IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 August 2022, accepted 25 August 2022, date of publication 29 August 2022, date of current version 8 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3202984

RESEARCH ARTICLE

Robust Watermarking via Multidomain Transform Over Wireless Channel: Design and Experimental Validation

JUNTAO MA, JIE CHEN, AND GANG WU, (Member, IEEE)

National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Gang Wu (wugang99@uestc.edu.cn)

This work was supported by the Fundamental Research Funds for the Central Universities under Grant ZYGX2020ZB042.

ABSTRACT Watermarking is a technique that provides ownership rights for shared data, and this technique can also help to transmit confidential information to realize secure communication. In this paper, we design a blind digital watermarking based on Discrete Wavelet Transform-Discrete Cosine Transform-Singular Value Decomposition (DWT-DCT-SVD) and optimize it by genetic algorithm (GA). This watermarking has both high robustness and high imperceptibility. Then we design a transmitter and receiver system based on the IEEE 802.11a and software-defined radio (SDR). We adopt several optimization methods for the system, such as ACK/HARQ mechanism, different redundant coding, frame length adaption, adaptive modulation, and so on, aiming to improve communication reliability and rate. We verify its high communication reliability and rate through actual experiments and complete the combination of digital watermarking and wireless transmission. We could build the application scenario of Image Security Wireless Communication based on Wireless Local Area Network (WLAN) protocol and SDR platform indoors or outdoors in small areas.

INDEX TERMS Discrete cosine transform, discrete wavelet transform, image communication, image forensics, singular value decomposition, wireless LAN.

I. INTRODUCTION

A. MOTIVATION AND BACKGROUND

With the rapid development of computer networks, communication, and digital processing technology, the Internet has gone deep into people's lives, building an information society connected with everything, bringing great convenience and change to people's lives. However, with the rapid spread of all kinds of information on the Internet, information security and copyright protection issues also have arisen. Various information theft and copyright theft incidents have increased, seriously infringing the legitimate rights and interests of digital product holders and becoming a major obstacle to digital technology's healthy and sustainable development. Under this background, information hiding technology is born [1] and thrived, and digital watermarking technology is an essential technology in information hiding technology for the evidence of rightful ownership [2].

In recent years, the application of digital watermarking technologies has developed rapidly, including fields of picture, video, audio, text, software, and so on. All kinds of digital watermarking technology help to ensure information security and copyright [3], [4]. For example, recently emerging central bank digital currencies also use digital watermarking for secure encryption and authentication [5], which can show the importance of digital watermarking technology in such an era of information and network.

The key to digital watermarking technology is using digital processing technology to embed the authentication information with security and confidentiality into the carrier. The performance of digital watermarking mainly depends on three aspects: security, robustness, and imperceptibility [6].

Image Security Wireless Communication in this paper uses WLAN protocol to realize secure image transmission with digital watermarking, even under varying channel conditions.

The associate editor coordinating the review of this manuscript and approving it for publication was Gulistan Raja.

Using this technology, we can build indoor or small-scale outdoor application scenarios for image security communication based on WLAN protocol and SDR platform, in which we can transmit images with watermark under different channel conditions and even transmit secret message as the watermark to ensure covert communication of information.

B. RELATED WORK AND CHANLLENGE

The research on digital watermarking generally includes three directions: Spatial domain, transform domain, and optimization.

The concept of the digital watermark was formally proposed by Van Schyndel *et al.* in an article entitled ''A digital watermark'' published by IEEE in 1994 [7]. They proposed two spatial domain embedding algorithms for the first time, which are more robust but less transparent.

Then Bors and Pitas proposed to embed the digital watermark based on Discrete Cosine Transform (DCT) in [8] in 1996, which marks the beginning of watermark embedding in the transform domain. DCT uses a cosine function as an orthogonal basis for transformation, which is equivalent to the real component of Fourier Transform, so that the coefficients after DCT are all positive numbers. They proposed a DCT-based watermarking algorithm with strong anti-interference ability under a certain JPEG compression ratio. Hsu and Wu also proposed a digital watermarking based on DCT in [9]. By carefully defining the user key, they adopted multiple watermarking and repeated embedding to enhance the robustness. In [10], C.-Y. Lin and S.-F. Chang proposed an effective image authentication technique that prevents malicious manipulation but allows JPEG lossy compression by retaining the relationships between discrete cosine transform coefficients at the same position in different blocks of the image when the DCT coefficients are quantized in JPEG compression.

Since the DCT-based methods were proposed, the algorithms of transform domain such as Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) have appeared successively, which makes digital watermarking possess good transparency, but at the cost of weakening its robustness. Xia *et al.* proposed to embed the digital watermark based on DWT in [11]. DWT has four subbands, representing the low-frequency, horizontal, vertical, and diagonal components. Usually, the digital watermark is embedded in the low-frequency subband, which can obtain high robustness and effectively resist attacks. In this method, Gaussian random noise is added to the significant coefficient of the wavelet transform domain, and decoding is layered. If the distortion of the watermark image is not severe, only a few bands of information can be used to detect the feature, thus saving the amount of calculation. Liu and Tan proposed a digital watermarking method that adds watermarks into the SVD domain of the original image in [12]. Unlike other unitary transformations that use fixed orthogonal bases (such as DFT and DCT), SVD uses an unfixed orthogonal basis, a one-way and asymmetric decomposition. These characteristics make the new algorithm have good performance in both security and robustness.

Since then, many digital watermarks combining SVD with other frequency-domain algorithms have appeared successively. Liu and Liu proposed a digital image watermarking algorithm based on DWT and SVD in [13], which has a stronger anti-attack ability than the SVD method. This algorithm is robust to JEPG compression, noise, low-pass filtering, median filtering, contrast enhancement, and other commonly used signal processing techniques. Lai and Tsai proposed a hybrid image watermarking technique based on DWT and SVD in [14], embedding the watermarking into the singular value of the subband covering the wavelet transform. This technique makes full use of the respective characteristics of the two transform domain methods, and the space-frequency localization of DWT and SVD can effectively represent the inherent algebraic properties of images. Experimental results show that the proposed method improves invisibility and robustness under attack.

The watermarking algorithm based on SVD does not have the disadvantage that traditional watermarking technology cannot resist attack. However, DCT-based watermarking provides compression, while DWT-based compression provides extensibility. Therefore, a new watermarking technique can be created by combining these three transforms. Navas *et al.* mentioned that watermarking method could be built based on DWT-DCT-SVD in [15]. The watermarking information is hidden in the DCT coefficients of the DWT coefficients, which brings robustness to the watermarking, and the visual watermark can be extracted without a reasonable amount of distortion even under various attacks. Although the presented work in this paper has similarities with those work based on DWT-DCT-SVD in [15], [16], and [17], the watermark embedding and extraction algorithm in this paper does not need prior information so that we can realize digital blind watermarking, such as [18].

With the continuous development of machine learning, in addition to the frequency domain algorithm, a digital watermark embedding algorithm based on the support vector machine (SVM) was proposed by Li *et al.* in [19]. Because of the excellent learning and generalization ability in addressing the problem of small sample learning, SVM is a good way to memorize the relationship between randomly selected image pixels and adjacent pixels. At the same time, SVM can adjust or compare the relationship between the embedded pixel and the output of SVM to extract the watermark. The experimental results show that SVM has good visual perception ability, high security, and practicability. Tsai *et al.* present a GA-based adaptive image watermarking technique in [20], aiming to use the GA algorithm to calculate the embedding strength of watermarks to improve the image's detection accuracy of watermarking based on correlation. Haribabu *et al.* proposed a digital image watermarking technology using an auto-encoder based on Convolutional Neural Networks (CNN) in [21], which was CNN's first attempt in the field of watermarking. Uchida *et al.* proposed embedding watermarks into Deep Neural Networks (DNN) in [22]. They defined watermarking requirements, embedding conditions, and attack types in DNN and proposed a general framework to embed watermarks in model parameters using a parameter regularizer. Numerous scientific researchers have studied various digital watermarking algorithms based on machine learning, deep learning, and different optimization algorithms, but high complexity and computation are the nonnegligible issues.

In recent years, there have been many new developments in digital watermarking. In a head-mounted display (HMD), the images should be pre-warped with barrel distortion to cancel pincushion distortion. Thinking about it, Tian *et al.* proposed a robust watermarking resistance against barrel distortion for HMDs in [23]. Considering the generative adversarial network, Hao *et al.* proposed a robust image watermark algorithm in [24], which includes two modules, generator and adversary. Generator is mainly used to embed the watermark into the image and recover the watermark from the image damaged by noise. Adversary is used to damage the image with the embedded watermark by noise.

As for transmission security, Yang and Johansson provided an overview of the potential use of cryptographic primitives in 5th generation mobile communication systems and beyond in [25]. While discussing the new security challenges brought by 5G, they also introduced the upcoming security architecture. Shen *et al.* examined the security challenges in edge-assisted and how the energy consumption constraints affect the design of security solutions in [26]. To solve the threat of privacy disclosure, Qu *et al.* proposed a generative adversarial network enhanced location privacy protection model to hide location and even trajectory information in [27]. It is evident that security is essential in wireless transmission, and this paper aims to utilize the imperceptibility of digital watermarking to realize Image Security Wireless Communication.

However, there are still several technical challenges in digital watermarking that need to be investigated as follows.

- The balance between imperceptibility and robustness of digital watermarking has a significant impact on the performance of digital watermarking, because it is difficult to find the best balance between high imperceptibility and robustness, so this paper takes it to account.
- Traditional digital watermarking is based on wire transmission conditions or not considering the transmission. Still, the communication of digital watermarking under wireless conditions is widespread in real life, and it seems to become a research hotspot in the future.
- Digital watermarking under wireless transmission conditions is affected by channel conditions because channel conditions are not constant but variant in the actual environment. This paper tries to get over the variant transmission conditions.

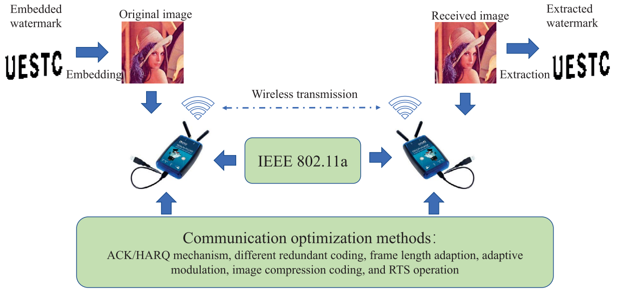

Embedded watermark
UESTC
Embedding
Original image
Received image
Extraction
Extracted watermark
UESTC
Wireless transmission
IEEE 802.11a
Communication optimization methods:
ACK/HARQ mechanism, different redundant coding, frame length adaption, adaptive modulation, image compression coding, and RTS operation

FIGURE 1. The main design framework of this paper.

C. CONTRIBUTIONS

In view of the above challenges, with the above digital watermarking technology on the basis of SDR, the contributions of this paper are as follows. Figure 1 shows the main design framework.

- We design a blind digital watermarking algorithm based on DWT-DCT-SVD and optimize it with genetic algorithm. The method based on DWT-DCT-SVD can make the watermark more imperceptible and robust, and the genetic algorithm optimizes the digital watermark by calculating the most appropriate watermark embedding factor to achieve a balance between robustness and imperceptibility.
- We combine the SDR and the image watermarking process to realize the Image Security Wireless Transmission based on IEEE 802.11a and PLUTO-SDR. We want to build the application scenario for image security communication based on WLAN protocol and SDR platform indoors or in a small outdoor area.
- We construct a transmitting and receiving experimental platform. We optimize and improve it through ACK/HARQ mechanism, different redundant coding, frame length adaption, adaptive modulation, and other methods. As a result, the image transmission rate is increased while the reliability of communication transmission is guaranteed.

II. DESIGN OF DIGTAL WATERMARKING

In this section, we will present our blind digital watermarking algorithm. Firstly, we will show the process flow of watermark embedding and extraction. Then, we will explain the embedding and extraction algorithm in detail. Finally, we will show how to utilize GA to optimize the watermarking.

A. EVALUATION OF WATERMARK

1) PEAK SIGNAL-TO-NOISE RATIO (PSNR)

The formula for PSNR of an image with a size of $M \times N$ is as follows, which mainly characterizes the imperceptibility of the image after the digital watermark is embedded. In general, when the PSNR is greater than 35dB, it is difficult for the human eyes to recognize the change in the image,

$$PSNR = 10\log \frac{255 \times M \times N}{\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}\left[\boldsymbol{I}(i,j)-\boldsymbol{I}'(i,j)\right]^2}, \tag{1}$$

where $\boldsymbol{I}\ (i,j)$ is the pixel value of the original image, $\boldsymbol{I}'\ (i,j)$ is the pixel value of the image embedded with the watermark.

Algorithm 1 Watermark Embedding

```
Require: Original image.
Ensure: Image with watermark.
  1. Convert the image from RGB space to YCrCb space. The size of image is 512 × 512 × 3.
      $\boldsymbol{Y} = 0.299\boldsymbol{R} + 0.587\boldsymbol{G} + 0.114\boldsymbol{B}$,
      $\mathbf{Cb} = -0.1687\boldsymbol{R} - 0.3313\boldsymbol{G} + 0.5\boldsymbol{B} + 128$,
      $\mathbf{Cr} = 0.5\boldsymbol{R} - 0.4187\boldsymbol{G} - 0.0813\boldsymbol{B} + 128$;
  2. Extract the 512 × 512 Y component, perform DWT on the Y component, and extract the 256 × 256 CA component.
      $[\mathbf{CA}, \sim, \sim, \sim] = DWT(\boldsymbol{Y})$;
  3. Perform 4×4 block DCT on the CA component.
      $\mathbf{CA}_{4\times4DCT} = DCT(\mathbf{CA}_{4\times4})$;
  4. Perform SVD on each 4 × 4 CA component after DCT.
      $[\boldsymbol{U}, \boldsymbol{S}, \boldsymbol{V}] = SVD(\mathbf{CA}_{4\times4DCT})$;
  5. Perform Arnold transform on the 64 × 64 watermark WT.
      $\boldsymbol{W} = Arnord(\mathbf{WT})$;
  6. Execute the watermark embedding algorithm on each matrix S according to the matrix W. WatEmb presents the function of the watermark embedding.
      $\tilde{\boldsymbol{S}} = WatEmb(\boldsymbol{S}, \boldsymbol{W})$;
  7. Synthesize a new 4 × 4 DCT block.
      $\tilde{\mathbf{CA}}_{4\times4DCT} = SVD_{synthesize}(\tilde{\boldsymbol{S}}, \boldsymbol{V}, \boldsymbol{D})$;
  8. Perform IDCT on each DCT block.
      $\tilde{\mathbf{CA}}_{4\times4} = IDCT(\tilde{\mathbf{CA}}_{4\times4DCT})$;
  9. Combine all the new 4 × 4 CA blocks into a new 256 × 256 CA component, and synthesize the new Y component by IDWT.
      $\tilde{\boldsymbol{Y}} = IDWT([\tilde{\mathbf{CA}}, \sim, \sim, \sim])$;
  10. Convert the image from YCrCb space to RGB space.
      $\tilde{\boldsymbol{R}} = \tilde{\boldsymbol{Y}} + 1.402(\mathbf{Cr} - 128)$,
      $\tilde{\boldsymbol{G}} = \tilde{\boldsymbol{Y}} - 0.34414(\mathbf{Cb} - 128) - 0.71414(\mathbf{Cr} - 128)$,
      $\tilde{\boldsymbol{B}} = \tilde{\mathbf{Y}} + 1.772(\mathbf{Cb} - 128)$;
```

2) NORMALIZED CORRELATION (NC)

The formula for NC of the digital watermark with a size of $P \times Q$ is as follows, which mainly characterizes the robustness of the digital watermark in the attack and extraction process,

$$NC = \frac{\sum_{i=1}^{P-1}\sum_{j=1}^{Q-1} \boldsymbol{W}(i,j)\boldsymbol{W}'(i,j)}{\sum_{i=1}^{M-1}\sum_{j=1}^{N-1} \boldsymbol{W}(i,j)^2}, \tag{2}$$

where $\boldsymbol{W}\ (i,j)$ is the pixel value of the digital watermark, and $\boldsymbol{W}'\ (i,j)$ is the pixel values of the extracted watermark.

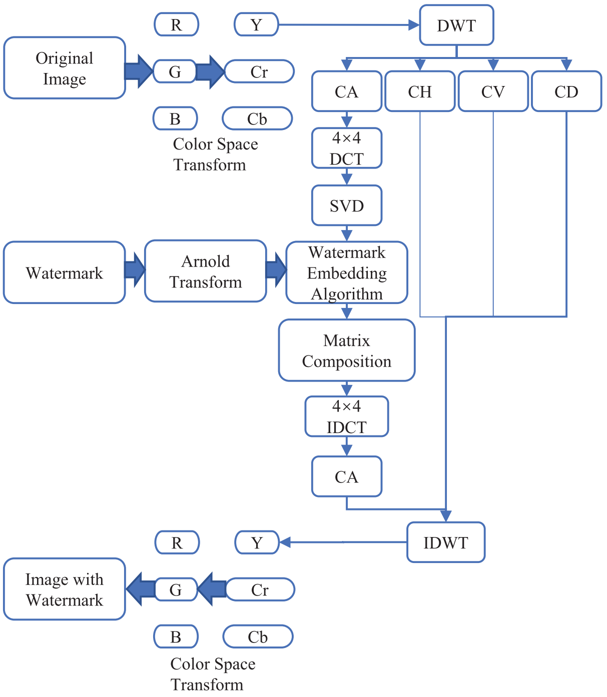


FIGURE 2. **Watermark embedding process.**

B. WATERMARK EMBEDDING

The watermark embedding process is shown as Algorithm 1 and Figure 2.

C. WATERMARK EXTRACTION

The watermark extraction process is shown as Algorithm 2 and Figure 3.

Algorithm 2 Watermark Extraction

```
Require: Image with watermark.
Ensure: Watermark.
  1. Convert the image from RGB space to YCrCb space. The size of image is 512 × 512 × 3.
      $\boldsymbol{Y} = 0.299\boldsymbol{R} + 0.587\boldsymbol{G} + 0.114\boldsymbol{B}$,
      $\mathbf{Cb} = -0.1687\boldsymbol{R} - 0.3313\boldsymbol{G} + 0.5\boldsymbol{B} + 128$,
      $\mathbf{Cr} = 0.5\boldsymbol{R} - 0.4187\boldsymbol{G} - 0.0813\boldsymbol{B} + 128$;
  2. Extract the 512 × 512 Y component, perform DWT on the Y component, and extract the 256 × 256 CA component.
      $[\mathbf{CA}, \sim, \sim, \sim] = DWT(\boldsymbol{Y})$;
  3. Perform 4×4 block DCT on the CA component.
      $\mathbf{CA}_{4\times4DCT} = DCT(\mathbf{CA}_{4\times4})$;
  4. Perform SVD on each 4 × 4 CA component after DCT.
      $[\boldsymbol{U}, \boldsymbol{S}, \boldsymbol{V}] = SVD(\mathbf{CA}_{4\times4DCT})$;
  5. Execute the watermark extraction algorithm on each Matrix S to obtain the matrix M. WatExt presents the function of the watermark extraction.
      $\boldsymbol{W} = WatExt(\boldsymbol{S})$;
  6. Perform Arnold inverse transform on the matrix W to obtain the watermark WT.
      $\mathbf{WT} = Arnord_{inverse}(\boldsymbol{W})$;
```

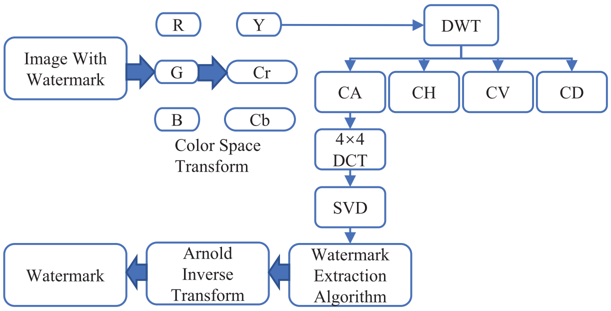


FIGURE 3. Watermark extraction process.

D. WATERMARK ALGORITHM

1) WATERMARK EMBEDDING ALGORITHM

The matrix $\boldsymbol{S}$ has the same number of elements as the watermark has the same number of pixels. For each matrix $\boldsymbol{S}$ of DCT block, $\boldsymbol{S}_{i,j}\left(1,1\right)$ is extracted in the 4×4 matrix $\boldsymbol{S}_{i,j}$, which is in row i and column j of the matrix $\boldsymbol{S}$. β is obtained by dividing $\boldsymbol{S}_{i,j}\left(1,1\right)$ by the watermark embedding factor α and rounding up,

$$\beta=\left\lceil\frac{\boldsymbol{S}_{i,j}\left(1,1\right)}{\alpha}\right\rceil. \tag{3}$$

Then the following operations are performed on $\boldsymbol{S}_{i,j}(1,1)$ according to the parity of β and the pixel value of the watermark image,

$$\boldsymbol{S}_{i,j}\left(1,1\right)=\begin{cases}\beta\times\alpha & \boldsymbol{W}\left(i,j\right)=0 \text{ and } \beta \text{ is odd}\\(\beta+1)\times\alpha & \boldsymbol{W}\left(i,j\right)=0 \text{ and } \beta \text{ is even}\\(\beta+1)\times\alpha & \boldsymbol{W}\left(i,j\right)=1 \text{ and } \beta \text{ is odd}\\\beta\times\alpha & \boldsymbol{W}\left(i,j\right)=1 \text{ and } \beta \text{ is even}\end{cases}, \tag{4}$$

where $\boldsymbol{W}\left(i,j\right)$ is the pixel value in row i and column j of the scrambled binary watermark image.

2) WATERMARK EXTRACTION ALGORITHM

For each matrix $\boldsymbol{S}$ of DCT block, $\boldsymbol{S}_{i,j}\left(1,1\right)$ is extracted in the 4×4 matrix $\boldsymbol{S}_{i,j}$, which is in row i and column j of the matrix $\boldsymbol{S}$. β is obtained by dividing $\boldsymbol{S}_{i,j}\left(1,1\right)$ by the watermark embedding factor α and rounding up. According to the following judgment, the scrambled watermark is obtained,

$$\boldsymbol{W}\left(i,j\right)=\begin{cases}1 & \beta \text{ is even}\\0 & \beta \text{ is odd}\end{cases}, \tag{5}$$

where $\boldsymbol{W}\left(i,j\right)$ is the pixel value in row i and column j in the scrambled binary watermark image.

After that, we will obtain the hidden watermark without any prior information.

E. OPTIMIZATION WITH GENETIC ALGORITHM

The embedding factor of the digital watermark determines the balance between the robustness and transparency of the digital watermark. If the fixed embedding factor is simply set without thinking, it may cause a large gap in the performance of the digital watermark in different images.

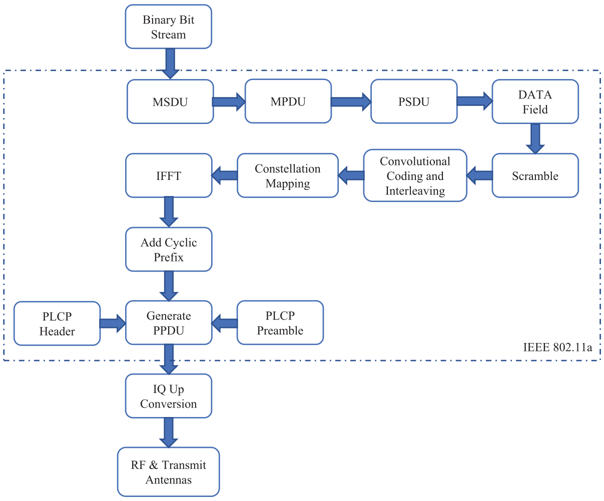


FIGURE 4. Transmitter block diagram.

Jagadeesh *et.al.* proposed a method that uses the genetic algorithm to optimize digital watermarking in [28]. Therefore, the genetic algorithm is also used in this paper to calculate the most suitable embedding factor to achieve the best balance of imperceptibility and robustness.

The fitness function is set as,

$$F=PSNR+\gamma NC, \tag{6}$$

where F means fitness, and γ is the weight of NC in the fitness function, which is the key to determining PSNR and NC. The optimal value of different images should be tested by multiple times.

III. WIRELESS WATERMARKING PROTOTYPE BASED ON IEEE 802.11a

In this section, we will present our transmitter and receiver system based on IEEE 802.11a [29]. Firstly, the transmitter and the receiver design are shown with process flow. Then we will explain how to use several optimization methods to optimize the communication system to improve communication rate and reliability.

A. TRANSMITTER DESIGN

The design of the transmitter is shown in Figure 4. Depending on IEEE 802.11a, the transmitter converts binary bitstreams to MAC service data units (MSDUs), MAC protocol data units (MPDUs), and physical service data units (PSDUs) in sequence and then completes the steps of the MAC layer. Then the transmitter performs physical operations on the data to generate physical protocol data units (PPDUs) and the transmitted signal. It's noticed that the transmitter will transmit signals at different coding rates and adjust the modulation order adaptively. Details are provided in the following section.

B. RECEIVER DESIGN

The design of the receiver is shown in Figure 5 according to IEEE 802.11a, including basic physical and MAC

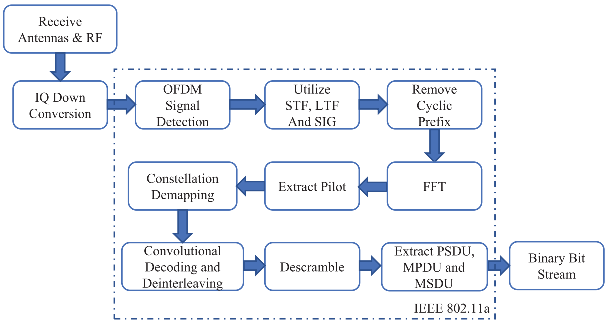


FIGURE 5. Receiver block diagram.

layer operations. In addition, the receiver will perform ARQ/HARQ operations according to the results of the cyclic redundancy check (CRC).

C. COMMUNICATION OPTIMIZATION METHODS

The following optimization methods are adopted at the transmitter and receiver to increase the image communication rate, reduce the transmission error rate, and ensure the reliability and efficiency of communication.

To effectively improve transmission reliability in the case of channel degradation, the transmitter and receiver adopt ACK/HARQ mechanism. After receiving the packet, the receiver will send acknowledge character (ACK) or hybrid automatic repeat request (HARQ) according to the results of the CRC, and the transmitter will execute the next step according to the received packet.

However, ACK and HARQ will bring about the delay between each packet received correctly. In consideration of it, the frame length adaption is adopted. The transmitter and receiver use windows of the same length, and each window consists of MPDU frames depending on the prearranged number. It can sharply reduce the influence of delay.

Besides, the transmitter adopts different redundant coding and adaptive modulation to improve the communication reliability and rate. At the transmitter, different redundant coding methods with the same traceback and different coding rates are used for each packet. Even if the channel becomes worse, the channel coding still has some degree of error correction ability. Adaptive modulation means that the receiver determines the modulation order based on the calculated SNR and sends it to the transmitter by ACK or HARQ. Then the transmitter sets the modulation order of the WLAN baseband signal according to the received packet. The method of adaptive modulation can effectively deal with changes in the channel environment.

The massive amount of data transmission bits is also a problem that needs to be considered. Before the transmission, the data will be processed by image compression coding, which can effectively reduce the number of transmission bits of the image. The coding includes JPEG compression, Run Length Encoding, and Huffman Encoding.

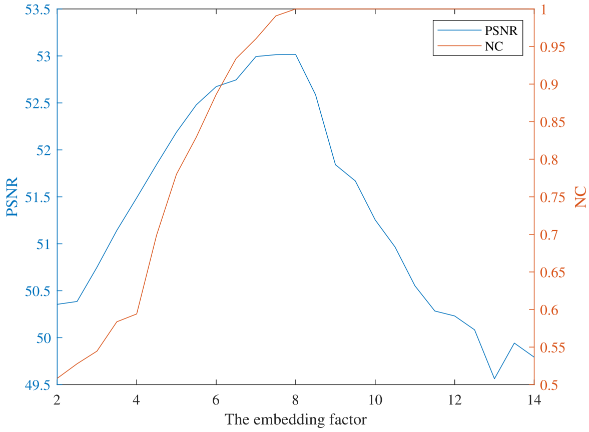


FIGURE 6. The relation between the embedding factor and PSNR/NC.

Before the transmitter transmits data for the first time, it will send a Request-to-Send (RTS) signal. When the receiver receives the RTS signal, it will send an ACK signal for confirmation to complete the handshake operation, thus ensuring the transceiver synchronization of the transmitter and receiver.

IV. SIMULATION AND EXPERIMENTAL RESULTS

In this section, we mainly conduct three evaluation experiments: digital watermark performance evaluation, packet error rate experiment, and SDR-based image communication experiment.

A. DIGITAL WATERMARK PERFORMANCE EVALUATION

1) RELATION BETWEEN EMBEDDING FACTOR, PSNR AND NC

The image chosen in this experiment is Lena. tiff, and the embedding factor ranges from 2 to 12.

From Figure 6, we can see the relation between the embedding factor and PSNR/NC. With the increase of the embedding factor, PSNR will show a peak-like trend of rising first and then declining, while NC will continue to increase until 1. This result visually verifies the importance of using the GA algorithm to find the optimal embedding factor to achieve the best balance between PSNR and NC.

2) EXPERIMENT RESULTS OF WATERMARK EMBEDDING FACTORS

Four images are used as the digital watermark embedding test images: Lena. tiff, Peppers. tiff, Baboon. tiff, and Airplane. tiff. Because the weight γ in the fitness function in the genetic algorithm is different, the optimal embedding factor is different. For each image, 44, 46, and 48 are used as the weight γ in the genetic algorithm to obtain the best embedding factor, PSNR, and NC. Besides, the algorithm proposed in this paper will be compared with the methods in [16], [17], and [18] on PSNR and NC.

It can be obtained from Table 1 that the optimal watermark embedding factor calculated by GA can make the PSNR of

TABLE 1. Optimal embedding factor for different images.

Image	γ	Best embedding factor	PSNR(dB)	NC
Lena	44	7.7433	53.2916	0.9986
	46	7.9342	53.0633	0.9997
	48	8.0478	53.1640	1.0000
Peppers	44	8.0472	53.2400	1.0000
	46	8.0085	53.2293	1.0000
	48	8.1281	53.2426	1.0000
Baboon	44	7.4966	53.0699	0.9986
	46	7.6078	53.0391	1.0000
	48	7.8893	53.0335	1.0000
Airplane	44	7.9969	53.2194	1.0000
	46	7.9873	53.1463	1.0000
	48	7.9863	53.1742	1.0000

TABLE 2. Comparison of the PSNR and NC of the proposed algorithm with other methods.

Methods	PSNR	NC
Methods [16]	49.3073	1.0000
Methods [17]	43.1230	1.0000
Methods [18]	35.2462	1.0000
proposed algorithm	53.1640	1.0000

the image far beyond the bounds of human perception by 35 dB, reaching about 50 dB. It indicates that the digital watermark has strong imperceptibility and is extremely too difficult to perceive that it can effectively play a hidden role. At the same time, the optimal watermark embedding factor can also make the NC of the digital watermark high, indicating that the digital watermark has very high robustness. Table 2 shows that compared with other algorithms, the watermarking algorithm proposed in this paper has the highest PSNR based on ensuring NC.

Unless watermarks, confidential images or binary bitstreams can also be embedded into images to achieve the purpose of secure and confidential communication. It can be seen from the above results that the digital watermark algorithm can bring higher PSNR and NC, which means the embedded content will have strong imperceptibility and robustness. Coupled with the unique digital watermark embedding and extraction algorithm, it will significantly increase the difficulty of stealing digital watermark or embedded content. Therefore, the digital watermarking has a high level of security.

Figure 7 shows that as the number of iterations increases, the optimal fitness of each generation will continue to converge to the optimal solution.

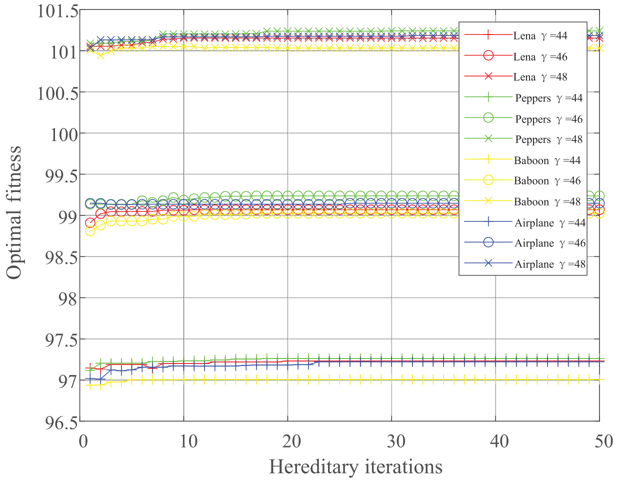


FIGURE 7. The convergence of genetic algorithm iteration.

TABLE 3. The NC of different images under attack.

Attack type	Lena	Peppers	Baboon	Airplane
PSNR (dB)	40.9756	40.7727	40.7224	41.3901
No attack	1	1	1	1
Brightness adjustment (+4)	0.9737	0.9557	0.9994	0.9984
Brightness adjustment (-4)	0.9598	0.9728	0.9899	0.9624
Gaussian noise(σ=0.01)	0.9473	0.9131	0.9583	0.9964
Salt and pepper(σ=0.01)	0.9928	0.9832	0.9968	0.9887
Median filter(3×3)	0.9948	0.9974	0.9343	0.9913
Mean filter (3×3)	0.9496	0.9682	0.9537	0.9557
Gaussian filter(3×3)	0.9563	0.9748	0.9655	0.9650
Clipping attack (1/16)	0.9259	0.9259	0.9259	0.9259
Clipping attack (1/8)	0.8706	0.8706	0.8706	0.8706
JPEG compression	1	0.9994	1	1

TABLE 4. Comparison of the NC of the proposed algorithm with method [18] under attack.

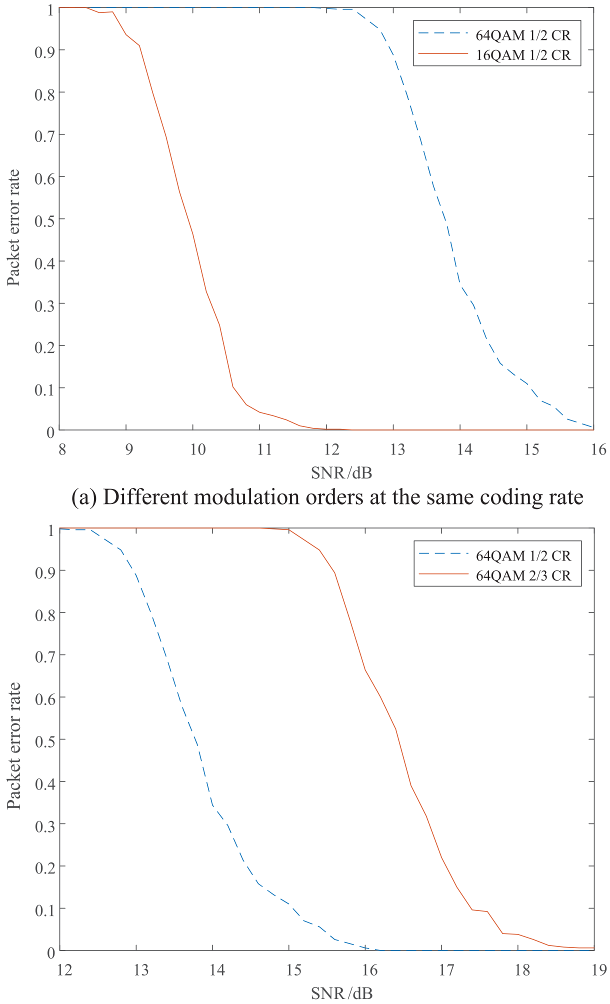
Attack type	method [18]	proposed algorithm
No attack	1.0000	1.0000
JPEG compression	1.0000	1.0000
Gaussian noise	0.8723	0.9473
Re-quantization	0.9875	1.0000
Up-sampling	1.000	1.000
Down-sampling	1.000	1.000
Low-pass filtering	1.000	1.000

3) ROBUSTNESS TEST RESULTS AND ANALYSIS OF WATERMARK

The images used in the robustness experiment are Lena. tiff, Peppers. tiff, Baboon. tiff, and Airplane. tiff. The image attack methods include brightness adjustment, noise attack, filter attack, clipping attack, and compression attack, including most of the attacks on digital images.

In addition, the NC of the proposed watermarking algorithm under various attacks is compared with method [18], which is also a blind watermarking algorithm. The test image is Lena. tiff.

From Table 3, it can be concluded that the digital watermark designed in this paper has good robustness against brightness adjustment, noise attacks, cropping attacks, filtering attacks, and JPEG compression attacks. Because of its excellent robustness against JPEG compression, the



(a) Different modulation orders at the same coding rate

(b) Different coding rates for the same modulation order

FIGURE 8. **Packet error rate under different modulation methods and coding rates.**

watermark can still be extracted wholly and effectively after image compression and decompression processing, ensuring its reliability in the communication transmission process.

Table 4 shows that compared with method [18], the watermarking algorithm proposed in this paper has the same excellent ability to resist JPEG compression, sampling, and filtering. Moreover, it has better performance under attacks of Gaussian noise and re-quantization.

In summary, the digital watermark designed in this paper can obtain the best balance between robustness and imperceptibility, which means it can simultaneously bring high imperceptibility and robustness.

B. PACKET ERROR RATE EXPERIMENT

Five hundred packets of data are generated randomly to calculate the packet error rate in this experiment. The first group is set to 64QAM while the convolutional coding rate is 1/2 and 16QAM while the convolutional coding rate is 1/2. The second group is set to 64QAM while the convolutional coding rate is 1/2 and 64QAM while the convolutional coding rate is 2/3. The simulation test condition selected the Gaussian channel. The result is shown in Figure 8.

It can be seen from the result that although the higher modulation order can increase the communication rate, the system will have poorer anti-interference performance as a price. The coding rate will also affect the anti-interference ability, and the lower coding rate means more redundant bits. Therefore, the system will have a stronger anti-interference ability.

The methods of different redundant coding and adaptive modulation designed in this paper will significantly ensure the balance between the communication rate and the anti-interference ability of the communication. Using different coding rates means that the lower coding rate will ensure transmission reliability if the channel deteriorates. Using adaptive modulation implies that when the channel deteriorates, a lower modulation order is used to provide transmission reliability. In contrast, a higher modulation order is used to ensure the transmission rate when the channel returns to normal.

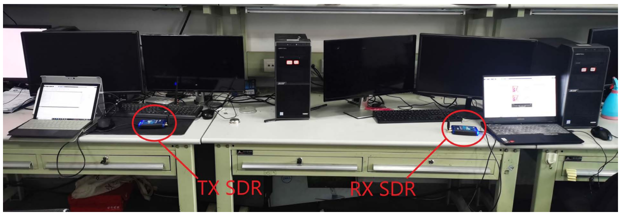


FIGURE 9. **Actual experiment environment.**

TABLE 5. **Setting of experimental conditions.**

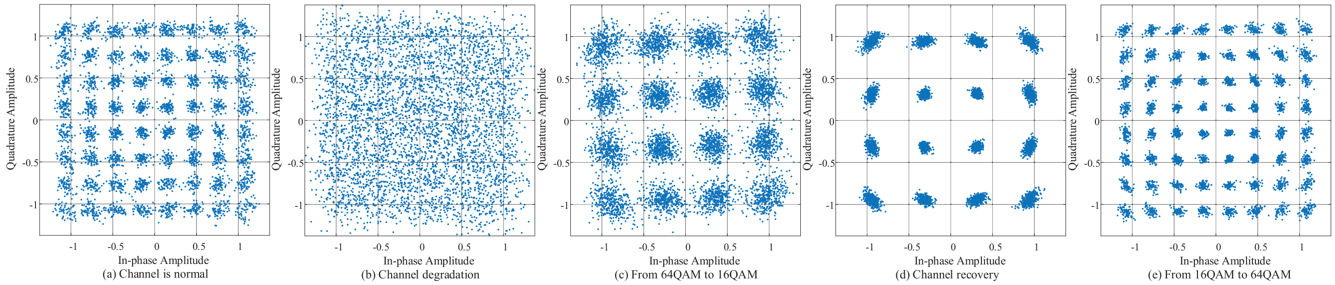
Parameter	Value
The carrier center frequency of data transmission	3.2 GHz
The carrier center frequency of ACK transmission	1.7 GHz
The watermark embedding factor	45
The gain of the transmitter	-10 dB
The gain of the receiver	AGC mode
The frame length	5

C. SDR-BASED IMAGE SECURITY COMMUNICATION EXPERIMENT

The actual experiment in this paper is based on the MATLAB software platform and ADALM PLUTO hardware platform. ADALM-PLUTO is an SDR hardware module designed and produced by Analog Devices Inc (ADI), which is based on AD9363 and provides a receiving and transmitting channel. The parameters of ADALM-PLUTO are shown in [30], the setting of experimental conditions is shown in Table 5, and the actual experiment environment is shown in Figure 9.

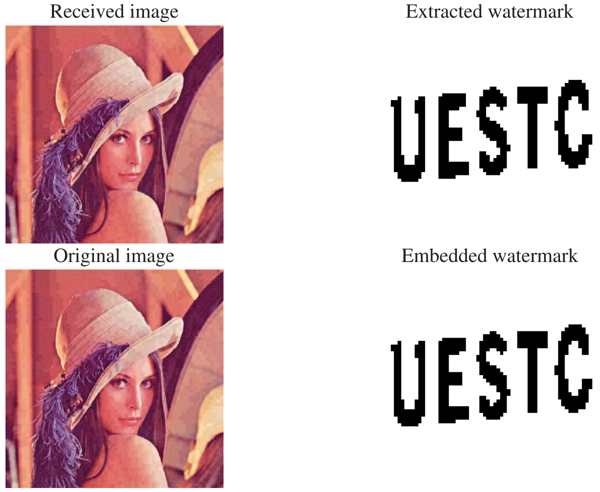
1) CONSTELLATION DIAGRAM EXPERIMENT

Figure 10 shows the change in the receiver's constellation diagram under changing channel conditions, in which channel condition deteriorates from normal and returns to normal.



(a) Channel is normal (b) Channel degradation (c) From 64QAM to 16QAM (d) Channel recovery (e) From 16QAM to 64QAM

FIGURE 10. Constellation diagrams under changing channel conditions.



Received image Extracted watermark Original image Embedded watermark

FIGURE 11. The comparison of transmission and reception.

TABLE 6. EVM and SNR in different constellation diagrams.

Condition	Constellation	EVM Peak	EVM RMS	SNR
Normal	(a)	21.718%	4.833%	30.8 dB
Deterioration	(b)	58.737%	13.506%	13.6 dB
Deterioration	(c)	58.263%	17.991%	17.1 dB
Normal	(d)	32.197%	7.938%	28.8 dB
Normal	(e)	18.962%	4.895%	30.6 dB

The modulation order is adaptively reduced when the channel condition deteriorates to ensure communication reliability. When the channel condition returns to normal, the transmitter and receiver restore the modulation order to provide a high communication rate.

2) EVM AND SNR EXPERIMENT

Table 6 shows the EVM and SNR tested by the receiver corresponding to the five constellation diagrams in the constellation diagram experiment. When the channel condition deteriorates, the EVM is higher, and the SNR is lower. When the channel condition becomes normal, the EVM decreases while the SNR increases.

3) COMPARISON EXPERIMENT OF SENDING AND RECEIVING IMAGES AND WATERMARK

Figure 11 shows the comparison of the original image, received image, embedded watermark, and extracted watermark, which verifies the success of the combination of digital watermarking and wireless transmission.

Through the above experiments, it can be seen that even under the deterioration of channel conditions, adaptive modulation and ACK/HARQ mechanism can balance the reliability and the rate of the communication system so that the communication system can obtain a high communication rate based on high reliability.

V. CONCLUSION AND POTENTIAL FUTURE DIRECTIONS

In this paper, we design a blind digital watermarking algorithm based on DWT-DCT-SVD and optimize it by the genetic algorithm. Then we verify its high imperceptibility and robustness through experiments and evaluation. Because of its high PSNR and the unique embedding and extraction algorithm proposed in this paper, we can fully guarantee its security so that confidential information can be embedded into the image as the watermark for secure communication and image forensics.

We design a transmitter and receiver system based on the IEEE 802.11a standard and combine it with digital watermarking to achieve Image Security Wireless Communication. We adopt the methods of ACK/HARQ mechanism, different redundant coding, frame length adaption, adaptive modulation, image compression coding, and RTS operation to ensure both high communication rate and reliability.

Toward future watermarking, there are still the following open problems, including machine learning and deep learning to realize the extraction of the watermark and fragile watermark to identify a tampered picture.

REFERENCES

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[3] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, no. 6, pp. 1064–1087, Jun. 1998.

[4] S. H. Low, N. F. Maxemchuk, and A. M. Lapone, "Document identification for copyright protection using centroid detection," *IEEE Trans. Commun.*, vol. 46, no. 3, pp. 372–383, Mar. 1998.

[5] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: Drivers, approaches and technologies," Bank Int. Settlements, Basel, Switzerland, BIS Working Papers 880, 2020.

[6] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.

[7] R. G. V. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2. Austin, TX, USA, Dec. 1994, pp. 86–90.

[8] A. G. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in *Proc. 3rd IEEE Int. Conf. Image Process.*, vol. 3. Lausanne, Switzerland, Sep. 1996, pp. 231–234.

[9] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. Image Process.*, vol. 8, no. 1, pp. 58–68, Jan. 1999.

[10] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, no. 2, pp. 153–168, Feb. 2001.

[11] X. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," in *Proc. Int. Conf. Image Process.*, vol. 1, Oct. 1997, pp. 548–551.

[12] R. Z. Liu and T. N. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Aug. 2002.

[13] F. Liu and Y. Liu, "A watermarking algorithm for digital image based on DCT and SVD," in *Proc. Congr. Image Signal Process.*, May 2008, pp. 380–383.

[14] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.

[15] K. A. Navas, M. C. Ajay, M. Lekshmi, T. S. Archana, and M. Sasikumar, "DWT-DCT-SVD based watermarking," in *Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops (COMSWARE)*, Jan. 2008, pp. 271–274.

[16] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik Int. J. Light Electron Opt.*, vol. 127, no. 2, pp. 964–972, 2016.

[17] A. A. Arrasyid, D. R. I. M. Setiadi, M. A. Soeleman, C. A. Sari, and E. H. Rachmawanto, "Image watermarking using triple transform (DCT- DWT-SVD) to improve copyright protection performance," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Nov. 2018, pp. 522–526.

[18] A. Rezaei and M. Khalili, "A robust blind audio watermarking scheme based on DCT-DWT-SVD," in *Fundamental Research in Electrical Engineering*. Switzerland: Springer, 2019, pp. 101–113.

[19] C.-h. Li, Z.-d. Lu, and K. Zhou, "An image watermarking technique based on support vector regression," in *Proc. IEEE Int. Symp. Commun. Inf. Technol. (ISCIT)*, Oct. 2005, pp. 177–180.

[20] H.-H. Tsai, W.-Y. Wang, X.-X. Yu, and H.-L. Won, "GA-based adaptive image watermarking with JND profile and fuzzy inference system," in *Proc. NSIP Abstr. IEEE-Eurasip Nonlinear Signal Image Process.*, May 2005, p. 5.

[21] K. Haribabu, G. R. K. S. Subrahmanyam, and D. Mishra, "A robust digital image watermarking technique using auto encoder based convolutional neural networks," in *Proc. IEEE Workshop Comput. Intell., Theories, Appl. Future Directions (WCI)*, Dec. 2015, pp. 1–6.

[22] Y. Uchida, Y. Nagai, S. Sakazawa, and S. Satoh, "Embedding watermarks into deep neural networks," in *Proc. ACM Int. Conf. Multimedia Retr.*, Jun. 2017, pp. 269–277.

[23] H. Tian, Y. Xiao, G. Cao, J. Ding, and B. Ou, "Robust watermarking of mobile video resistant against barrel distortion," *China Commun.*, vol. 13, no. 9, pp. 131–138, Sep. 2016.

[24] K. Hao, G. Feng, and X. Zhang, "Robust image watermarking based on generative adversarial network," *China Commun.*, vol. 17, no. 11, pp. 131–140, Nov. 2020.

[25] J. Yang and T. Johansson, "An overview of cryptographic primitives for possible use in 5G and beyond," *Sci. China Inf. Sci.*, vol. 63, no. 12, Nov. 2020, Art. no. 220301.

[26] S. Shen, K. Zhang, Y. Zhou, and S. Ci, "Security in edge-assisted Internet of Things: Challenges and solutions," *Sci. China Inf. Sci.*, vol. 63, no. 12, Nov. 2020, Art. no. 220302.

[27] Y. Qu, J. Zhang, R. Li, X. Zhang, X. Zhai, and S. Yu, "Generative adversarial networks enhanced location privacy in 5G networks," *Sci. China Inf. Sci.*, vol. 63, no. 12, Nov. 2020, Art. no. 220303.

[28] B. Jagadeesh, S. S. Kumar, and K. R. Rajeswari, "Image watermarking scheme using singular value decomposition, quantization and genetic algorithm," in *Proc. Int. Conf. Signal Acquisition Process.*, Feb. 2010, pp. 120–124.

[29] *Part11: Wireless LAN Medi um Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band*, Standard 802.11a, 1999.

[30] *ADALM-PLUTO Datasheet (PDF) Analog Devices*. Accessed: May 15, 2022. [Online]. Available: https://pdf1.alldatasheet.com/datasheet-pdf/view/1354493/AD/ADALM-PLUTO.html

JUNTAO MA was born in Sichuan, China, in 1998. He received the B.S. degree in electronic and information engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2021, where he is currently pursuing the M.S. degree in information and communication engineering. His current research interests include 5G communication and quality of experience.

JIE CHEN was born in Sichuan, China, in 1998. He received the B.S. degree in electronic and information engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2021, where he is currently pursuing the M.S. degree in information and communication engineering. His current research interests include 5G communication and quality of experience.

GANG WU (Member, IEEE) received the B.Eng. and M.Eng. degrees from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 1996 and 1999, respectively, and the Ph.D. degree from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2004.

In June 2004, he joined UESTC, where he is currently a Professor with the National Key Laboratory of Science and Technology on Communications. He was a Research Fellow of the Positioning and Wireless Technology Centre, Nanyang Technological University, Singapore, from November 2005 to February 2007. He was a Visiting Professor with the Georgia Institute of Technology, Atlanta, GA, USA, from October 2009 to September 2010. His research interests include signal processing and resource management for 5G/6G and artificial intelligence for PHY/MAC design in wireless communications systems. He was a co-recipient of the IEEE GLOBECOM 2012 Best Paper Award. He is currently an Associate Editor of *Science China Information Sciences*, the Chair of IEEE Comsoc Chengdu Chapter, and the Secretary of the IEEE Chengdu Section.