Reversible Data Hiding Based Key Region Protection Method in Medical Images

Jian Li
Qilu University of Technology (Shandong Academy of Science)
Shandong Provincial Key Laboratory of Computer Networks
Jinan, China
ljian_20@163.com

Zelin Zhang
Qilu University of Technology (Shandong Academy of Science)
Shandong Provincial Key Laboratory of Computer Networks
Jinan, China
qluzzl@126.com

Shengyu Li
School of Computing
University of South Alabama
Mobile, AL, U.S.A.
sl1721@jagmail.southalabama.edu

Ryan Benton
School of Computing
University of South Alabama
Mobile, AL, U.S.A.
rbenton@southalabama.edu

Yulong Huang
College of Allied Health Professions
University of South Alabama
Mobile, AL, U.S.A.
yh1623@jagmail.southalabama.edu

Mohan Vamsi Kasukurthi
School of Computing
University of South Alabama
Mobile, AL, U.S.A.
mk1530@jagmail.southalabama.edu

Dongqi Li
School of Computing
University of South Alabama
Mobile, AL, U.S.A.
kevinldq2018@gmail.com

Jingwei Lin
Ocean School
Fuzhou University
Fuzhou, China
549841688@qq.com

Glen M. Borchert
Department of Pharmacology
University of South Alabama
Mobile, AL, U.S.A.
borchert@southalabama.edu

Shaobo Tan
School of Computing
University of South Alabama
Mobile, AL, U.S.A.
fantasyzhitsb@gmail.com

Bin Ma *
Qilu University of Technology (Shandong Academy of Science)
Shandong Provincial Key Laboratory of Computer Networks
Jinan, China
mab@qlu.edu.cn

Meihong Yang *
Qilu University of Technology (Shandong Academy of Science)
Shandong Provincial Key Laboratory of Computer Networks
Jinan, China
yangmh@sdas.org

Jingshan Huang *
School of Computing
University of South Alabama
Mobile, AL, U.S.A.
huang@southalabama.edu

***Abstract*—The transmission of medical image data in an open network environment is subject to privacy issues including patient privacy and data leakage. In the past, image encryption and information-hiding technology have been used to solve such security problems. But these methodologies, in general, suffered from difficulties in retrieving original images. We present in this paper an algorithm to protect key regions in medical images. First, coefficient of variation is used to locate the key regions, a.k.a. the lesion areas, of an image; other areas are then processed in blocks and analyzed for texture complexity. Next, our reversible data-hiding algorithm is used to embed the contents from the lesion areas into a high-texture area, and the Arnold transformation is performed to protect the original lesion information. In addition to this, we use the ciphertext of the basic information about the image and the decryption parameter to generate the Quick Response (QR) Code to replace the original key regions. Consequently, only authorized customers can obtain the encryption key to extract information from encrypted images. Experimental results show that our algorithm can not only restore the original image without information loss, but also safely transfer the medical image copyright and patient-sensitive information.**

***Keywords*—reversible data hiding, key region, QR code, image segmentation, texture complexity, selective encryption**

I. INTRODUCTION

In recent years, medical imaging research has made remarkable progress largely due to the rapid development of multimedia technologies. Medical images have become an indispensable and effective auxiliary means for modern medical diagnosis [1]. However, sharing and openness of these networks subject the transmission of medical images on potential exposure, and problems such as illegal copying, content tampering, and copyright loss are often encountered [2]. Due to this, interest in developing novel strategies to enhance medical image security has dramatically increased, particularly in the areas of information hiding and image encryption [3].

Reversible data hiding (RDH) embeds secret information into the carrier data and then completely extracts the secret information with no loss to the carrier data (lossless) [4–6]. In 1997, Barton [7] proposed the concept of reversible data hiding. Since that time, a large number of reversible data hiding schemes and algorithms have been proposed [8–10]. Celik et al. [11] proposed a compression-based reversible data hiding scheme, embedding secret data into the redundant space generated by image lossless compression, which has low computational complexity. In 2003, Tian [12] proposed a reversible data hiding algorithm based on difference expansion creating an extended reversible data hiding algorithm that extends the difference between two adjacent pixels into a vacant least significant bit. In order to avoid the overflow or underflow problem, the method uses location map technology, based on histogram shifting, which was first proposed by Ni et al. [13]. This algorithm constructs a histogram based on the pixel distribution of the original image and embeds information through histogram shifting. Most of the above medical image protection algorithms are primarily concerned with the

[*] Corresponding Authors: mab@qlu.edu.cn, yangmh@sdas.org, and huang@southalabama.edu

978-1-7281-1867-3/19/$31.00 ©2019 IEEE

978-1-7281-1867-3/19/$31.00 ©2019 IEEE

protection of image copyright and the enhancement of the visual quality of the embedded image.

However, information hiding technology focuses on image copyright protection, pursuing the confidentiality of watermark information and the authenticity of image content. Because of this, the protection of carrier image content is insufficient and security is low. In order to enhance the security of image transmission, most medical images are encrypted and transmitted to enhance image security.

Zahia [14] similarly proposed a selective encryption image scheme based on JPEG2000. This scheme combines the idea of permutation and selective encryption to reduce the amount of data encryption processed. The symmetric encryption AES in CFB mode the encrypts the exchange code blocks to improve image security. More recently, Hiba [15] combined reversible data hiding technology with standard encryption standards to provide image security at different stages while ensuring blindness in extraction and increasing the load capacity of the algorithm. However, the encrypted image has a small intrusive capacity and cannot carry large amounts of personal information and image information. Furthermore, due to the invisibility of the encrypted image, it is difficult to achieve secure retrieval in an open network environment making the encrypted medical image is extremely vulnerable to cyberattacks.

In this study, we present a medical image key information protection algorithm based on Quick Response Code (QR Code) [16]. Our algorithm begins by locating an image's key region (one that contains important pathological features or diagnosis and treatment information) then processes the other areas of the image in blocks. We propose a process that (a) allows for encryption of sensitive information (b) allows the embedding of patient information and (c) ensure the result is the same size as the original image. Importantly, this methodology offers several significant advantages for protecting medical image copyrights and patient information as compared to existing strategies.

The description of our algorithm and results are organized as follows. Section II introduces related work in Histogram shifting, Arnold Transformation, and QR Code technology, respectively. Section III describes our methodology in detail. Section IV reports experimental results of this study along with a detailed discussion, and finally, Section V concludes with future directions.

II. Related Work

A. Histogram Shifting

Reversible data hiding schemes based on histogram shift [13] have attracted extensive attention due to their low computational complexity and high image quality. The main steps are as follows:

Step 1: Generate the gray histogram of the original image (gray histogram shows the number of times the image pixel values appear, i.e. the frequency of pixels), find the peak point *P* and zero point *Z*, and store the peak point and zero point as auxiliary information.

Step 2: Traverse the whole image from left to right, top to bottom. The pixel between the zero point *Z* and the peak point *P* is shifted toward the zero point by one unit, and the gray histogram next to the peak point is vacated to create a space for embedding secret information. In equation (1), *h* represents the original pixel value and *h'* represents the shifted pixel value.

$$h' = \begin{cases} 0, & h = P+1 \\ h+1, & P \le h < Z \\ h-1, & Z < h \le P \end{cases} \quad (1)$$

Step 3: Images are scanned in the same order, and if the pixel value is equal to the peak pixel value *P*, hidden information is embedded. Assuming a rightward shift, if the information bit to be embedded is "1", the pixel value is increased by 1, and the pixel value is changed to *P+1*; if the information bit to be embedded is "0", the pixel value remains unchanged and is still *P*.

B. Arnold Transformation

Scrambling is a common image encryption method. So-called "scrambling" means to use certain rules to scramble the information sequence of the image, that is, to process the position or gray scale (color) of pixels in the image, to disturb its components, to destroy its correlation, and to transform it into unrecognizable pixel blocks or pixel point sets similar to white noise, thus improving image security.

Our algorithm uses Arnold transformation, which is an image pixel transformation theory proposed by Arnold [17], and is often called Cat Mapping. Cat Mapping can be seen as the process of cutting, splicing and rearranging pixels in a square digital image matrix. Through this process, we will obtain a new digital image matrix.

III. Methodology

A. Key Region Selection Scheme

For common medical images, the key region is a disease precursor region that provides diagnostic information. This region is rich in texture and high in information content, and contains important pathological features along with information about diagnosis and treatment. Complex texture means rich image information, along with the higher probability of lesion information in this region. The coefficient of variation is usually used to measure the degree of dispersion of different samples. The coefficient of variation is a normalized measure of the degree of dispersion. The larger the coefficient of variation is, the more information the image block contains. The smaller it is, the more unitary the gray scale of the image.

The coefficient of variation C_v is obtained according to equation (2), σ means standard deviation, and μ means the overall average. The original medical image is divided into non-overlapping blocks according to a certain size, the C_v value of each sub-block is calculated and sorted in blocks, and the image block with the largest C_v value is selected as the key region.

$$C_v = \frac{\sigma}{\mu} \quad (2)$$

B. Select the Texture Area as the Embedding Area

Mean Squared Error (MSE) can be used to evaluate the degree of image change, so this scheme uses MSE to calculate the texture complexity of the image. The MSE of each sub-block of the image is calculated according to equation (3). *m* and *n* respectively represent the rows and columns of the image, *I* represents the original image, and I_{ave} represents the pixel mean value of the image block. The MSE is sorted from small to large according to the position of the corresponding image block, the sequence of MSE is obtained by using the sorting algorithm, and the threshold value T is set. When the image block *MSE*>*T*, Treat the image block as an embedded area.

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j)-I_{\text{ave}}(i,j)\right]^2 \tag{3}$$

C. Patient QR Code Replacement Program

Our algorithm generates a QR Code by using the basic information of the medical image and the ciphertext of the parameters required for decryption. The basic information of the medical image includes the hospital information, the department information, the doctor information, the patient number, the image capturing time, the contact telephone number, and the medical image type. The ciphertext is produces by applying the RSA encryption algorithm to the parameters of Arnold transformation.

After generating the QR Code by using the information above, the QR Code is placed into the key region of the medical image as a 160*160 gray image block composed of 25,600 pixels. A smaller key area of 64*64 was tried. However, the smaller the size, the less accurate it is to find the lesion area. For a larger key area of 200*200, the actual embedding capacity is less than the required embedding capacity.

D. Information Embedding

This section introduces the embedding and encryption process of the image.

Step 1: Select key region. Each pixel value of the key region is converted into a binary form, which is used as the secret information of the binary stream to be embedded.

Step 2: According to the embedding area selection scheme, select the embedded area .

Step 3: The target pixel prediction is realized by using the four adjacent pixel points. $v_{i,j-1}$, $v_{i,j+1}$, $v_{i-1,j}$, and $v_{i+1,j}$, around each pixel, and the prediction error $d_{i,j}$ is obtained by subtracting the original pixel value $v_{i,j}$ from the prediction value $u_{i,j}$. The formula is as follows:

$$\begin{cases} u_{i,j}=\dfrac{v_{i,j-1}+v_{i,j+1}+v_{i-1,j}+v_{i+1,j}}{4} \\ d_{i,j}=\left\lfloor u_{i,j}-v_{i,j}\right\rfloor \end{cases} \tag{4}$$

Step 4: Generate a prediction error histogram of each image block, selecting pixel points with a prediction error of [-3, 3] as embedding points, translating to obtain an embedding space, and embedding secret information wherein the formula [*p, q*] represents an error selection range and *b* represents secret information [18], [19]. The formula is as follows:

$$D_{i,j}=\begin{cases} 2d_{i,j}+b, d_{i,j}\in[p,q] \\ d_{i,j}+q+1, d_{i,j}>q \\ d_{i,j}+p, d_{i,j}<p \end{cases} \tag{5}$$

Step 5: Arnold transformation is carried out on the embedded area, where the embedded area is divided into 8*8 image blocks.

Step 6: The basic information of the image and a section of ciphertext obtained by RSA encryption Arnold transformation related parameters are generated into a QR Code with the same size as the key region. The QR Code replaces the key region to obtain the encrypted image.

E. Information Extraction

This section introduces the decryption and recovery process of the image.

Step 1: Scan that QR Code of the image to obtain basic information and ciphertext of the image, and then decrypt using the key obtained through authorization to obtain plaintext.

Step 2: Decrypt with plaintext (Arnold transformation related parameters) to obtain decrypted images.

Step 3: Calculate MSE of each image block, sort from small to large, and select texture area and smooth area according to threshold *T*. Where the MSE value is greater than *T*, it belongs to the texture region and serves as the embedding region. Among them, the QR Code region is the key region and not the embeddable region.

Step 4: Perform diamond prediction on each embedded region image block based on the embedding sequence, predict the even layer first, then the odd layer, and then extract secret information by using equation (6).

$$b=D_{i,j}\bmod 2 \tag{6}$$

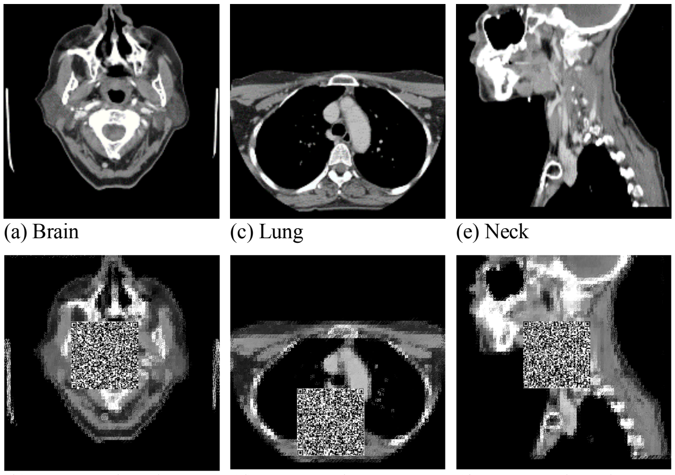
Step 5: Generate a prediction error histogram of each image block then translate and recover the image by using equation (7) .

$$d_{i,j}=\begin{cases} D_{i,j}/2, d_{i,j}\in[2p,2q+1] \\ D_{i,j}-q-1, d_{i,j}>2q+1 \\ D_{i,j}-p, d_{i,j}<2p \end{cases} \tag{7}$$

Step 6: The extracted secret information is recombined into data, and a one-dimensional array recombined into 160*160 image blocks by using consistent QR Code sizes. Image blocks are then merged into the key region to restore the original image.

IV. Experimental Results and Discussion

The experimental environment for this experiment is MATLAB 2016a, Intel(R) Core(TM) i7-6700 CPU processor. In order to evaluate the performance of the experimental protocol, we selected three standard grayscale medical images as the carrier image for experimental evaluation. Three DICOM format grayscale medical images (size of 512×512) have been selected from The Cancer Imaging Archive (TCIA) medical image database [20] to evaluate the performance of the proposed scheme. Fig. 3 shows the original image and the encryption effect. Experiments have been performed on 200 image instances in Brain System, Neck System, Respiratory System, and Bone Joint. Out of all these instances, 70% accurately blocked the informative region. Also, we support semi-automatic calibration of key regions. After the key area is embedded, the clinician will be able to add or adjust the key area.


(a) Brain (c) Lung (e) Neck

(b) Encrypted Brain (d) Encrypted Lung (f) Encrypted Neck

Fig. 1. Original and encrypted image examples.

Fig. 1 shows the original medical images and their corresponding encrypted images. It can be seen from the figure that the key region of the medical image and the surrounding texture areas are encrypted, the key regions are covered by the QR Codes, and the pixel positions of the surrounding texture areas are changed.

A. Embedded Image Extraction

In Fig. 2, (a) shows the original medical image and (b) the encrypted image. As can be seen from the figure, the key area of the medical image and the surrounding texture area are encrypted, the key area is covered by the QR Code, and the pixel bits in the surrounding texture area changed significantly. Panel (c) shows the scrambled decrypted image. Here, the key area in the image is also covered with the QR Code, and the other high-texture areas are embedded with the secret information, which is visually different from the original image. Panel (d) shows a reduced image after the secret information was extracted and the image block reconstituted into 160*160 replacing the QR Code region.

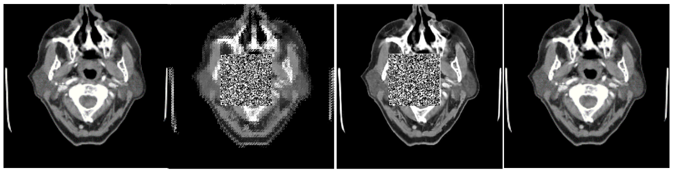

(a) Brain (b) Encrypted Image (c) Decrypted Image (d) Reduced Image

Fig. 2. Key regions in medical images.

TABLE I. PSNR AND SSIM OF THE FULLY ENCRYPTED AND RESTORED MEDICAL IMAGES

		PSNR	SSIM
Brain	Encryption	13.8033	0.4250
	Decryption	15.8551	0.6632
	Reduction	∞	1
Lung	Encryption	12.9810	0.5404
	Decryption	14.3018	0.7921
	Reduction	∞	1
Neck	Encryption	13.2778	0.4613
	Decryption	14.7978	0.7487
	Reduction	∞	1

Table I shows the fully encrypted images of the three experimental images. The Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) were obtained by scrambling the decrypted image and then comparing the restored image with the original image [5]. The higher the PSNR value, the smaller the change of visual quality and distortion degree after embedding the secret information. The higher the SSIM value, the higher the structural similarity of the algorithm. When PSNR is infinite, it means that the image is recovered without loss. When SSIM is 1, it also shows that the image is lossless. It can be seen that the PSNR and SSIM of the encrypted and decrypted images are not high, mainly because the 160*160 size key region image blocks are replaced, so that the PSNR and SSIM of the images are lower, and the restored PSNR and SSIM of the image proofs can be recovered without information loss while maintaining an extremely high level of data security.

B. Key Region for Conservation

Fig. 3 demonstrates the key image area of the brain. Fig.3 shows the key image area of an imaged lung. 3(a) is the key area of the original image which contains a lot of diagnostic information; 3(b) is the key area of the medical image extracted by the unauthorized user who tried to forcibly extract secret information. It is obvious that only the chaotic image can be obtained by unauthorized users. Therefore, the security of the image is greatly improved. 4(c) is the key area of the medical image extracted by the authorized user. After the user is authorized to obtain the key, the relevant parameters of the Arnold transformation are decrypted, and the image obtained by scrambling and decrypting is extracted to obtain the key area of the image.

Table II shows the PSNR and SSIM of the unauthorized and authorized extraction of the key areas of the three experimental images as compared with the key areas of the original image. Notably, the PSNR of the key areas not authorized for extraction is consistently less than 10, and the SSIM is less than 0.1.

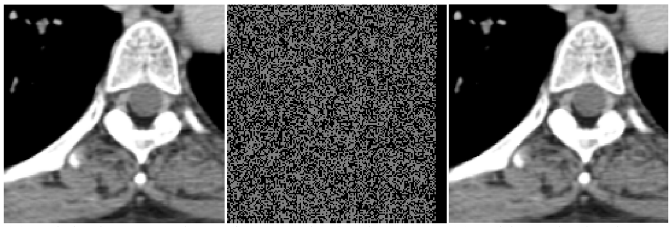

(a) Original Key Region Image (b) Unauthorized (c) With Authorization

Fig. 3. Example key regions in lung image.

TABLE II. PSNR AND SSIM OF UNAUTHORIZED AND AUTHORIZED EXTRACTION OF THE KEY AREAS IN MEDICAL IMAGES

		PSNR	SSIM
Brain	Unauthorized	7.8222	0.0093
	Authorized	∞	1
Lung	Unauthorized	7.2152	0.0182
	Authorized	∞	1
Neck	Unauthorized	7.0283	0.0060
	Authorized	∞	1

V. CONCLUSION

In this paper, a novel process was designed to allow for the storage of medical images in such a way that the key region information is removed, encrypted, and then embedded in the image itself. Our methodology also enables the flawless recovery of the entire image. As an added bonus, the addition of the QR code to the image permits us to obtain (a) mapping out of the key region, (b) the transmission of basic patient information, and (c) the transmission of the information needed to recover the image. The entire result is the same size as the original image; hence, we can replace the original image in storage without additional costs. The feasibility of the approach has been demonstrated on three medical images, representing three different areas of the human body.

The primary catch is that the original key needs to be known; the loss of the key would require that the original image would have to be accessed (unless it had been destroyed). However, this is a common issue with any encryption scheme. A secondary catch is, the software would need to be told to identify and find the QR code region; this can be done in a fairly trivial way fashion given the unnatural symmetry in three corners of the QR region.

Future work will include larger scale testing, including the computational costs. We will investigate how to use overlapping blocks to place the block several times on the lesion area, instead of applying the one-time placement of the non-overlapping blocks. It may result in higher accuracy. Additionally, we will explore cases where multiple regions are considered sensitive. Finally, we will study the effects of attacks seeking to compromise the image as well as defenses. The envisioned attacks can be alterations to the QR code (both the encrypted and unprotected) as well as attacks to the textured areas. Defenses will include the ability to determine what alterations occurred as well as the ability to recover from alternations.

ACKNOWLEDGMENT

This study was partially supported by National Natural Science Foundation of China (Nos: 61872203, 61802212 and 61502241).

REFERENCES

[1] H. Satoh et al., “Teleradiology network system on cloud using the web medical image conference system with a new information security solution,” in Medical Imaging 2013: Advanced PACS-based Imaging Informatics and Therapeutic Applications, 2013, vol. 8674, p. 86740X.

[2] T. Avudaiappan, R. Balasubramanian, S. S. Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, and K. Shankar, “Medical Image Security Using Dual Encryption with Oppositional Based Optimization Algorithm,” J Med Syst, vol. 42, no. 11, p. 208, Sep. 2018.

[3] C. Wang, X. Wang, Z. Xia, and C. Zhang, “Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm,” Information Sciences, vol. 470, pp. 109–120, Jan. 2019.

[4] B. Ma et al., “Adaptive error prediction method based on multiple linear regression for reversible data hiding,” J Real-Time Image Proc, vol. 16, no. 4, pp. 821–834, Aug. 2019.

[5] B. Ma, B. li, X.-Y. Wang, C.-P. Wang, J. Li, and Y.-Q. Shi, “A code division multiplexing and block classification-based real-time reversible data-hiding algorithm for medical images,” J Real-Time Image Proc, vol. 16, no. 4, pp. 857–869, Aug. 2019.

[6] B. Ma, B. Li, X.-Y. Wang, C.-P. Wang, J. Y. Li, and Y. Q. Shi, “Code Division Multiplexing and Machine Learning Based Reversible Data Hiding Scheme for Medical Image,” Security and Communication Networks, vol. 2019, pp. 4732632–4732632, 2019.

[7] J. M. Barton, “Method and apparatus for embedding authentication information within digital data,” US5646997A, 08-Jul-1997.

[8] 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.

[9] B. Ma and Y. Q. Shi, “A Reversible Data Hiding Scheme Based on Code Division Multiplexing,” IEEE Transactions on Information Forensics and Security, vol. 11, pp. 1–1, Sep. 2016.

[10] R. Gurusamy and V. Subramaniam, “A machine learning approach for MRI brain tumor classification,” Computers, Materials and Continua, vol. 53, pp. 91–109, Jan. 2017.

[11] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB Data Embedding,” Trans. Img. Proc., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[12] J. Tian, “Reversible Data Embedding Using a Difference Expansion,” Circuits and Systems for Video Technology, IEEE Transactions on, vol. 13, pp. 890–896, Sep. 2003.

[13] Zhicheng Ni, Yun-Qing Shi, N. Ansari, and Wei Su, “Reversible data hiding,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[14] Z. Brahimi, H. Bessalah, A. Tarabet, and M.-K. Kholladi, “Selective encryption techniques of JPEG2000 codestream for medical images transmission,” presented at the WSEAS Transactions on Circuits and Systems, 2008, vol. 7, pp. 1–4.

[15] H. Abdel-Nabi and A. Al-Haj, “Medical imaging security using partial encryption and histogram shifting watermarking,” in 2017 8th International Conference on Information Technology (ICIT), 2017, pp. 802–807.

[16] S. Tiwari, “An Introduction to QR Code Technology,” in 2016 International Conference on Information Technology (ICIT), 2016, pp. 39–44.

[17] V. I. Arnold and A. Avez, “Ergodic Problems of Classical Mechanics.,” ZAMM - Journal of Applied Mathematics and Mechanics / Zeitschrift für Angewandte Mathematik und Mechanik, vol. 50, no. 7–9, pp. 506–506, 1970.

[18] W. Puech, “Image Encryption and Compression for Medical Image Security,” 2008 First Workshops on Image Processing Theory, Tools and Applications, pp. 1–2, 2008.

[19] X. Wang, B. Ma, J. Li, and Y. Shi, “Adaptive image reversible data hiding error prediction algorithm based on multiple linear regression (In English),” Journal of applied science, p. 2018.

[20] “The Cancer Imaging Archive (TCIA),” The Cancer Imaging Archive (TCIA). [Online]. Available: //www.cancerimagingarchive.net/. [Accessed: 23-Oct-2019].