This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

Application of Robust Zero-Watermarking Scheme Based on Federated Learning for Securing the Healthcare Data

Baoru Han, Rutvij H. Jhaveri , *Senior Member, IEEE*, Han Wang, *Senior Member, IEEE*, Dawei Qiao*, and Jinglong Du

***Abstract*—The privacy protection and data security problems existing in the healthcare framework based on the Internet of Medical Things (IoMT) have always attracted much attention and need to be solved urgently. In the teledermatology healthcare framework, the smartphone can acquire dermatology medical images for remote diagnosis. The dermatology medical image is vulnerable to attacks during transmission, resulting in malicious tampering or privacy data disclosure. Therefore, there is an urgent need for a watermarking scheme that doesn't tamper with the dermatology medical image and doesn't disclose the dermatology healthcare data. Federated learning is a distributed machine learning framework with privacy protection and secure encryption technology. Therefore, this paper presents a robust zero-watermarking scheme based on federated learning to solve the privacy and security issues of the teledermatology healthcare framework. This scheme trains the sparse autoencoder network by federated learning. The trained sparse autoencoder network is applied to extract image features from the dermatology medical image. Image features are undergone to two-dimensional Discrete Cosine Transform (2D-DCT) in order to select low-frequency transform coefficients for creating zero-watermarking. Experimental results show that the proposed scheme has more robustness to the conventional attack and geometric attack and achieves superior performance when compared with other zero-watermarking schemes. The proposed scheme is suitable for the specific requirements of medical images, which neither changes the important information contained in medical images nor divulges privacy data.**

***Index Terms*—Zero-watermarking, federated learning, IoMT, sparse autoencoder network**

This work was supported by the Science and Technology Research Program of Chongqing Education Commission of China (Grant No. KJQN201800442), and the General Project of Chongqing Natural Science Foundation of China (Grant No. cstc2020jcyj-msxmX0422). (Corresponding author: Dawei Qiao.)

Baoru Han and Jinglong Du are with the College of Medical Informatics, Chongqing Medical University, Chongqing 400016, China (e-mails: baoruhan@cqmu.edu.cn; jldu@cqu.edu.cn).

Rutvij H. Jhaveri is with the Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, India rutvij.jhaveri@sot.pdpu.ac.in

Han Wang is with the Faculty of Data Science, City University of Macau, Macao 999078, China. (e-mail: hanwang1214@126.com).

Dawei Qiao is with the School of Emergency Management, Henan Polytechnic University, Jiaozuo 454000, China. (email: daweihpu@163.com)

I. Introduction

As the rapid development of the Internet of Medical Things (IoMT) technology, wearable devices of patients are gradually being applied to a variety of healthcare-related activities, and have become an important part of the new type of smart healthcare [1-2]. The healthcare framework based on IoMT employs personal wearable sensors to obtain personal information, making it possible to provide individuals with a full range of personalized medical services [3]. The healthcare data obtained by the IoMT from the human body must be confidential, reliable, and complete [4-5]. At the same time, it cannot be identified and tracked without authorization. At present, one of the biggest challenging problems in the IoMT healthcare framework is the issue of healthcare data information security [6-7]. Teledermatology is one important application of IoMT, which also have to solve the security problem including preventing dermatology medical image from being tampered with and authenticating the authenticity and reliability of dermatology medical image. Therefore, the security protection of dermatology medical image is an urgent problem to be solved [8].

Researchers have proposed various zero-watermarking methods to effectively solve the above problem that does not change the original information of the image [9]. The zero-watermarking method was initially proposed by Wen et al. [10]. In [11], a robust zero-watermarking scheme was designed, which used the invariants of orthogonal Fourier-Melin moments to construct a zero-watermarking. Wang et al. [12] proposed a robust zero-watermarking algorithm, which achieved effective resistance to different attacks. This algorithm applied the polar complex exponential transform to build zero-watermarking. In [13], a robust zero-watermarking scheme for medical image tamper location based on hyperchaos was given by Xiao et al. For medical image certification, Kavitha et al. [14] provided two zero-watermarking algorithms, which were highly robust to various attacks, and provides additional information about clinical results to remote radiologists. In [15], a novel zero-watermarking scheme for the medical image in encryption domain was offered. Singh et al. [16] offered a zero-watermarking scheme, which relied on the singular value of wavelet coefficients. Liu et al. [17] gave a robust zero-watermarking schem , which was based on the 3D hyperchaos and 3D dual-tree complex wavelet transform, satisfied the security of medical data transmission and storage in the IoMT. Currently, the research of the zero-watermarking scheme had made great progress, but there are still some

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

problems. The prominent problem is that these classical zero-watermarking schemes have poor robustness, especially in resisting geometric attacks.

Recent research shows that using the sparse autoencoder network to extract image scale, brightness, texture and other more complex image features could enable the image zero-watermarking algorithm to have better robustness and imperceptibility [18-19]. The training of the traditional sparse autoencoder network needs to transfer the dermatology image generated from the patient's wearable device to the central server. Due to the sensitivity of dermatology healthcare data, the method of transmitting the patient image to a central server may cause serious security and privacy problems. Therefore, it is not feasible to construct large medical image data sets using small image data sets from different sources. Federated learning is a machine learning framework in which multiple clients cooperate to solve machine learning problems, which is coordinated by a central server [20-21]. It allows all participants to build models without disclosing their data, and then use the data resources in the whole data federation to improve the model performance of each member. In [22], a federated learning framework with difference perception proposed was proposed by Yan et al, which could solve the cross-client variation problem in medical image data. Liu et al. [23] proposed the federated model performed better than a model trained separately on each individual and nearly as well as the server model. Rajendran et al. [24] explored several federated learning implementations by applying them in both a simulated environment and an actual implementation using electronic health record data from two academic medical centers. Federated learning is an effective method, which is becoming more and more popular as a feasible solution in this telemedicine framework [25].

Motived by the above-mentioned observations, this paper proposes a robust zero-watermarking scheme based on federated learning that can be applied to the protection of the teledermatology framework. This scheme combines federated learning, sparse autoencoder network, and 2D-DCT to extract the feature vector of the original dermatology medical image to construct a zero-watermarking. A chaotic system is used to encrypt the watermarking image to improve the security of the watermarking information. Experimental results show that the proposed scheme can realize the embedding and extraction of watermarking in a dermatological medical image, and has strong robustness against the conventional attack and geometric attack. The main contributions of this paper can be summarized as follows.

1) A robust zero-watermarking scheme based on federated learning is presented to solve the privacy and security issues of the teledermatology healthcare framework.
2) Sparse autoencoder network and 2D-DCT are used to extract stable and unchanging robust features to construct zero-watermarking,
3) The federated learning was used to train the sparse autoencoder network so that the decentralized participants could cooperate in the training of the sparse autoencoder network model without disclosing private data to other participants.
4) The proposed scheme could reduce some system privacy risks brought by traditional centralized machine learning methods, effectively solve the problem of data island.

II. Related Work

A. Federated learning

Federated learning is a distributed machine learning framework with privacy protection and secure encryption technology [26-27]. It aims to allow decentralized participants to collaborate on machine learning model training without disclosing private data to other participants. At the same time, it ensures the decentralized machine learning setting of training data. Federated learning uses local data collection and minimization principles, which can reduce many systematic privacy risks and costs brought by traditional centralized machine learning methods.

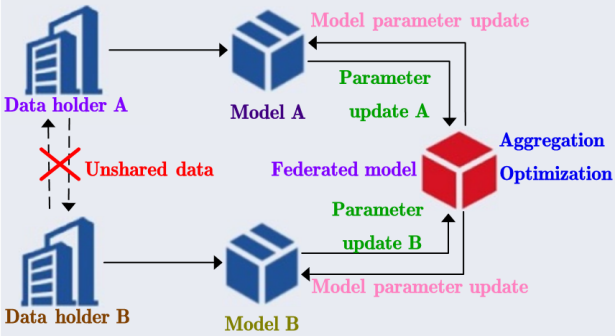


Fig. 1 System architecture of federated learning.

The system architecture of federated learning is shown in Fig.1. Each data holder has relevant data of its users. Considering data privacy protection and security, data holder A and data holder B cannot exchange data. The data holders use the federated learning system to establish the model and use local updates to achieve the learning goal. A typical federal learning flow is as follows.

Step 1: the server selects the qualified client.

Step 2: each selected client downloads the latest model from the server.

Step 3: each selected client trains the model with local data, updates its model parameters and uploads them to the server.

Step 4: the server aggregates the model parameters uploaded by each user and updates the server model parameters.

Step 5: the server returns the updated model to each selected client.

Step 6: each selected client updates its model.

In this paper, federated learning is used to train the sparse autoencoder network, so that the decentralized participants can cooperate in the training of the sparse autoencoder network model without disclosing private data to other participants.

B. Sparse Autoencoder Network

Sparse autoencoder network is a common unsupervised feature extraction algorithm [28]. The sparse autoencoder network structure is displayed in Fig.2. An input layer, a hidden layer, and an output layer constitute the main structure. In the sparse autoencoder network, it is divided into two stages: coding and decoding.

For datasets $x = (x_1, x_2, x_3 \cdots\cdots x_n)$, n is the number of data. The dimension of each data is m, namely

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

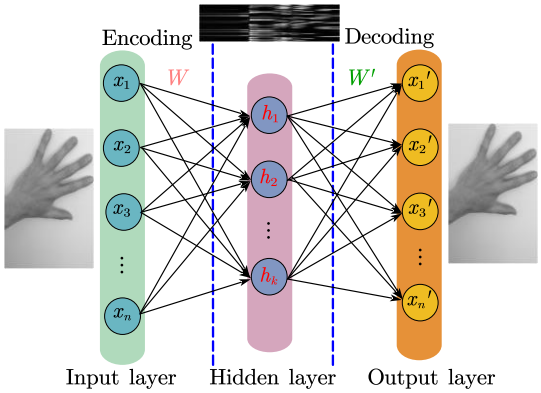


Fig. 2 Sparse autoencoder network structure.

$x_i \epsilon \boldsymbol{R}^m (i=1,2,\cdots,n)$. In the process of data encoding, each data is represented in a hidden layer. The encoding process is expressed by

$$h_i = f(Wx_i + b) \tag{1}$$

where W and b represents the weight and deviation between the input layer and the hidden layer, respectively, and $f(\cdot)$ denotes the activation function of the hidden layer. Then the hidden layer representation is decoded to get the reconstructed data x'. The decoding process can be described as

$$x_i' = f'(W'h_i + b') \tag{2}$$

among them, W' and b' respectively represents the weight and bias between the hidden layer and the output layer, $f'(\cdot)$ denotes the activation function of the output layer.

The sparse autoencoder network reconstructs the output data through the input data and obtains the hidden characteristics of the data, to make the output data equal to the input data as much as possible. That is, the difference between the input data x_i and the output data x'_i is minimized. The loss function of the whole training data set is

$$J(W,b) = \frac{1}{n}\sum_{i=1}^{n} L(x_i, x'_i) = \frac{1}{n}\sum_{i=1}^{n} \|x_i - x'_i\|^2 \tag{3}$$

where L is the mean square error loss function of a single data. To obtain deeper features and reduce the size of weights, the regularization term L is usually added to the loss function to prevent the over-fitting problem. λ is the penalty factor and controls the influence of the regularization term on weight attenuation. So the loss function can be written as

$$J(W,b) = \frac{1}{n}\sum_{i=1}^{n} L(x_i, x'_i) + \frac{\lambda}{2}\|W\|^2 \tag{4}$$

The sparse autoencoder network is acquired by adding sparsity constraints to the loss function on account of the autoencoder network [29]. This sparsity is suitable for the hidden layer neurons of the autoencoder network. Most of the outputs of hidden layer neurons are suppressed to make the network sparse. KL divergence is used to force it to be close to a given sparse value, which is added to the loss function as a penalty term. The penalty term can be expressed as

$$KL(\rho \| \hat{\rho}_j) = \rho \log \frac{\rho}{\hat{\rho}_j} + (1-\rho)\log \frac{1-\rho}{1-\hat{\rho}_j} \tag{5}$$

where ρ represents the sparsity parameter, the average activity of hidden neuron j is $\hat{\rho}_j$.

$$\hat{\rho}_j = \frac{1}{m}\sum_{i=1}^{m} [a_j(x_i)] \tag{6}$$

where m represents the number of neurons in the hidden layer. Given the input x, $a_j(x_i)$ is the activation value of hidden layer neuron j in the sparse autoencoder network.

Therefore, the loss function of the sparse autoencoder network is

$$J_s(W,b) = \frac{1}{n}\sum_{i=1}^{n} L(x_i, x'_i) + \frac{\lambda}{2}\|W\|^2 + \beta\sum_{j=1}^{m} KL(\rho \| \hat{\rho}_j) \tag{7}$$

where β is the sparsity penalty factor weight.

C. Discrete Cosine Transform (DCT)

Let $g(x,y)$ denote the original image data, whose size is $M \times N$. $G(u,v)$ is the transformed frequency domain data. Given $y,v = 0,1,2,\cdots,N-1$, the 2D-DCT formula is

$$G(u,v) = c(u)c(v)* \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} g(x,y)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{8}$$

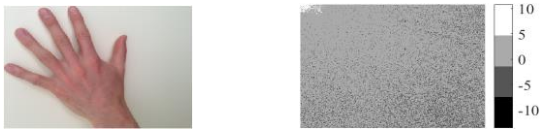
where

$$c(u) = \begin{cases} \sqrt{1/M} & u=0 \\ \sqrt{2/M} & u=1,2,\cdots M-1 \end{cases} \tag{9}$$

$$c(v) = \begin{cases} \sqrt{1/N} & v=0 \\ \sqrt{2/N} & v=1,2,\cdots N-1 \end{cases} \tag{10}$$

The 2D inverse DCT formula is

$$g(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u)c(v) G(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)}{2N} \tag{11}$$



(a) Hand dermatology medical image (b) Cosine domain image

Fig. 3 DCT of the hand dermatology medical image.

As shown in Fig. 3, a hand dermatology medical image is treated by a 2D-DCT, and its main features are concentrated in the upper left corner of the transformed image.

D. Logistic Chaotic System

A logistic chaotic system is a kind of simple but widely used chaotic system. The formula is as follows.

$$b_{n+1} = ab_n(1-b_n) \tag{12}$$

where $b_n \epsilon (0,1)$ $0 < a \leqslant 4$ is called a branch parameter. The number of iterations is n. When $3.5699456\cdots < a \leqslant 4$, the logistic map is chaotic. The sequence generated by the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

initial condition b_0 under the Logistic mapping iteration is aperiodic, non-convergent, extremely sensitive to the initial condition, and has some characteristics of random signals. b_0 takes any value in the range of $(0,1)$, and the computer is used to perform iterative operations to obtain the mapping branch diagram, as shown in Fig. 4.

In this paper, the chaotic sequence is created by a Logistic chaotic system. The position index of chaotic sequence ordering is used to change the position of each pixel in the binary watermarking image. It makes the content of the watermarking image invisible from the vision and achieves the purpose of hiding the information of the watermarking image.

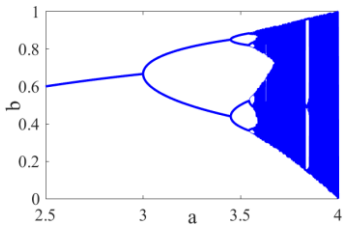


Fig.4 Bifurcation plot of Logistic chaotic system.

III. The Proposed Watermarking Scheme

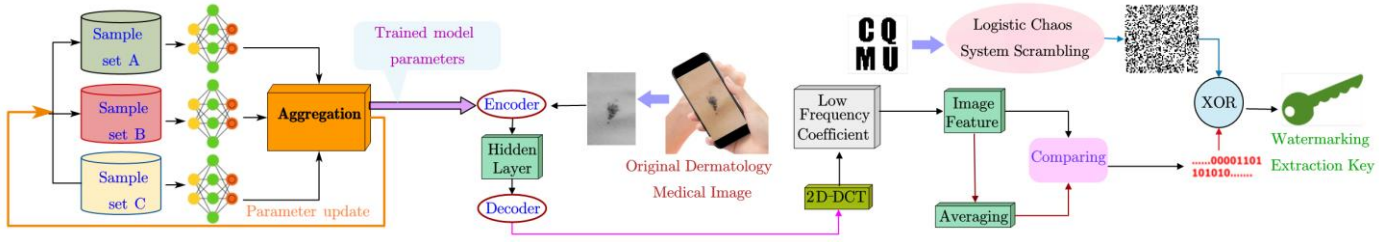
The zero-watermarking scheme mainly includes two processes: the watermarking embedding process and the watermarking extraction process. Fig.5(a) and Fig.5(b) illustrate the flow chart of the scheme for watermarking embedding and watermarking extraction, respectively.

A. Watermarking embedding process

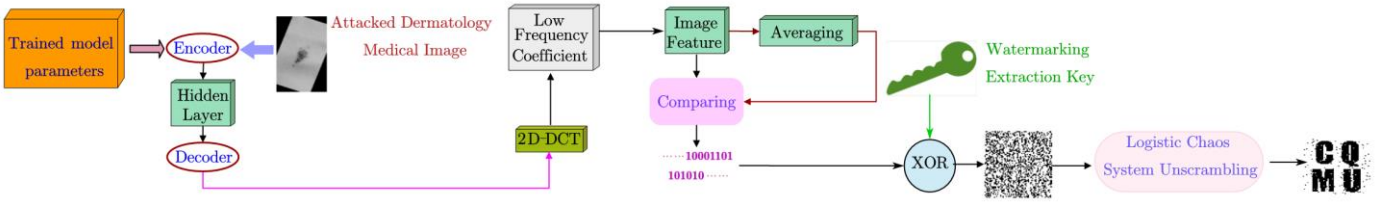
The watermarking embedding process involves extracting robust features from the dermatology medical image and combining them with the binary watermarking image to generate the watermarking extraction key. Firstly, a sparse autoencoder network is trained using federated learning. Secondly, the feature of dermatology medical image obtained by smartphone is extracted by the trained sparse autoencoder network. Thirdly, the image features are transformed by 2D-DCT, and the low-frequency transform coefficients are selected. Then, the gray levels of the low-frequency coefficients are compared with their average values to generate a binary feature vector. Finally, the binary vector is XOR calculated with the scrambled watermarking image to generate the watermarking extraction key. The specific step-by-step process is explained as Algorithm 1.

Algorithm 1: Embedding process

1. **Input:** Dermatology medical image x, original watermarking image y.
2. **Scramble the original watermarking image**
   Set the initial values b_0 and a of Logistic chaotic system
   Generate chaotic sequence
   Scramble the original watermarking image y
   Get the scrambled watermarking image $y_{scrambled}$
3. **Training sparse autoencoder network with federated learning**
   Initialize parameters
   Server executes:
   for each round t=1,2,… **T do**
   autoenc_t ← randomly choose a set of clients
   for each client autoenc_t **in parallel do**
   weight_t ← ClientUpdate
   weight_m ← mean(weight_t)
   Server send weight_m to all chosen client
   ClientUpdate
   While epoch < MaxEpochs and Performance <Performance goal **do**
   autoenc_trained ← train autoencoder
   end while
   return weight to server
4. **Extracting image features**
   image_features ← predict(autoenc_trained, x)
5. **Get binary eigenvector**
   DCT_features ← 2D-DCT(image_features)
   features ← DCT_features (1:8,1:8)
   features_ mean ← mean(features)
   Compare grayscale value
   if grayscale > features_ mean **do**
   key ← 1
   else
   key ← 0
   end if
6. **Generate key**
   key_orig ← key $\oplus$ $y_{scrambled}$
7. **Output:** The watermarking extraction key key_orig



(a) The flowchart of watermarking embedding



(b) The flowchart of watermarking extraction

Fig.5 The overall framework of the proposed watermarking scheme.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

B. Watermarking extraction process

The watermarking extraction process is approximating to the watermarking embedding process. The difference is that dermatological medical image have been attacked. The feature extraction of the attacked dermatology medical image is adopted by the same trained sparse autoencoder network. The generation method of the binary feature vector is the same as that mentioned in the watermarking embedding process. This robust binary feature vector is strategically combined with the received watermarking extraction key to successfully extract the watermarking image. A logistic chaotic system is still selected for the inverse scrambling of the extracted watermarking image. The correlation of the watermarking image is calculated. The explicit steps are Algorithm 2.

Algorithm 2: Extraction process

1. Input: The watermarking extraction key key_orig, the attacked dermatology medical image $x_{attacked}$

$x_{attacked} \leftarrow$ Various attacks on the dermatology medical image x

2. Extracting image features

image_features1 $\leftarrow$ predict (autoenc_ trained, $x_{attacked}$)

3.Get binary eigenvector

DCT_features1 $\leftarrow$ 2D-DCT(image_features1)

features1 $\leftarrow$ DCT_features1 (1:8,1:8)r

features1_ mean $\leftarrow$ mean(features1)

Compare grayscale value

if grayscale > features1_ mean **do**

key_attacked $\leftarrow$ 1

else

key_attacked $\leftarrow$ 0

end if

4. Extract the watermarking image $y_{extract}$

$y_{extract} \leftarrow$ key_attacked $\oplus$ key_orig

5.Reverse scrambling the extracted watermarking image $y_{extract}$

Adopt the initial values b_0 and a of Logistic chaotic system

Generate chaotic sequence

Reverse scrambling the extracted watermarking image $y_{extract}$

Get the inversely scrambled watermarking image $y_{inverse}$

6. Calculate Normalized-Correlation(NC)

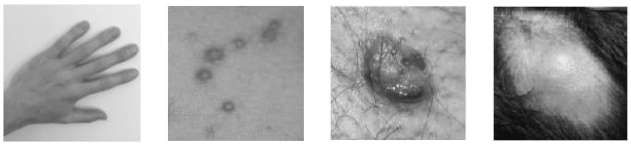
$$NC \leftarrow \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} y(i,j)y_{inverse}(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} y(i,j)y(i,j)}$$

M and N are the size of the dermatology medical image.

7. Output: NC

IV. Experiments and Discussion

To assess the performance of the proposed robust zero-watermarking scheme in this paper, four dermatology medical images with the size of 128×128, as shown in Fig. 6, are selected in the experiment. The value of each pixel is between 0 and 255, which is represented by 8 bits. Although all experiments of the proposed robust zero-watermarking watermarking scheme are performed on BMP images, it is also applicable to other types of dermatology medical images. The simulation software used were Matlab R2020a and Python3.6. The configuration of the experimental computer was that the GPU was Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz, and the Memory was 16GHz. The binary image with the size of 64×64 that shown in Fig.7(a) is used as watermarking image. Fig.7(b) exhibits the scrambled watermarking image. Some experiments were carried out by using conventional attack and geometric attack to test the robustness of the proposed robust zero-watermarking scheme.



(a) Image A (b) Image B (c) Image C (d)Image D

Fig.6 The dermatology medical images

(a)Original watermarking image (b)Scrambled watermarking image

Fig.7 The watermarking images.

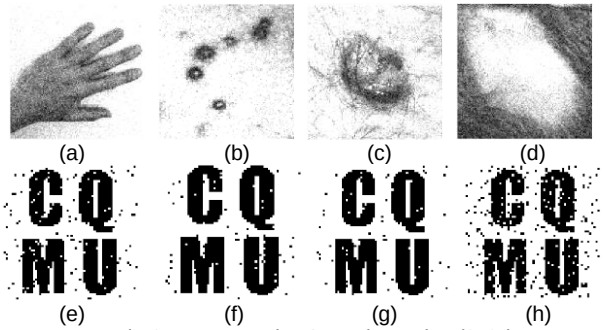
A. Robustness Against Conventional Attacks

Table I lists the NC values of test dermatology medical images under Gaussian noise attack. As shown in Table I, the NC values are very close to 1. Fig.8 shows the dermatology medical images attacked by Gaussian white noise mean (25%) and the recovered watermarking images. These watermarking images are visible. It is proved that the proposed scheme can resist Gaussian noise attack well.

In the JPEG compression attack experiment, the original dermatology medical images are examimated with 5%, 10%, 15%, 20%, and 25% compression quality respectively. The examinations of four original dermatology medical images are shown in Table II. It can be found that the NC values are almost all 1. The recovered watermarking image with JPEG compression intensity of 25% is very distinct, as shown in Fig. 9. The results indicate that the proposed robust scheme has good robustness under JPEG compression attack.

TABLE I
NC UNDER GAUSSIAN NOISE ATTACK

Gauss white noise mean	5%	10%	15%	20%	25%
Image A	0.9877	0.9877	0.9877	0.9753	0.9753
Image B	1	0.9877	1	1	0.9877
Image C	1	1	1	0.9877	0.9877
Image D	0.9753	0.9753	0.9628	0.9502	0.9502



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig.8 Images under Gaussian noise (25%).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

TABLE II
NC UNDER JPEG COMPRESSION ATTACK

JPEG compression quality	5%	10%	15%	20%	25%
Image A	1	1	1	1	1
Image B	1	1	1	1	1
Image C	1	1	1	1	1
Image D	1	0.9877	0.9877	0.9877	0.9877

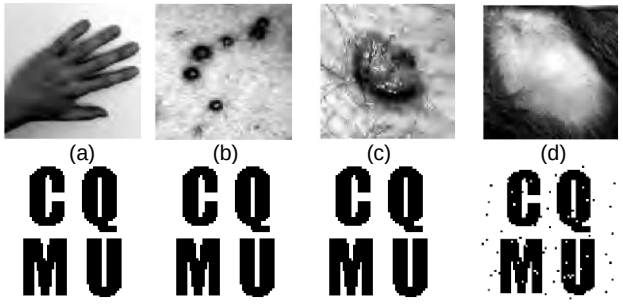


Fig.9 Images under JPEG compression (25%).

TABLE III
NC UNDER MEDIAN FILTERING ATTACK

Median filtering size	[5*5] 20 times	[10*10] 20 times	[15*15] 20 times	[20*20] 20 times	[25*25] 20 times
Image A	0.9753	0.9375	0.9502	0.9502	0.9627
Image B	0.9753	0.8867	0.9753	0.8863	0.9502
Image C	0.9879	0.9122	0.9752	0.9119	0.9753
Image D	0.9877	0.9627	0.9877	0.9502	0.9753

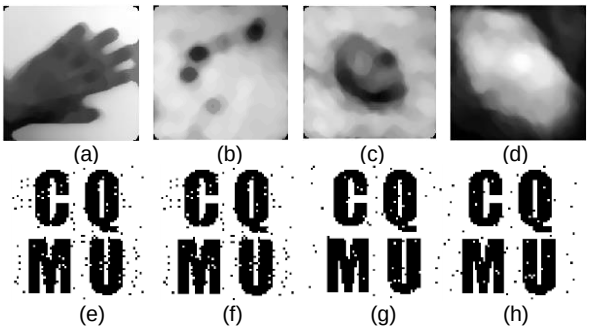


Fig.10 Images under median filtering attack (25*25)

The median filtering method is applied to the dermatology medical image. Table III gives the NC values for this attack. Fig.10 presents the experimental images of median filtering size of 25*25. The results show that the NC values of the four dermatology medical images are larger than 0.88, which shows that the recovered watermarking images have good similarity with the original watermarking image, and the proposed robust zero-watermarking scheme can effectively resist the median filtering attack.

B. Robustness Against Geometric Attacks

The dermatology medical images rotated by $25°$ and the recovered watermarking images are shown in Fig.11. Although the rotation angle is so large, the recovered watermarking image can still be distinguished. It can be concluded by observing the data in Table IV that when the rotation angle increases, the NC value decreases. The NC values of all test images were more than 0.93. The results reveal that the proposed robust zero-watermarking scheme has a strong anti-rotation attack ability.

In the experiment of scaling attack, two scaling factors are used to scale the image. Table V provides the experimental data of scaling attack. The scaled dermatology medical images and the restored watermarking images are shown in Fig.12. We can find that the proposed robust zero-watermarking scheme has better robustness to scaling attacks.

The dermatology medical images are cropped along the Y-axis. The robust performance data obtained are given in Table VI. It can be seen from the table that the cropping attack has a certain influence on the NC values of the recovered watermarking images. Fig.13 shows the experimental images under cropping attack (10%). Among them, the effect of restoration watermarking image is very good. The above analysis shows that the proposed watermarking scheme can effectively restore the watermarking image, and it is very robust against cropping attacks.

TABLE IV
NC UNDER ROTATION ATTACK

Rotation angle (Clockwise)	5°	10°	15°	20°	25°
Image A	0.9502	0.9502	0.9502	0.9628	0.9503
Image B	0.9628	0.9628	0.9753	0.9753	0.9378
Image C	0.9877	0.9877	0.9877	0.9877	0.9877
Image D	0.9628	0.9628	0.9627	0.9627	0.9627

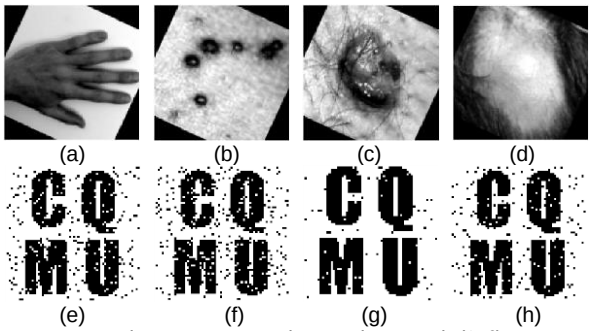


Fig.11 Images under rotation attack (25º).

TABLE V
NC UNDER SCALING ATTACK

Scaling factor	(1/32,32)	(1/16,16)	(1/8,8)	(16,1/16)	(32,1/32)
Image A	0.9628	0.9753	1	1	1
Image B	0.9628	0.9753	0.9877	1	1
Image C	0.9879	1	1	1	1
Image D	0.9628	1	0.9877	0.9877	0.9877

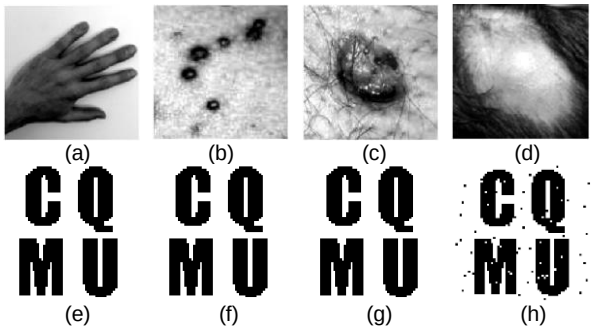


Fig.12 Images under scaling attack (32,1/32).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

TABLE VI
NC UNDER CROPPING ATTACK

Cropping scale (Y-axis)	2%	4%	6%	8%	10%
Image A	1	1	1	1	1
Image B	0.9753	0.9753	0.9753	0.9753	0.9753
Image C	1	0.9877	0.9877	0.9877	0.9877
Image D	1	1	0.9877	0.9877	0.9877

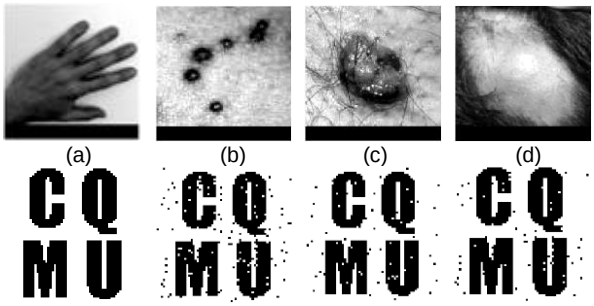


Fig.13 Images under cropping attack (10%) .

TABLE VII
NC UNDER TRANSLATION ATTACK

Translation distance (up)	2%	4%	6%	8%	10%
Image A	1	1	1	0.9726	0.9726
Image B	0.9628	0.9628	0.9628	0.9503	0.9628
Image C	0.9877	0.9877	0.9753	0.9753	0.9753
Image D	0.9877	0.9627	0.9627	0.9627	0.9627

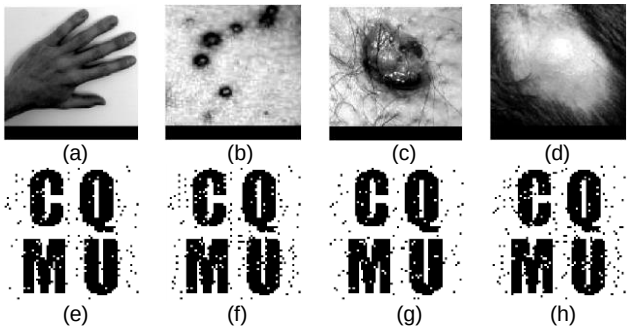


Fig.14 Images under translation attack (up10%).

We carry out translation attack to assess the performance of the proposed scheme. The translation distance is 2%, 4%, 6%, 8% and 10%, respectively. Fig.14 shows the experimental images under translation attack (10%). Table VII provides the NC values of the recovered watermarking image after the translation attack. Look at Table VII, the NC value of the recovered watermarking image is above 0.95, especially with the enhancement of translation distance, the change range of NC value is very small, which is close to 1. The above results explain that the proposed robust zero-watermarking scheme has higher robustness for translation attacks.

C. Comparison with Representative Schemes

The robustness of the proposed scheme is compared with six representative zero-watermarking schemes, among which [30-32,34-35] are five zero-watermarking schemes for medical images, and the scheme [33] is a zero-watermarking for the natural image. The zero-watermarking scheme [30] for the medical image is based on Discrete Wavelet Transform (DWT) and DCT. A new medical image zero-watermarking scheme based on dual-tree complex wavelet transform and DCT was introduced in [31]. The scheme [32] adopted the Contourlet transform and DCT to construct zero-watermarking for medical image. A robust watermarking scheme [34] for medical image based on DCT is proposed. The scheme [35] was put forward a zero-watermarking algorithm for medical image based on VGG19 deep convolution neural network. These five watermarking schemes are robust zero-watermarking schemes that have emerged in recent years for the privacy and security of medical image. The scheme [33] describes in detail the zero-watermarking method based on the Contourlet-DCT hybrid transform and singular value decomposition.

The comparison of the schemes is carried out through the same medical image. The attack types include conventional attack and geometric attack, which are Gaussian noise attack, JPEG compression attack, median filtering attack, rotation attack, scaling attack, cropping attack, and translation attack. The comparison between the proposed scheme and compared schemes [30-35] against conventional attacks are given in Fig.15, Fig.16, and Fig.17. The comparisons between the proposed scheme and the other six zero-watermarking schemes [30-35] anti-geometric attacks are presented in Fig.18, Fig.19, Fig. 20, and Fig.21. In Fig. 15, the proposed scheme has better robustness than the other five schemes [30-31,33-35], which is almost the same as the scheme [32]. As shown in Fig.16, the NC value of the schemes [30-35] are obviously lower than that of the proposed scheme. We can see from Fig.17, the proposed scheme evidently outperforms the other six schemes [30-35] in resisting median filtering attack. For rotation attacks, the robustness of the proposed scheme is significantly better than the other six schemes [30-35] in Fig.18. In Fig.19, the NC value of the proposed

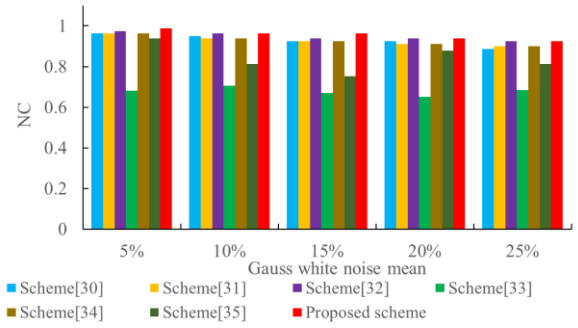


Fig.15 Robustness comparison under Gauss noise attack.

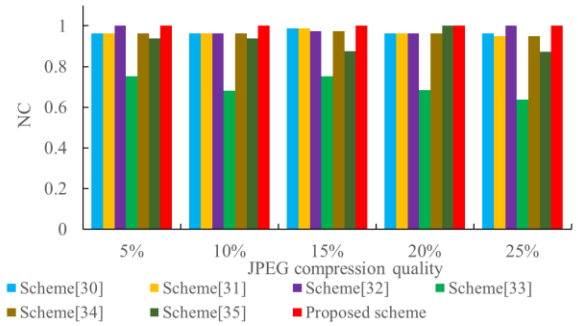


Fig.16 Robustness comparison under JPEG compression attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2021.3123936, IEEE Journal of Biomedical and Health Informatics

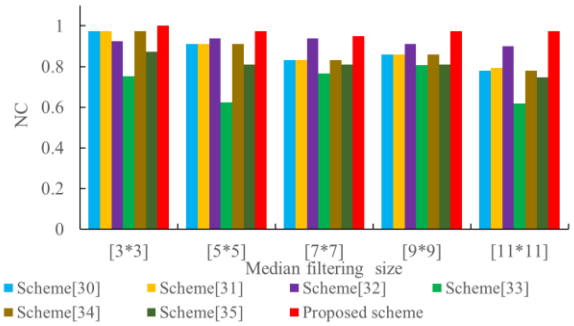


Fig.17 Robustness comparison under median filtering attack.

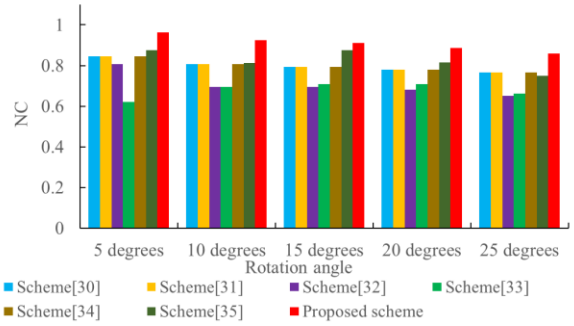


Fig.18 Robustness comparison under rotation attack.

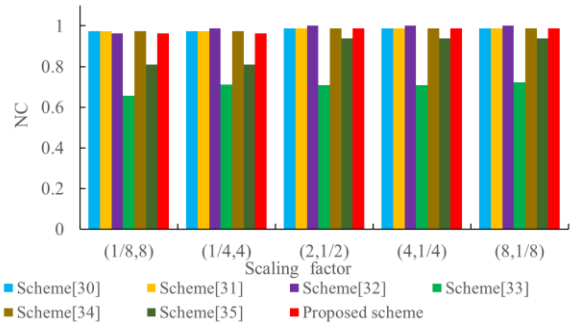


Fig.19 Robustness comparison under scaling attack.

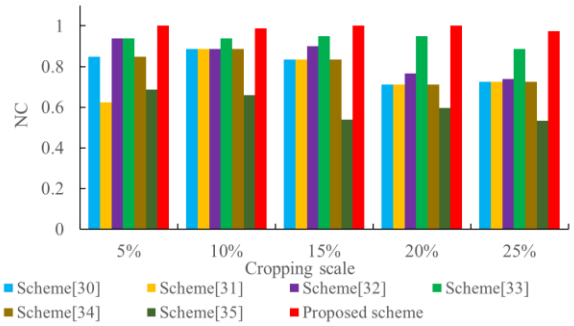


Fig.20 Robustness comparison under cropping attack.

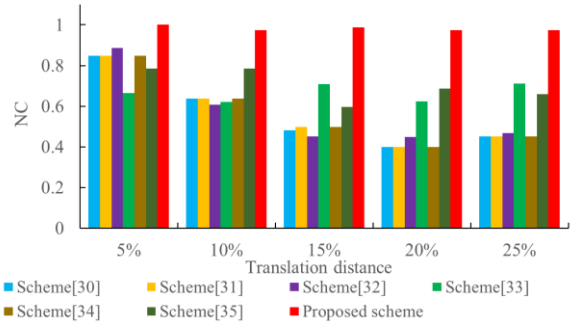


Fig.21 Robustness comparison under translation attack.

scheme is almost the same as the schemes [30-31,34], much larger than the scheme [33,35], and slightly smaller than that of [32]. As shown in Fig.20, with the increase of cropping intensity, the NC value of the zero-watermarking schemes [30-35] is more and more obviously smaller than that of the proposed scheme. The results in Fig.21 show that the proposed scheme has a stronger ability to resist translation attack than the other six schemes [30-35].

From the above comparison and analysis, it can be seen that in the JPEG compression attack, median filtering attack, rotation attack, cropping attack, and translation attack, the robustness of the proposed scheme is significantly better than the six zero-watermarking schemes. In addition, the proposed scheme has almost the same ability to resist Gaussian noise attack and scaling attack as the other six schemes [30-35]. Therefore, the zero-watermarking scheme proposed in this paper is obviously stronger than the six schemes in terms of robustness against the conventional attack and geometric attack.

V. Conclusion

In this paper, a novel robust zero-watermarking scheme based on federated learning against the conventional attack and geometric attack is proposed, which can be used in the teledermatology framework. This scheme is based on the data privacy protectiveness of federated learning, the robustness of extraction feature of sparse autoencoder network and the stability of low-frequency coefficients of cosine transform. The scheme does not need the original dermatology medical image for watermarking extraction, nor does it require dermatological medical images to be uploaded to a central server. And it realizes the protection of dermatology medical image. Experimental results show that the proposed scheme is robust to both conventional and geometric attacks. Compared with other representative schemes, it has better robustness and strong application value when protecting the privacy and security of the dermatology medical image for the teledermatology healthcare framework.

References

[1] B. Zhao, K. Fan, K. Yang, Z. Wang, H. Li, and Y. Yang, "Anonymous and privacy-preserving federated learning with industrial big data," *IEEE T Ind Inform*, vol. 17, no. 9, pp. 6314–6323, 2021.

[2] R. M. Swarna Priya, P. K. R. Parimala, M. Koppu, et al., "An Effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT Architecture," *Comput Commun*, vol. 160, pp. 139–149, 2020.

[3] M. H. Chinaei, H. Habibi Gharakheili, and V. Sivaraman, "Optimal witnessing of healthcare IoT data using blockchain logging contract," *IEEE Internet Things*, vol. 8, no. 12, pp. 10117–10130, 2021.

[4] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet Things*, vol. 8, no. 2, pp. 881–888, 2021.

[5] M. A.Rahman, M. S.Hossain, M. S.Islam, N. A.Alrajeh, and G .Muhammad., "Secure and provenance enhanced Internet of health things framework: a blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071-205087, 2020.

[6] L Cilliers, "Wearable devices in healthcare: Privacy and information security issues," *Health Inf Manag J*, vol.49, no.2, pp.150–156, 2020.

[7] Y. Zhuang, L. R. Sheets, Y.W. Chen, Z. Y. Shae, J. J. Tsai, and C. R. Shyu,

"A patient-centric health information exchange framework using blockchain technology," *IEEE J Biomed Health*, vol. 24, no. 8, pp. 2169–2176, 2020.

[8] A. Krall, D. Finke, and H. Yang, "Mosaic privacy-preserving mechanisms for healthcare analytics," *IEEE J Biomed Health*, vol. 25, no. 6, pp. 2184–2192, 2020.

[9] C. Wang, X. Wang, Z. Xia, and C. Zhang, "Ternary radial harmonic fourier moments based robust stereo image zero-watermarking algorithm," *Inform Sciences*, vol. 470, pp. 109–120, 2019.

[10] Q. Wen, T. F. Sun, and S. X. Wang, "Concept and application of zero-watermark," *Acta Electronica Sinica*, vol. 2003, no. 02, pp. 214–216, 2003.

[11] Z. Shao, Y. Shang, Y. Zhang, X. Liu, and G. Guo, "Robust watermarking using orthogonal fourier–mellin moments and chaotic map for double images," *Signal Process*, vol. 120, pp. 522–531, 2016.

[12] C. P. Wang, X. Y. Wang, X. Chen, and C. Zhang, "Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping," *Multimed Tools Appl*, vol. 76, no. 24, pp. 26 355–26 376, 2017.

[13] Z.J.Xiao, N. Li, Y.B. Wang, et al, "Zero-watermarking scheme for medical image temper location based on hyper-chaos encryption," *Comput Eng Appl*, vol. 53, no. 7, pp. 115–120, 2017.

[14] C. Kavitha and S. Sakthivel, "An effective mechanism for medical images authentication using quick response code," *Cluster Comput*, vol. 22, no. 2, pp. 4375–4382, 2019.

[15] J. Liu, J. Li, Y.Chen, et al, "A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain," *Comput Mater Con*, vol. 61, no. 1, pp. 363–378, 2019.

[16] A. Singh and M. K. Dutta, "A robust zero-watermarking scheme for tele-ophthalmological applications," *J King Saud Univ Sci*, vol. 32, no. 8, pp. 895–908, 2020.

[17] J. Liu, J. Ma, J. Li, M. Huang, N. Sadiq and Y. Ai, "Robust watermarking algorithm for medical volume data in internet of medical things," *IEEE Access*, vol. 8, pp. 93939–93961, 2020.

[18] X. Liu, Y. Zhang, S. Du, J. Zhang, M. Jiang, and H. Fang, "Discriminative and geometrically robust zero-watermarking scheme for protecting DIBR 3D videos," *in Proc. IEEE Int. Conf. Multimed Expo*, 2021, pp. 1–6.

[19] J. Xu, L. Xiang, Q. Liu, H. Gilmore, J. Wu, J. Tang, and A. Madabhushi, "Stacked sparse autoencoder (SSAE) for nuclei detection on breast cancer histopathology images," *IEEE T Med Imaging,* vol. 35, no. 1, pp. 119–130, 2015.

[20] L. Lyu et al., "Towards Fair and Privacy-Preserving Federated Deep Models," IEEE T Parall Distr, vol. 31, no. 11, pp. 2524-2541, 2020,

[21] V. Mothukuri, R. M, Parizi ,S. Pouriyeh, et al., "A survey on security and privacy of federated learning," *Future Gener Comp Sy*, vol. 115, pp. 619–640, 2021.

[22] Z. Yan, J. Wicaksana, Z. Wang, X.Yang, K.T.Cheng, "Variation-aware federated learning with multi-source decentralized medical image data," *IEEE J Biomed Health Inform*, vol.25, no.7, pp.2615–2628, 2021.

[23] J.C. Liu, J . Goetz, S.Sen, A.Tewari, "Learning from others without sacrificing privacy: simulation comparing centralized and federated machine learning on mobile health data," *JMIR mHealth uHealth*, vol. 9, no.3, pp.23728, 2021.

[24] S.Rajendran, JS.Obeid, H.Binol, et al, "Cloud-based federated learning implementation across medical centers," *JCO Clin Cancer Inform*., no.5, pp.1–11, 2021.

[25] G.A.Kaissis, M.R. Makowski, D.Rückert, et al, "Secure, privacy-preservingand federated machine learning in medical imaging," *Nat Mach Intell*, no.2, pp.305–311, 2020.

[26] V. Mothukuri, P. Khare, R. M. Parizi, et al., "Federated learning-based anomaly Detection for IoT security attacks," *IEEE Internet Things,* pp. 2327–4662, 2021.

[27] H.Y. Zhu, et al, "Distributed additive encryption and quantization for privacy preserving federated deep learning," Neurocomputing, vol. 463, pp. 309–327, 2021.

[28] A. Ali and F. Yangyu, "Automatic modulation classification using deep learning based on sparse autoencoders with nonnegativity constraints," *IEEE Signal Proc Let*, vol. 24, no. 11, pp. 1626–1630, 2017.

[29] M. La.ngkvist and A. Loutfi, "Learning feature representations with a cost-relevant sparse autoencoder," *Int J Neural Syst*, vol. 25, no. 1,pp. 1450034, 2015.

[30] C. Dong, J. Li, and Y. Chen, "A DWT-DCT based robust multiple watermarks for medical image," *in Proc. IEEE Int. Conf. Sym Photo Opto*, 2012, pp. 1–4.

[31] J. Liu, J. Li, K. Zhang, U. A. Bhatti, and Y. Ai, "Zero-watermarking algorithm for medical images based on dual-tree complex wavelet transform and discrete cosine transform," *J Med Imag Health In*, vol. 9, no. 1, pp. 188–194, 2019.

[32] X. Wu, J. Li, R. Tu, J. Cheng, U. A. Bhatti, and J. Ma, "Contourlet-DCT based multiple robust watermarkings for medical images," *Multimed Tools Appl*, vol. 78, no. 7, pp. 8463–8480, 2019.

[33] X.Liu, Z. Zhou, and W.C. zhang, "Zero-watermarking algorithm based on Contourlet-DCT hybrid transform," *Video Eng*, vol. 41, no. 4, pp. 32–36, 2017.

[34] M. Sui, J. Li, " Robust watermarking for medical images based on arnold scrambling and DCT," *Appl Res Comp*, vol. 30, no.8, pp.2552–2556, 2013.

[35] B.R.Han, J.L. Du, Y.Y. Jia, and H.,Z.Zhu, "Zero-watermarking algorithm for medical image based on VGG19 deep convolution neural network," *J Healthc Eng*, vol. 2021, pp.1–12 , 2021.

Baoru Han received his M.Sc. in Circuits and Systems from Yanshan University of China in 2007. He received the PhD. degree in Information and Communication Engineering at Hainan University of China in 2016. He is a Professor with the College of Medical Informatics, Chongqing Medical University. His current research interests include medical image processing, artificial intelligence and intelligent medical.

Dr. Rutvij H. Jhaveri (Senior Member IEEE) is Assistant Professor in the Department of Computer Science & Engineering, Pandit Deendayal Energy University, Gandhinagar, India. He conducted his postdoctoral research from Nanyang Technological University, Singapore. He has 19+ years of experience in teaching and research. He obtained his B.E. (Computer Engineering) from Birla Vishvakarma Mahavidyalaya, India, M. Tech (Research) from S.V. National Institute of Technology, Surat, India and Ph.D. from CHARUSAT University, India. In 2017, he was awarded Pedagogical Innovation Award by Gujarat Technological University, India. He authored 90+ publications in various prestigious journals and conferences. His research publications are cited 1700+ times with h-index 20. He also has Australian patents to his credit. He is editorial board member and reviewer of several journals of international repute. He is also serving as a guest editor in several international journals of repute. Apart from this, he also served as a committee member in "Smart Village Project" - Government of Gujarat, India at Bharuch district during the year 2017. He is a life member of several professional bodies such as CSI and ISTE. His research interests include network security, software-defined networking in IIoT/CPS with machinelearning and data analytics.

Han Wang (SM'21) received his B.S. degree in electrical engineering from Hubei University of Nationalities, China, in 2009, the M.S. and Ph.D. degree in information and communication system from Hainan University, Haikou, China, in 2013 and 2017, respectively. He has worked in China Mobile Jiangxi branch as a network engineer for one year. He is an Associate Professor with Yichun University. He is currently a Postdoctoral Research Fellow at City University of Macau. He is the author of over 30 papers published in related international conference proceedings and journals. His current research interests include intelligent communication, filter-bank multicarrier communications and

information theory.

Dawei Qiao received the B. Sc. degree in public management with the School of Medicine, Henan Polytechnic University, Jiaozuo, China, in 2021. Before this, she worked at the Hospital of Henan Polytechnic University from 2015 to 2018. Her current research interests include artificial intelligence, health management, e-health and internet of medical things.

Jinglong Du received the Ph.D. degree from the College of Computer Science, Chongqing University, Chongqing, China, in 2020. He is currently a postdoctoral researcher at the College of Medical Informatics, Chongqing Medical University. His research interests include machine learning, medical image processing and analysis, MRI super-resolution and deep learning.