Computers, Materials & Continua CMC, vol.64, no.3, pp.1797-1817, 2020

Privacy Protection for Medical Images Based on DenseNet and Coverless Steganography

Yun Tan[1], Jiaohua Qin[1,*], Hao Tang[2], Xuyu Xiang[1], Ling Tan[2] and Neal N. Xiong[3]

Abstract: With the development of the internet of medical things (IoMT), the privacy protection problem has become more and more critical. In this paper, we propose a privacy protection scheme for medical images based on DenseNet and coverless steganography. For a given group of medical images of one patient, DenseNet is used to regroup the images based on feature similarity comparison. Then the mapping indexes can be constructed based on LBP feature and hash generation. After mapping the privacy information with the hash sequences, the corresponding mapped indexes of secret information will be packed together with the medical images group and released to the authorized user. The user can extract the privacy information successfully with a similar method of feature analysis and index construction. The simulation results show good performance of robustness. And the hiding success rate also shows good feasibility and practicability for application. Since the medical images are kept original without embedding and modification, the performance of crack resistance is outstanding and can keep better quality for diagnosis compared with traditional schemes with data embedding.

Keywords: Privacy protection, medical image, coverless steganography, DenseNet, LBP.

1 Introduction

With the development of wireless communication, cloud computing and artificial intelligence, the internet of medical things (IoMT) has become a high-profile application area. To meet the needs of diagnosis and research, medical images, as the most important part of medical data, are more and more widely transmitted and exchanged among different hospitals and research institutes around the world through Internet and mobile communication. Unlike other industries, the core content of the leaked data in the medical industry is private information, as well as clinical information containing examination results and diagnostic records. The relatively weak protection means and the high value of medical data are the two main factors leading to the growing risk of medical data, which has gradually become one of the bottlenecks restricting the wide application of IoMT. It is urgent to strengthen the information security and privacy protection of medical images during transmission, storage and usage. In one hand, the

[1] College of Computer Science and Information Technology, Central South University of Forestry & Technology, Changsha, 410114, China.

[2] The Second Xiangya Hospital of Central South University, Changsha, 410011, China.

[3] Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, 74464, USA.

[*] Corresponding Author: Jiaohua Qin. Email: qinjiaohua@163.com.

Received: 30 March 2020; Accepted: 29 April 2020.

private and confidential information should not be arbitrarily leaked, stolen, misused and abused. In another hand, the quality and reliability of medical images should be ensured.

Cryptography and steganography are the most common methods for privacy protection, which have been applied widely for medical images [Kavitha and Saraswathi (2017), Dorgham, Al-Rahamneh, Almomani et al. (2018)]. Cryptography usually disorders the original information in order to make it incomprehensible, and thereby avoid illegal acquisition. Chai et al. [Chai, Zhang, Gan et al. (2019)] proposed a scheme based on Latin square and chaotic system to help privacy protection. A quantum selective encryption method was proposed by Heidari et al. [Heidari, Naseri and Nagata (2019)], which was more time-efficient compared with other schemes. Digital watermarking and steganography usually need to embed the secret or copyright information to the carrier and try to achieve best imperceptibility and robustness [Xiang, Wu, Li et al. (2018), Tan, Qin, Xiang et al. (2019), Wan, Wang, Li et al. (2020)]. Fakhari et al. [Fakhari, Vahedi and Lucas (2011)] proposed a watermarking approach based on wavelet transformation for medical images protection, which used variable parameters and places for embedding. It shew good invisibility and robustness for common attacks. A reversible data hiding scheme in medical images was proposed by Yang et al. [Yang, Zhang, Liang et al. (2016)]. Information was embedded into the texture area to improve the quality of diagnosis part. Al-Dmour et al. [Al-Dmour and Al-Ani (2016)] proposed a private information hiding scheme based on edge detection and coding mechanism. IWT-SVD transform was used in watermarking by Priyanka et al. [Priyanka and Maheshkar (2017)], which was combined with LSB embedding to realize privacy protection and tamper detection. Recently, Lee [Lee (2019)] proposed an adaptive reversible watermarking algorithm based on estimated error expansion, which shew good performance on capacity and perceptual quality. However, all these methods need to modify the original medical images by embedding or disorder, which will result in the variation of the information characteristics. This kind of methods based on traditional steganography may be detected by steganalysis [Kang, Liu, Yang et al. (2019)]. Therefore, the hidden private information is possible to be intercepted, which lead to further risk of illegal copying, dissemination and tampering. At the same time, the quality of medical images has been affected more or less.

Recently coverless steganography has become a research hotspot. It mainly analyses and extracts the features of the carrier image or text, then establishes certain correlated mapping rules between the features and secret information [Qin, Luo, Xiang et al. (2019), Zhou, Qin, Xiang et al. (2020)]. At the receiver, the authorized user can use the mapping relationship to extract secret information. Since no modification has been made to the carrier, the quality of the original carrier can be guaranteed and the anti-steganalysis ability can be enhanced. Zhou et al. [Zhou, Sun, Harit et al. (2015)] used robust hash algorithm to generate hash sequence as the earliest scheme of coverless steganography. Subsequently the histograms of oriented gradients (HOG) was used [Zhou, Wu and Yang (2017)]. Zheng et al. [Zheng, Wang, Ling et al. (2017)] used the information of scale-invariant feature transform (SIFT) feature points to design image hash. Later, the average pixel values of sub-images were calculated and used for information mapping [Zou, Sun, Gao et al. (2018)]. Recently, discrete cosine transform (DCT) [Zhang, Peng and Long (2018)] and discrete wavelet transform (DWT) [Liu, Xiang, Qin et al. (2020)] of adjacent blocks were used to generate a robust feature sequence and shew good performance. In a

word, how to extract carrier features and construct mapping rules between secret information and carrier features are the key points of coverless steganography algorithm based on feature mapping.

In this work, we focus on the private protection issue of medical images based on coverless steganography. The paper is organized as follows: we describe the motivation of our work in Section II. Preliminaries are introduced in Section III and the proposed method is described in Section IV. Experimental results and comparisons are shown in Section V. Finally, we conclude this paper in Section VI.

2 Motivations

For most medical images, the private information of patients and medical institutions are usually displayed directly on the images for convenience, as shown in Fig. 1. Therefore, if the medical images are leaked or illegally used, it could cause great mental damage to patients, and may even lead to huge economic losses, resulting in adverse social impact. At the same time, other privacy information such as clinical information is often saved independently, which can easily lead to information confusion and inconvenient use. How to hide the privacy information in the images and reduce the risk of privacy information leakage is a very important issue. The existing traditional schemes has two defects: the inadequate resistance to steganalysis and the impact on the original medical images. This situation prompts us to improve the privacy protection problem of medical images.

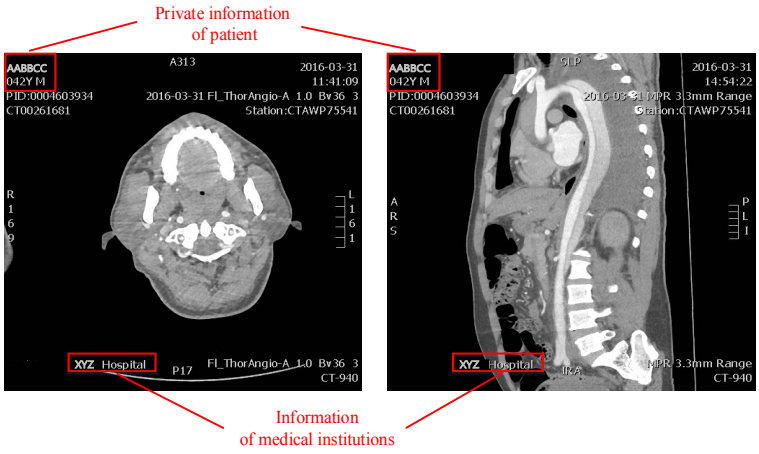

Figure 1: Examples of medical images

We think the coverless steganography is suitable for private protection of medical images based on the two considerations as follows:

1) Medical image is an important basis for doctors to obtain pathological information of patients and make a diagnosis. The quality of medical image data is extremely strict and cannot be modified. Coverless steganography won't modify the carriers.

2) In order to resist the attack risks in IoMT applications, the ability of anti-steganalysis and robustness are quite essential. Coverless steganography has shown good performance in this respect.

However, the characteristics of medical images are different from natural images. Medical images are mostly gray-scale images with black background. Different image contents may have similar gray-scale information. Noise, artifacts and geometric distortion may be introduced in the process of medical imaging. Thus, the existing coverless steganography algorithms based on natural images cannot be directly transplanted to medical images.

At the same time, the methods based on neural network learning have been applied widely on data processing and analysis in IoT applications [Wang, Kong, Guan et al. (2019)]. Especially with the development of deep learning algorithms, it has shown outstanding performance of feature learning and extraction [Wang, Qin, Xiang et al. (2019)]. Therefore, the deep learning network can be considered to distinguish the subtle feature differences between medical images.

The main contributions of this work are as follows: firstly, we construct a novel privacy protection scheme of medical images based on DenseNet and coverless steganography. Secondly, the mapping algorithm between the features of medical images and hidden information is proposed. Finally, the performance of the proposed scheme is analyzed and the feasibility of the proposed scheme is considered.

3 Preliminaries

3.1 Densely connected convolutional network

Convolutional neural network has become one of the most important network structures of deep learning. The number of network layers continues to increase, which brings the problems of model degradation and gradient vanishing. At the same time, the number of parameters also increases. In order to solve these problems, densely connected convolutional network (DenseNet) was proposed by Huang et al. [Huang, Liu, Maaten et al. (2017)]. As shown in Fig. 2, there are direct connections between each two layers in DenseNet. Therefore, each layer uses the features of all the previous layers as its inputs, and also uses its own features as the inputs of all the subsequent layers. Assuming the network has L layers, then the number of connections N is:

$$N = \frac{L(L+1)}{2} \tag{1}$$

The output of the lth layer is:

$$x_l = H_l([x_0, x_1, ..., x_{l-1}]) \tag{2}$$

where x_i is the output of the ith layer and H_l is the non-linear transformation operation including batch normalization, ReLU, pooling and convolution.

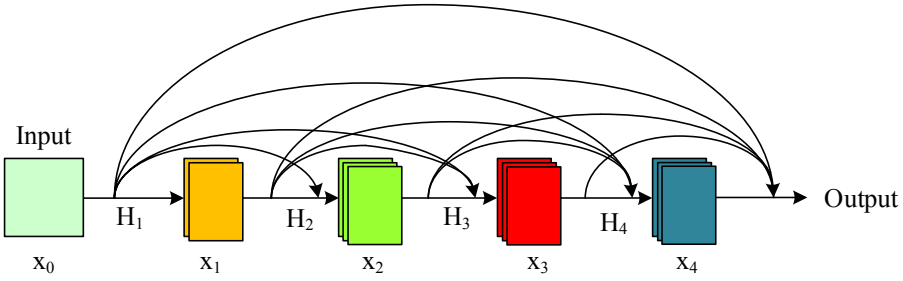

Figure 2: Concept of dense connection

Compared with other networks, DenseNet has two main advantages as follows:

1) It can distinct the information as reserved or transmitted to the network. Only small part of feature maps will be added to the network and the rest of the feature maps are unchanged. Thus it needn't to relearn redundant feature maps and only requires fewer parameters than traditional convolutional networks.

2) Each layer has direct access to the gradients from the loss function and the original input signal, thereby the information flow and gradients throughout the network is improved. Therefore, the problems of gradient vanishing and model degradation are alleviated. And the training of the network is also simplified.

Based on these two benefits, DenseNet is suitable for feature extraction in real time applications [Luo, Qin, Xiang et al. (2019)].

3.2 Robust PCA

Principal Component Analysis (PCA) is one of the most widely used data dimension reduction algorithms, which can remove some redundant information and noise from the data and make the data simpler and more efficient. Assuming the high-dimensional data as $\mathbf{D} \in \mathbb{R}^{m \times n}$, the goal of PCA is to estimate the low-dimensional subspace as $\mathbf{M}$ with minimum error deviation $\mathbf{S}$. This mathematical problem can be expressed as Eq. (3):

$$\min_{\mathbf{M},\mathbf{S}} \|\mathbf{S}\|_F, s.t.\ \mathbf{D} = \mathbf{M} + \mathbf{S}, \text{rank}(\mathbf{M}) \ll \min(m, n) \tag{3}$$

where $\|\cdot\|_F$ is the Frobenius norm. In order to solve Eq. (3), many algorithms have been proposed such as singular value decomposition (SVD) based method, which is proved to be effective for small additive noise. Furthermore, in order to solve the estimation problem of $\mathbf{M}$ even with large error $\mathbf{S}$, robust PCA has been raised and also attracted wide attention. This problem can be expressed as:

$$\min_{\mathbf{M},\mathbf{S}} \|\mathbf{M}\|_* + \lambda \|\mathbf{S}\|_1, s.t.\ \mathbf{D} = \mathbf{M} + \mathbf{S} \tag{4}$$

where $\|\cdot\|_*$ is the matrix nuclear norm, λ is a weight factor, and $\|\cdot\|_1$ denotes the l_1 norm. Lin et al. proposed an inexact augmented Lagrange multipliers (IALM) algorithm to solve this problem, which has good performance of convergence speed [Lin, Chen and Ma (2013)].

3.3 Local binary pattern

Local binary pattern (LBP) is an operator used to describe the local texture features of an image, which was proposed by Ojala et al. [Ojala, Pietikainen and Harwood (1996)]. It has remarkable advantages such as rotation invariance and grayscale invariance and has been applied widely in face recognition and target detection.

For a given grayscale image, assuming a pixel (x, y) with intensity i and its neighbor pixel has the intensity i_n. Set (x, y) as central pixel and is compared with the gray value of adjacent pixels. If the surrounding pixel i_n is larger than the central pixel value i, the flag value $s(n)$ of the pixel position is marked as 1, otherwise as 0 in Eq. (5):

$$s(n) = \begin{cases} 1, i_n > i \\ 0, i_n < i \end{cases} \tag{5}$$

where n means the nth pixel of neighbor area. Then the LBP value of (x,y) is calculated according to

$$\mathrm{LBP}(x, y) = \sum_{n=0}^{N} 2^N s(n) \tag{6}$$

where N is the total number of neighbor pixels, $s(n)$ is the flag value of the nth pixel position calculated previously.

4 Proposed privacy protection scheme for medical images

4.1 Deployment setting

The deployment setting structure of our scheme in IoMT is described in Fig. 3. The medical images group achieved by modern medical imaging equipment are transmitted to edge computing, which will finish the privacy protection process. Then the medical images group are packed together with the mapping indexes of privacy information and sent to medical image cloud platform. The authorized user can download the medical images package and extract privacy information successfully, which can be used for diagnosis normally.

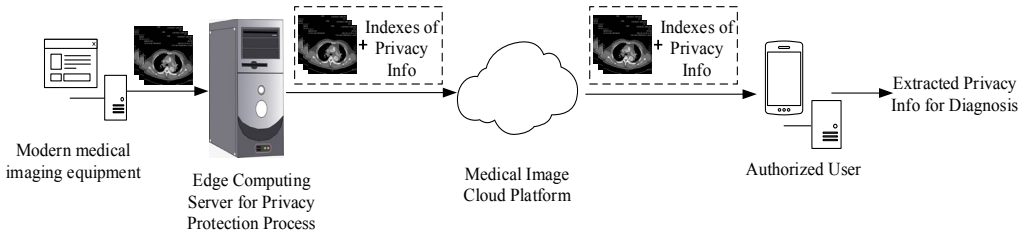

Figure 3: Deployment setting structure in IoMT

4.2 Framework of proposed scheme

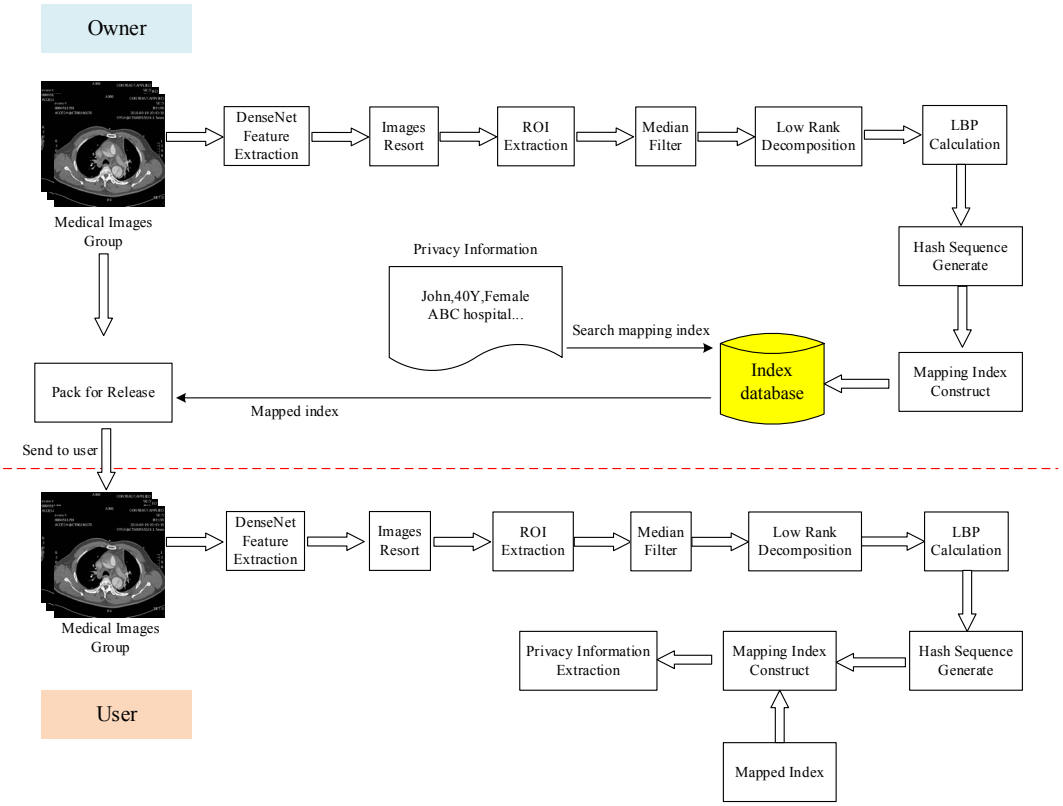

Figure 4: Framework of proposed privacy protection scheme for medical image

The framework of the proposed privacy protection scheme for medical images is shown in Fig. 4. For a given group of medical images of one patient, DenseNet is used to extract the features of the medical images. Then the images are sorted by the DenseNet feature similarity. For the regrouped images, LBP feature will be calculated and the indexes for subsequent information mapping will be constructed. The corresponding mapped indexes of secret information will be packed together with the medical images group and released to the authorized user. Then the user can extract the privacy information with the similar method of feature analysis and index construction. The specific steps of our scheme are shown below:

1) For the medical images group, DenseNet is used to extract features of every image. Then the images are reordered according the mutual feature similarity of each two images.

2) For every medical image, only part of the image region contains meaningful features, such as human tissues, organs, etc. Therefore, region of interest (ROI) is extracted firstly in order to eliminate the interference of text region and background noise points.

3) Median filter is applied for noise removal of ROI.

4) For the preprocessed image, low rank decomposition is applied to obtain the stable patterns and remove the sparse part component [Yang, Yin and Yang (2019)].

5) Divide the low rank image to sub-blocks and LBP feature is calculated for each subblock. LBP feature matrix is constructed for each image.

6) The feature difference matrix of neighbor images is calculated and the Hash sequence is generated.

7) Mapping index database is constructed based on the generated hash sequence. The index is sorted by hash value and mapped to letters "a"~"Z" and numbers "0"~"9" in turn.

8) For the private information such as name, age, gender, medical institutions, etc., search corresponding mapped indexes from index database.

9) The index numbers are packed together with medical images group for release to user.

10) At receiver, Steps 1) to 7) is repeated to construct the same index database. From the mapped index number, the corresponding row of feature difference matrix can be found. Then the hash sequence can be generated and privacy information can be recovered through demapping from letters "a"~"Z" and numbers "0"~"9" to hash value.

Through the above procedure, the privacy protection and transmission are implemented successfully for medical images.

4.3 DenseNet feature extraction and similarity measure

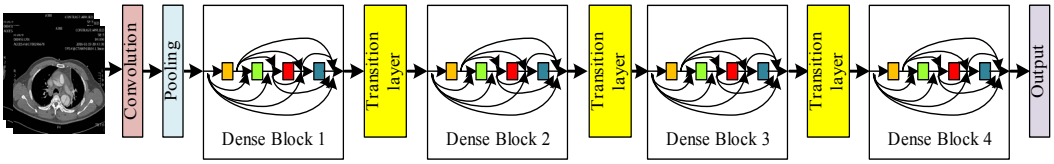

Figure 5: DenseNet feature extraction

In order to ensure the order of the images in the group, we use DenseNet to extract the features. The structure of DenseNet feature extraction is shown in Fig. 5.

DenseNet is mainly composed by DenseBlock and transition layer. There are 4 DenseBlocks and 3 transition layers. Since we only focus on the extracted features, the classification layer is not needed. The DenseNet is pre-trained and shared by both owner and user in real applications, which can ensure the efficiency of the scheme. Assuming the extracted feature of ith image is $\boldsymbol{f}_i$, then the feature vectors of the image group is

$$\mathbf{F}=\{\boldsymbol{f}_1, \boldsymbol{f}_2, \ldots \boldsymbol{f}_n\} \tag{7}$$

where n is the number of medical images in the image group. Euclidean distance is used to measure the similarity of the features. For feature vector $\boldsymbol{f}_x$ and $\boldsymbol{f}_y$, their Euclidean distance d_{xy} can be calculated as follows:

$$d_{xy} = \sqrt{\sum_{i=1}^{m} (f_{x\_i} - f_{y\_i})^2} \tag{8}$$

where m is the dimension of the feature vector, f_{x_i} and f_{y_i} are the ith elements of feature vector $\boldsymbol{f}_x$ and $\boldsymbol{f}_y$ respectively. Then we can achieve the similarity matrix **D** as follows:

$$\mathbf{D}=\begin{vmatrix} d_{11}\ d_{12}\ldots d_{1m} \\ d_{21}\ d_{22}\ldots d_{2m} \\ \ldots \\ d_{m1}\ d_{m2}\ldots d_{mm} \end{vmatrix} \tag{9}$$

Here **D** is a symmetric matrix. We can select any column of similarity values as the benchmark and reorder the medical images.

4.4 ROI extraction

For medical images, the pixels of ROI have obvious higher gray value, as shown in Fig. 6. In order to extract the ROI, the grayscale threshold h_g is used to obtain the segment binary image $\mathbf{I_s}$ as follows:

$$I_s(x,y)=\begin{cases} 1, if\ \ I(x,y)>h_g \\ 0, if\ \ I(x,y)\le h_g \end{cases} \tag{10}$$

where $I\ (x, y)$ is the pixel of original image and $I_s\ (x, y)$ is the pixel of segment binary image. h_g is the threshold, which can be set as a certain value or calculated by maximum variance method. In order to further remove the text part from $\mathbf{I}_s$, the properties of connected areas are measured. If the connected areas are smaller than the threshold h_a, it will be eliminated from the binary image and the modified binary image $\mathbf{I}_s'$ is obtained. Then the dot multiplication is applied for the original image and the binary image as Eq. (11):

$$\mathbf{I_R}=\mathbf{I}\odot\mathbf{I}_s' \tag{11}$$

where $\odot$ means dot multiplication, $\mathbf{I_R}$ is the segmented image of ROI. The whole process is shown in Fig. 6.

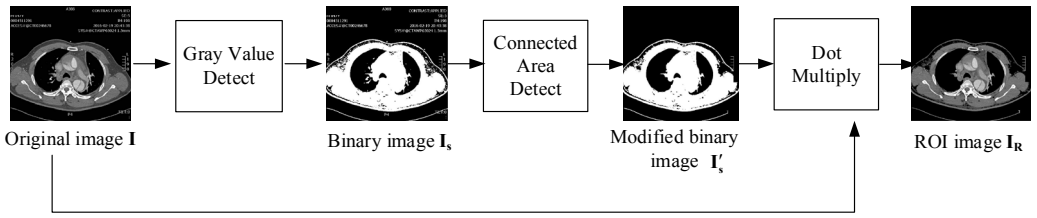

Figure 6: Process of ROI extraction

4.5 Low rank decomposition

With low rank decomposition, the image matrix **D** can be separated as two parts:

$$\mathbf{D}=\mathbf{M}+\mathbf{S} \tag{12}$$

where **M** is the stable course structure part and **S** is the sparse part [Yang, Yin and Yang (2019)]. We can define the augmented Lagrangian function as Eq. (13):

$$L(X,Y,\mu)=f(X)+\langle Y,h(X)\rangle+\frac{\mu}{2}\|h(X)\|_F^2 \tag{13}$$

where $\langle Y,h(X)\rangle=\mathrm{tr}(Y^T h(X))$ and μ is a positive scalar. The decomposition can be implemented by IALM algorithm as Algorithm 1 [Lin, Chen and Ma (2009)]. It has been proved that the IALM algorithm will converge if $\{\mu_k\}$ is non-decreasing and $\sum_{k=1}^{+\infty}\mu_k^{-1}=+\infty$.

Algorithm 1: IALM

Input: $\mathbf{D}\in\mathbb{R}^{m\times n}$, positive weighting parameter λ

Output: $\mathbf{M}_k$, $\mathbf{S}_k$

1: Initialize as $J(\mathbf{D})=\max(\|\mathbf{D}\|_2,\lambda^{-1}\|\mathbf{D}\|_\infty)$, $\mathbf{Y_0}=\mathbf{D}/J(\mathbf{D})$, $S_0=0$, $\mu_0>0$, $\rho>1$, $k=0$

2: Solve $\mathbf{M}_{k+1}=\arg\min_{\mathbf{M}} L(\mathbf{M},\mathbf{S}_k,\mathbf{Y}_k,\mu_k)$

3: Solve $\mathbf{S}_{k+1}=\arg\min_{\mathbf{S}} L(\mathbf{M}_{k+1},\mathbf{S},\mathbf{Y}_k,\mu_k)$

4: $\mathbf{Y}_{k+1}=\mathbf{Y}_k+\mu_k(\mathbf{D}-\mathbf{M}_{k+1}-\mathbf{S}_{k+1})$

5: Update μ_k to μ_{k+1}

6: k=k+1

7: Repeat Steps 2 to 6 until converge

4.6 LBP feature extraction

We use LBP to describe the texture feature of medical image, which has good robustness against brightness variation and angle rotation. However, the original LBP feature has similar size as original image. Therefore, we construct an LBP feature matrix.

The whole process of LBP feature extraction is shown in Fig. 7. Firstly, the low rank component image **M** is divided to four blocks as $\mathbf{M_1}$, $\mathbf{M_2}$, $\mathbf{M_3}$ and $\mathbf{M_4}$. Secondly, LBP operator is calculated for every block. Thirdly, every LBP block is further divided into 9 sub-blocks. The sum of all the LBP elements of every sub-block is calculated. Finally, the LBP feature matrix **L** is constructed.

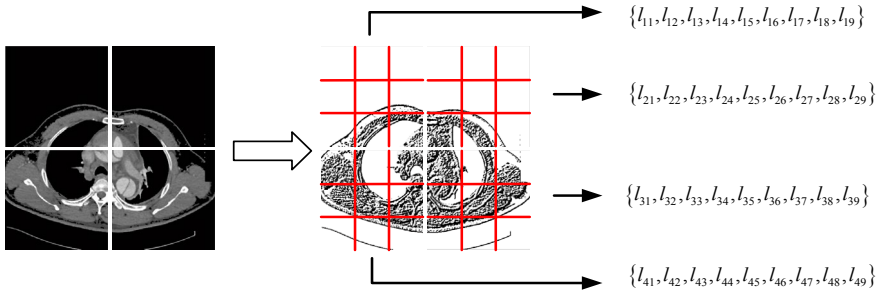

Figure 7: LBP calculation

The algorithm is described in Algorithm 2.

Algorithm 2: LBP Calculation

Input: image set $\mathbf{M}=\{\mathbf{M_1}, \mathbf{M_2}, \mathbf{M_3}, \mathbf{M_4}, \ldots, \mathbf{M_N}\}$
Output: LBP feature matrix **L**
1: Initialize m as 0, initialize **L** as all zero matrix
2: For k=1 to N
3: Divide $\mathbf{M}_k$ to $\mathbf{M}_{k1}$, $\mathbf{M}_{k2}$, $\mathbf{M}_{k3}$, $\mathbf{M}_{k4}$
4: for i=1 to 4
5: m=m+1;
6: $\mathbf{B}_i$=LBP_Calc($\mathbf{M}_{ki}$)
7: Divide $\mathbf{B}_i$ to $\mathbf{B}_{i1}$, B_{i2}, …, $\mathbf{B}_{i9}$
8: for j=1 to 9
9: l_{mj}=sum($\mathbf{B}_{ij}$)
10: end
11: end
12: end

Then the hash sequences are generated based on the elements of difference feature matrix as follows:

$$b_{mi} = \begin{cases} 0, \text{ if } w_{mi} < thres \\ 1, \text{ if } w_{mi} \geq thres \end{cases} \tag{14}$$

and

$$thres = \frac{1}{9}\sum_{i=1}^{9} w_{mi} \tag{15}$$

where w_{mi} is the (m, i) element of matrix **W**. Each row of the difference feature matrix corresponds to a hash sequence $b_{m1}b_{m2}b_{m3}...b_{m9}$. The algorithm is described below.

Algorithm 3: Hash sequence generation

Input: LBP feature matrix **W**, number of images N
Output: hash sequence set **B**
1: Initialize **B**=∅
2: For m=1 to $4\times(N-1)$
3: for i=1 to 9
4: b_{mi}=Hash(w_{mi})
5: end
6: **B**={**B**, $b_{m1}b_{m2}b_{m3}...b_{m9}$}
7: end

4.8 Index table construction

In order to realize the protection of privacy information, the basic idea is to construct a related mapping rule between the secret information and the generated hash sequences. Since the hidden information is usually text consisting of letters and numbers, we sort the generated hash sequences and map them with the character table. In order to extract the hidden information efficiently, the source of the hash sequence should also be recorded in the table. As shown in Fig. 8, the mapping index table is constructed by 3 columns: Character, Hash Sequence and RowNum. Character includes 62 characters from lower case "a" to capital "Z" and the number "0" to "9". Hash Sequence is generated from the medical image by the method described in previous Section 4.4, which is sorted from small to large. RowNum means the row number of the difference feature matrix that generates the corresponding hash sequence, with which the authorized user can extract the hidden privacy information conveniently from the medical images group.

Character	Hash Sequence	Row Num
"a"	000000101	1,9,27
"b"	000000111	13
...	...	...
"Z"	100100001	2,6
"0"	100100100	152
"1"	100100110	456
...	...	...
"9"	111110000	356, 431

Figure 8: Structure of mapping index

4.9 Privacy protection and extraction

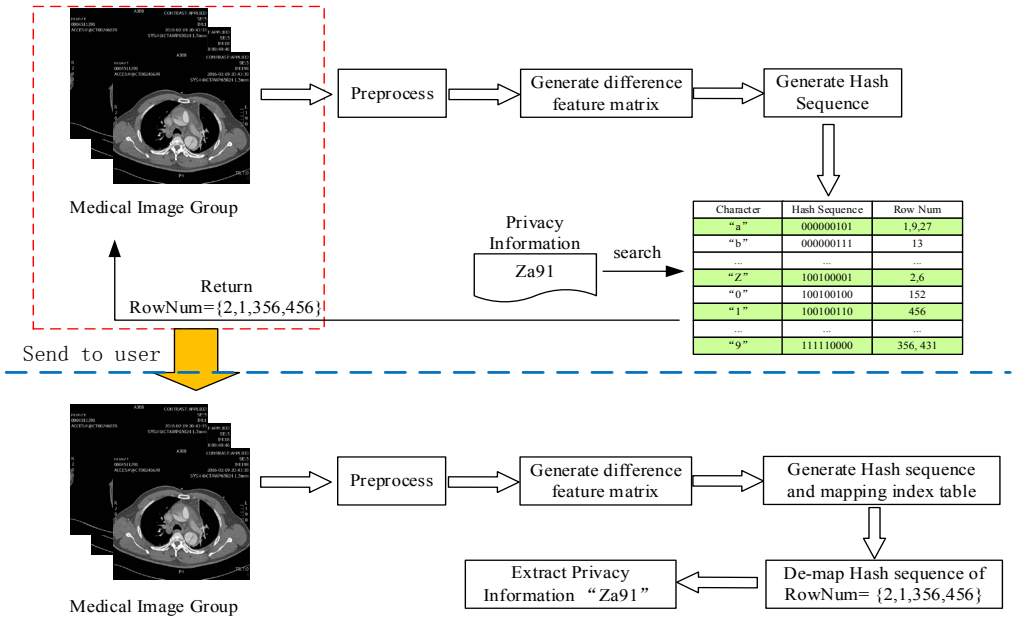

Figure 9: Example of privacy protection procedure

For a given group of medical images, the privacy information can be mapped to the hash sequences according to the mapping index table. Then the corresponding row number can be packed together with the medical images and delivered to the authorized user. At the receiver, the privacy information can be extracted successfully based on the received row number.

In Fig. 9, there is an example that shows the whole process. Assuming the privacy information is "Za91", firstly the medical groups will be preprocessed including reorder based on DenseNet features, ROI extraction, median filtering and low rank decomposition. Then the LBP feature is calculated, which will generate the feature difference matrix. After hash sequence generation, the mapping index table can be constructed. Next, the corresponding index item of privacy information "Za91" can be found, as marked with green in Fig. 9. Since there are multiple row numbers for the same hash sequence, we can choose anyone randomly. Here the first RowNum of every index item is selected as {2, 1, 356, 456}. Finally, the RowNum set is packed together with the medical image group and sent to the user. The user can generate the hash sequence and mapping index table similarly. After demapping the hash sequences of the items with RowNum as {2, 1, 356, 456}, the privacy information "Za91" can be extracted successfully.

5 Experimental results and analysis

Intel (R) Core i7-6500X CPU @ 2.5 GHz is used for the experiments. The algorithm is simulated by Matlab 2018a and MySQL workbench 6.3. Ten groups of CTA medical images are used for robustness experiments, which come from the clinical data of the

department of cardiovascular surgery in the Second Xiangya Hospital of Central South University in China. Each group contains 500~700 images of the same patient and each image has 512×512 pixels. In Fig. 10, part of the test images in one group are shown. It can be seen that the images have high correlation and similarity.

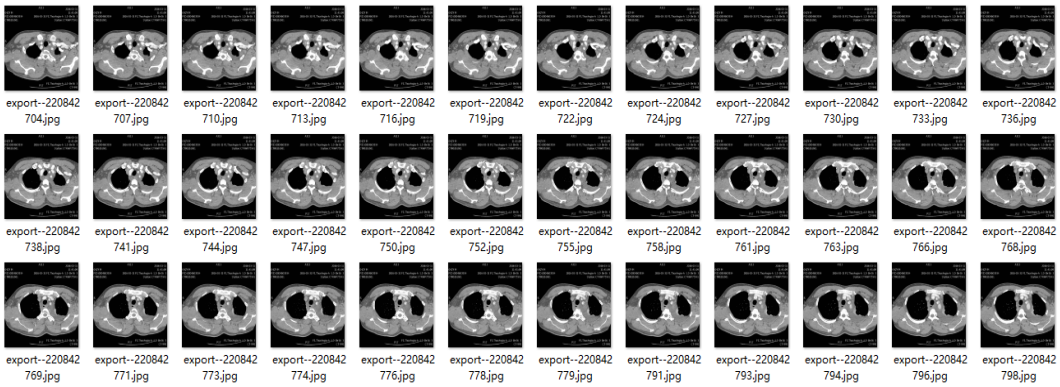

Figure 10: Part of the test medical images

5.1 Robustness analysis

The robustness against attacks is simulated in this section. The bit accuracy and block accuracy are analyzed.

Table 1: Accuracy with different attacks

Attack		*Bit Accuracy*	*Block Accuracy*
Gauss noise	σ=0.01	0.9863	0.8814
	σ=0.005	0.9908	0.9204
	σ=0.001	0.9934	0.9423
Speckle noise	σ=0.01	0.9932	0.9407
	σ=0.005	0.9938	0.9454
	σ=0.001	0.9945	0.9516
Salt & pepper noise	σ=0.01	0.9938	0.9454
	σ=0.005	0.9941	0.9501
	σ=0.001	0.9955	0.9641
Median filtering	3×3	0.9922	0.9329
	5×5	0.9882	0.9329
	7×7	0.9816	0.8424
Mean filtering	3×3	0.9638	0.7239
	5×5	0.9683	0.7598
	7×7	0.9657	0.7161
Gauss filtering	3×3	0.9939	0.9501

	5×5	0.9939	0.9470
	7×7	0.9941	0.9485
Intensity adjust	Gamma=0.5	0.9889	0.9048
	Gamma=0.7	0.9905	0.9142
	Gamma=1.3	0.9743	0.8003
Edge cropping	10%	0.9853	0.8705
	20%	0.9685	0.7504
Rotate	10°	0.8851	0.2839
	20°	0.8005	0.1045
Scaling	0.3	0.9825	0.8518
	0.5	0.9898	0.9111
	1.5	0.9889	0.9033
Gamma Correction	0.8	0.9794	0.8268
	0.9	0.9873	0.8924
JPEG compression	Q=10	0.9936	0.9423
	Q=50	0.9938	0.9485

Assuming the original bits are $b_1b_2...b_m$ and the extracted bits at receiver are $b_1'b_2'...b_m'$, then the bit accuracy is:

$$Acc\_bit = 1 - \frac{\sum_{i=1}^{m} c_i}{m}, c_i = b_i \oplus b_i' \tag{16}$$

Since in our scheme, the hash sequences are mapped to characters one by one. Even one bit error may lead to the wrong detection of one character. Therefore, we take a hash sequence $b_{i1}b_{i2}...b_{i9}$ as a block and the total number of block is *N*, then the block accuracy is more meaningful, which is defined as:

$$Acc\_block = \frac{\sum_{i=1}^{N} f(i)}{N} \tag{17}$$

and

$$f(i) = \begin{cases} 1, & \text{if } b_{i1}'b_{i2}'...b_{i9}' \oplus b_{i1}b_{i2}...b_{i9} = 0 \\ 0, & \text{if } b_{i1}'b_{i2}'...b_{i9}' \oplus b_{i1}b_{i2}...b_{i9} \neq 0 \end{cases} \tag{18}$$

Table 2: Robustness comparison with different methods

Attack Types		*Pixel Method*	*SIFT Method*	*DCT Method*	*DWT Method*	*Proposed Method*
Gauss noise	σ=0.001	0.9907	0.7991	0.9829	**0.9969**	0.9423
Salt & Pepper	σ=0.001	**0.9921**	0.8894	0.9766	0.9891	0.9641
Speckle noise	σ=0.01	**0.9907**	0.7617	0.9782	0.9844	0.9407
Median filtering	3×3	0.7399	0.1464	0.7399	0.9050	**0.9329**
Mean filtering	3×3	0.9875	0.9673	0.9876	**0.9953**	0.7239
Gauss filtering	3×3	0.9953	0.3847	0.9953	**0.9984**	0.9501
Edge cropping	20%	0.3723	0.0093	0.3723	**0.8396**	0.7504
Rotate	10	0.0701	0.0016	0. 0701	0.0748	**0.2839**
Scaling	3	**0.9984**	0.9891	**0.9984**	0.9969	0.9454
JPEG compression	Q=10	0.8676	0.7819	**0.8676**	0.8302	0.7254
Gamma Correction	0.8	**0.9050**	0.6293	**0.9050**	0.7990	0.8268

The bit accuracy and block accuracy with different attacks are shown in Tab. 1. It can be seen that the proposed scheme has good robustness against different attacks including Gauss noise, speckle noise, salt and pepper noise, median filtering, Gauss filtering, intensity variation, scaling and edge cropping, which can achieve bit accuracy as high as 0.98 and the block accuracy is close or even higher than 0.80.

We also use the methods based on pixel [Zhou, Sun, Harit et al. (2015)], SIFT [Zheng, Wang, Ling et al. (2017)], DCT [Zhang, Peng and Long (2018)] and DWT [Liu, Xiang, Qin et al. (2020)] on medical images and compare the robustness performance with our scheme, as in Tab. 2. Here the accuracy means block accuracy. It is shown that our proposed scheme has better performance with median filtering and rotation. Although the overall performance of DWT method is best, but it is not suitable for medical images, which will be tested in next subsection.

5.2 Practicability analysis

In the proposed scheme, theoretically each image can generate 4 hash sequences. However, usually the medical images have high correlation and similarity. There is a high probability that different images will generate the same hash sequence. Therefore, the hiding success rate is quite important for the practicability and feasibility of the proposed scheme. For the text of privacy information, they are mainly constructed by letters and numbers. Therefore, totally there are 62 characters required, which include the letters from lower case “a” to capital “Z” and the numbers “0” to “9”. Assuming that we choose n medical images from the test image group, there are k different hash sequence

are generated. Therefore, the hiding success rate is defined as:

$$R_{suc} = \frac{k}{62} \times 100\% \tag{19}$$

Here n is increased by 50 every time. The hiding success rate curve is shown in Fig. 11.

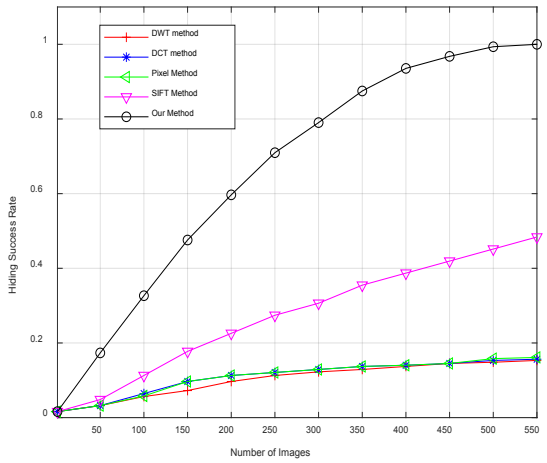

Figure 11: Hiding success rate with different image number

It can be seen that the hiding success rate will increase with the increment of the image number. When the number of medical images exceeds 550, the hiding success rate can arrive at 100%. Since the number of a group of CTA images is usually more than 550 in clinical data, the proposed scheme is practicable for privacy protection of real clinical medical images. However, the hiding success rate of other methods is very low, which means that the methods based on natural images are not applicable for medical images.

5.3 Security analysis

In our scheme, the privacy is hidden based on DenseNet and coverless steganography. The medical images are kept original without embedding and modification. In one hand, it greatly reduces the possibility of being detected and cracked. In another hand, the medical images have been kept original and reliable for diagnosis. Since the feature difference matrix is used for mapping, if there are missing images or confused with other groups of medical images, for example, images of different patients are mixed together, then the privacy information cannot be extracted normally. As shown in Fig. 11, with the increase of the proportion of lost images, the accuracy is rapidly reduced. In practical application, when some images of the patient are lost, the integrity of information is damaged, and such images cannot be used for diagnosis. We can think this may be caused by illegal embezzlement or disclosure, so it is reasonable that privacy information cannot be extracted normally. This also further protects the security of patients' privacy.

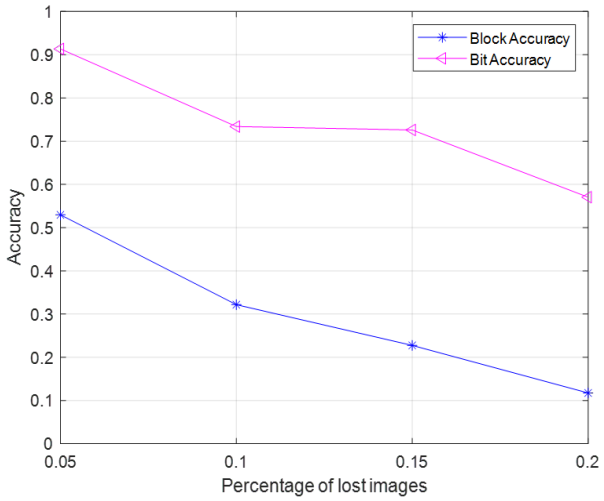

Figure 11: Block Accuracy with lost images

6 Conclusions

In this paper, we propose a privacy protection scheme for medical images based on DenseNet and coverless steganography. For a given group of medical images of one patient, through feature extraction and hash generation, the mapping index can be constructed. Then the privacy information can be mapped to the hash sequences. The corresponding mapped indexes of secret information will be packed together with the medical images group and released to the authorized user. The user can extract the privacy information successfully with the similar method of feature analysis and index construction. The simulation results show good performance of robustness. And the hiding success rate also shows good feasibility and practicability. Since the medical images are kept original without embedding and modification, the performance of crack resistance is also outstanding and can keep good quality for diagnosis. Next, we will further improve the scope of its application for different kinds of medical images.

Funding Statement: This work was supported in part by the National Natural Science Foundation of China under Grant 61772561, author J. Q, http://www.nsfc.gov.cn/; in part by the Key Research and Development Plan of Hunan Province under Grant 2018NK2012, author J. Q, and 2019SK2022, author H. T, http://kjt.hunan.gov.cn/; in part by the Science Research Projects of Hunan Provincial Education Department under Grant 18A174, author X. X, and Grant 19B584, author Y. T, http://kxjsc.gov.hnedu.cn/; in part by the Degree & Postgraduate Education Reform Project of Hunan Province under Grant 2019JGYB154, author J. Q, http://xwb.gov.hnedu.cn/; in part by the National Natural Science Foundation of Hunan under Grant 2019JJ50866, author L.T, 2020JJ4140, author Y.T, and 2020JJ4141, author X.X, http://kjt.hunan.gov.cn/; in part by the Postgraduate Excellent teaching team Project of Hunan Province under Grant [2019] 370-133, author J. Q, http://xwb.gov.hnedu.cn/; and in part by the Postgraduate Education and Teaching

Reform Project of Central South University of Forestry & Technology under Grant 2019JG013, author X. X, http://jwc.csuft.edu.cn/.

Conflicts of Interest: We declare that we have no conflicts of interest to report regarding the present study.

References

Al-Dmour, H.; Al-Ani A. (2016): Quality optimized medical image information hiding algorithm that employs edge detection and data coding. *Computer Methods and Programs in Biomedicine*, vol. 127, no. 1, pp. 24-43.

Chai, X.; Zhang, J.; Gan, Z.; Zhang, Y. (2019): Medical image encryption algorithm based on Latin square and memristive chaotic system. *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35419-35453.

Dorgham, O.; Al-Rahamneh, B.; Almomani, A.; AlHadidi, M.; Khatatneh, K. F. (2018): Enhancing the security of exchanging and storing DICOM medical images on the cloud. *International Journal of Cloud Applications and Computing*, vol. 8, no. 1, pp. 154-172.

Fakhari, P.; Vahedi, E.; Lucas, C. (2011): Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. *Digital Signal Processing*, vol. 21, no. 3, pp. 433-446.

Heidari, S.; Naseri, M.; Nagata, K. (2019): Quantum selective encryption for medical images. *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 3908-3926.

Huang, G.; Liu, Z.; Maaten, L. V. D.; Weinberger, K. Q. (2017): Densely connected convolutional networks. *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1-9.

Kang, Y. H.; Liu, F. L.; Yang, C. F.; Xiang, L. Y.; Luo, X. Y. et al. (2019): Color image steganalysis based on channel gradient correlation. *International Journal of Distributed Sensor Networks*, vol. 15, no. 5, pp. 1550147719852031.

Kavitha, P. K.; Saraswathi, P. V. (2017): A survey on medical image encryption. *1st International Conference on Applied Soft Computing Techniques*, vol. 3, no. 5, pp. 1-8.

Lee, H. (2019): Adaptive reversible watermarking for authentication and privacy protection of medical records. *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 19663-19680.

Lin, Z.; Chen, M.; Ma, Y. (2013): The augmented Lagrange multiplier method for exact recovery of corrupted low-rank matrices. arXiv: 1009.5055, pp. 1-23.

Liu, Q.; Xiang, X.; Qin, J.; Tan, Y.; Tan, J. et al. (2020): Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. *Knowledge-Based Systems*, vol. 192, no. 1, pp. 105375-105389.

Luo, Y.; Qin, J.; Xiang, X.; Tan, Y.; Liu, Q. et al. (2019): Coverless real-time image information hiding based on image block matching and dense convolutional network. *Journal of Real-Time Image Processing*, vol. 17, no. 1, pp. 125-135.

Ojala, T.; Pietikainen, M.; Harwood, D. (1996): A comparative study of texture measures with classification based on feature distributions. *Pattern Recognition*, vol. 29, no. 1, pp. 51-59.

Priyanka; Maheshkar, S. (2017): Region-based hybrid medical image watermarking for secure telemedicine applications. *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3617-3647.

Qin, J.; Luo, Y.; Xiang, X.; Tan, Y.; Huang, H. (2019): Coverless image steganography: a survey. *IEEE Access*, vol. 7, no. 1, pp. 171372-171394.

Tan, Y.; Qin, J.; Xiang, X.; Ma, W.; Pan, W. et al. (2019): A robust watermarking scheme in YCbCr color space based on channel coding. *IEEE Access*, vol. 7, no. 1, pp. 25026-25036.

Wan, W.; Wang, J.; Li, J.; Meng, L.; Sun, J. et al. (2020): Pattern complexity-based JND Estimation for quantization watermarking. *Pattern Recognition Letters*, vol. 130, no. 1, pp. 157-164.

Wang, B.; Kong, W.; Guan, H.; Xiong, N. (2019): Air quality forecasting based on gated recurrent long short term memory model in Internet of Things. *IEEE Access*, vol. 7, no. 1, pp. 69524-69534.

Wang, J.; Qin, J.; Xiang, X.; Tan, Y.; Pan, N. (2019): CAPTCHA recognition based on deep convolutional neural network. *Mathematical Biosciences and Engineering*, vol. 16, no. 5, pp. 5851-5861.

Xiang, L. Y.; Wu, W. S.; Li, X.; Yang, C. F. (2018): A linguistic steganography based on word indexing compression and candidate selection. *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28969-28989.

Yang, H.; Yin, J.; Yang, Y. (2019): Robust image hashing scheme based on low-rank decomposition and path integral LBP. *IEEE Access*, vol. 7, no. 1, pp. 51656-51664.

Yang, Y.; Zhang, W.; Liang, D.; Yu, N. (2016): Reversible data hiding in medical images with enhanced contrast in texture area. *Digital Signal Processing*, vol. 52, no. 1, pp. 13-24.

Zhang, X.; Peng, F.; Long, M. (2018): Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238.

Zheng, S.; Wang, L.; Ling, B.; Hu, D. (2017): Coverless information hiding based on robust image hashing. *International Conference on Intelligent Computing*, vol. 10363, no. 1, pp. 536-547.

Zhou, Z.; Qin, J.; Xiang, X.; Tan, Y.; Liu, Q. et al. (2020): News text topic clustering optimized method based on TF-IDF algorithm on Spark. *Computers, Materials & Continua*, vol. 62, no. 1, pp. 217-231.

Zhou, Z.; Sun, H.; Harit, R.; Chen, X.; Sun, X. (2015): Coverless image steganography without embedding. *International Conference on Cloud Computing and Security*, vol. 9483, no. 1, pp. 123-132.

Zhou, Z.; Wu, Q. M. J.; Yang, C. N. (2017): Coverless image steganography using histograms of oriented gradients-based hashing algorithm. *Journal of Internet Technology*, vol. 18, no. 5, pp. 1177-1184.

Zou, L.; Sun, J.; Gao, M.; Wan, W.; Gupta, B. B. (2018): A novel coverless information hiding method based on the average pixel value of the sub-images. *Multimedia Tools and Applications*, vol. 21, no. 1, pp. 1-16.