143, May 2016.

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

[21] W. Hong, T.-S. Chen, and H.-Y. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

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

[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 Security, vol. 13, no. 7, pp. 1670–1681, Jul. 2018.

[24] X. Wu, J. Weng, and W. Yan, “Adopting secret sharing for reversible data hiding in encrypted images,” Signal Process., vol. 143, pp. 269–281, Feb. 2018.

[25] C. Li, C. Xu, C. Gui, and M. D. Fox, “Distance regularized level set evolution and its application to image segmentation,” IEEE Trans. Image Process., vol. 19, no. 12, pp. 32–43, Aug. 2010.

[26] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[27] S. Weng, J. S. Pan, and L. Zhou, “Reversible data hiding based on the local smoothness estimator and optional embedding strategy in four prediction modes,” Multimedia Tools Appl., vol. 76, no. 11, pp. 13173–13195, 2017.

[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.

[29] S. Li, G. Chen, and X. Mou, “On the dynamical degradation of digital piecewise linear chaotic maps,” Int. J. Bifurcation Chaos, vol. 15, no. 10, pp. 3119–3151, 2005.

[30] Open Access Biomedical Image Search Engine. Accessed: 2019. [Online]. Available: https://openi.nlm.nih.gov

[31] 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.

[32] Y. Wu, Y. Zhu, Y. Yang, W. Zhang, and N. Yu, “A no-reference quality assessment for contrast-distorted image based on improved learning method,” Multimedia Tools Appl., vol. 78, no. 8, pp. 10057–10076, 2019.