



Research article

Digital media zero watermark copyright protection algorithm based on embedded intelligent edge computing detection

Hongyan Xu*

Department of Academic Research, Harbin Normal University, Harbin 150025, Heilongjiang, China

* **Correspondence:** Email: hsdxhy100@hrbnu.edu.cn.

Abstract: With the rapid development of computer technology and network communication technology, copyright protection caused by widely spread digital media has become the focus of attention in various fields. For digital media watermarking technology research emerge in endlessly, but the results are not ideal. In order to better realize the copyright identification and protection, based on the embedded intelligent edge computing detection technology, this paper studies the zero watermark copyright protection algorithm of digital media. Firstly, this paper designs an embedded intelligent edge detection module based on Sobel operator, including image line buffer module, convolution calculation module and threshold processing module. Then, based on the embedded intelligent edge detection module, the Arnold transform of image scrambling technology is used to preprocess the watermark, and finally a zero watermark copyright protection algorithm is constructed. At the same time, the robustness of the proposed algorithm is tested. The image is subjected to different proportion of clipping and scaling attacks, different types of noise, sharpening and blur attacks, and the detection rate and signal-to-noise ratio of each algorithm are calculated respectively. The performance of the watermark image processed by this algorithm is evaluated subjectively and objectively. Experimental data show that the detection rate of our algorithm is the highest, which is 0.89. In scaling attack, the performance of our algorithm is slightly lower than that of Fourier transform domain algorithm, but it is better than the other two algorithms. The Signal to Noise Ratio of the algorithm is 36.854% in P6 multiplicative noise attack, 39.638% in P8 sharpening edge attack and 41.285% in fuzzy attack. This shows that the algorithm is robust to conventional attacks. The subjective evaluation of 33% and 39% of the images is 5 and 4. The mean values of signal to noise ratio, peak signal to noise ratio, mean square error and mean absolute difference are 20.56, 25.13, 37.03 and 27.64, respectively. This shows that the watermark image processed by this algorithm has high quality. Therefore, the digital media zero watermark copyright protection algorithm based on embedded intelligent edge computing detection is more robust, and its watermark invisibility is also

very superior, which is worth promoting.

Keywords: embedded intelligent edge detection; zero watermarking algorithm; copyright protection; digital media; algorithm robustness

1. Introduction

1.1. Background significance

The development of the Internet has provided effective and convenient means for accessing digital products. However, due to the digital nature of digital media works, they are easily tampered with and attacked during transmission, and copyright protection has a long way to go [1,2]. Attackers duplicating, tampering and disseminating these copyright-applied digital product publications without the authorization of the product author to obtain illegal income. This behavior harms the interests of copyright owners and related publishers, and also hinders them. The orderly development of the multimedia industry and copyright protection industry. Digital watermarking technology plays an important role in the copyright protection of digital media information. It is a new direction in the field of information security. Better research on digital watermarking technology can help improve the efficiency of digital media information copyright protection. The zero-watermark technology is an emerging digital watermark technology that realizes copyright protection by embedding watermarks without any modification to the original image. How to improve the robustness of the zero-watermark technology is one of the important contents of current research.

1.2. Related work

Image edge detection technology has been developing with the progress of the times, and the research results are also quite rich, which is widely used in different fields. Wang C proposed a robust zero-watermarking algorithm for stereo images. Calculate the TRHFM of the original stereo image, and then use logical mapping to randomly select TRHFM; the article uses the amplitude of the selected TRHFMs to obtain a binary feature image, and applies bitwise XOR operation to the replaced logo image and binary feature image to obtain a zero watermark image. The results show that the proposed stereo image zero-watermarking algorithm has strong robustness against various asymmetric and symmetrical attacks, and has superiority compared with other zero-watermarking algorithms [3]. Xia extends the traditional integer-order polar harmonic transforms (IoPHTs) to the decimal order to construct DoPHTs, which effectively improves the performance of IoPHTs. Three forms of DoPHT are used to construct triple zero watermark information. Geometrically invariant DoPHTs are used to improve its robustness to geometric attacks, and a chaotic system is used to scramble the logo image and feature image to enhance its security. The results show that the algorithm has strong robustness to common image processing attacks and geometric attacks, and is better than other algorithms [4]. Watermark copyright protection algorithm can realize the copyright protection of digital media works, which has been a hot topic in various fields. Zhang introduced the advantages and disadvantages of digital watermarking technology in copyright protection, the characteristics of 3D geological model itself, and the relatively mature 3D model digital watermarking algorithm [5]. In order to protect the

copyright of digital assets, Wang proposed a digital watermarking technology which embeds color fast response code into color image [6]. He uses contourlet discrete cosine transform singular value assignment (DCT-SVD) technology to embed and extract the watermark, and Arnold scrambling encryption is applied to the watermark. His research has important reference significance for this study. Although the robustness of watermark is strong, its invisibility needs to be further improved.

1.3. Innovative points in this paper

In order to improve the robustness of the zero-watermark copyright protection algorithm and improve the quality of watermarked images, this paper studies the zero-watermark copyright protection algorithm based on embedded intelligent edge computing detection technology. The innovations of this research are as follows: (1) Based on Sobel operator, an embedded intelligent edge detection module is designed, including image line buffer module, convolution calculation module and threshold processing module. (2) Based on the embedded intelligent edge detection module designed in this paper, combined with Arnold transform technology and transform domain algorithm, a zero-watermark copyright protection algorithm is constructed. (3) The robustness of the proposed algorithm is tested by cropping, zooming, sharpening and fuzzing attacks. The algorithm solves the contradiction between watermark transparency and robustness, and has good robustness to common signal processing.

2. Embedded intelligent edge computing detection and zero watermark copyright protection algorithm

2.1. Embedded intelligent image edge detection

2.1.1. Embedded image acquisition

Embedded system is application-oriented and based on computer technology, including embedded processor, peripheral hardware equipment, embedded operating system and user's application software [7]. The basic principle of embedded processor is similar to that of ordinary desktop computer, but the former can adapt to the environment quickly. In addition, it has the advantages of small size and low power consumption. The peripheral hardware equipment has the auxiliary functions of storage, communication, debugging and display. Embedded operating system is used to manage memory allocation, interrupt processing and task scheduling. It can be divided into sequential execution, time-sharing operation and real-time operation.

The traditional image acquisition technology has the disadvantage of slow speed and poor effect, so the new image acquisition must have the characteristics of large storage device capacity, high interactivity and high compression [8]. Embedded image compression technology can reduce the amount of data in the calculation by compression algorithm, and then restore the data through reconstruction algorithm. This can save storage space and improve transmission efficiency. At the same time, there are a lot of redundant information in the image information. Image compression can reduce the redundancy, filter the objective information which is not sensitive, and increase the compression ratio. At present, the common image compression includes lossy compression and lossless compression.

2.1.2. Image edge detection algorithm

Using the characteristics that the gray value or brightness of the edge area changes to a certain extent, and using specific mathematical tools, the pixel points in the image are calculated one by one, and the boundary line of the object image can be searched [9]. Then, in the edge detection algorithm based on the first derivative, Let $f(a,b)$ be the gray information of an image, and the partial derivatives in the horizontal direction and vertical direction are shown in Formula 1 and Formula 2 respectively:

$$f_a(a,b) = \frac{\partial f(a,b)}{\partial a} \quad (1)$$

$$f_b(a,b) = \frac{\partial f(a,b)}{\partial b} \quad (2)$$

The partial derivative of a pixel on the angle ε of the image is shown in Formula 3:

$$f_\varepsilon = f_a(a,b)\cos\varepsilon + f_b(a,b)\sin\varepsilon \quad (3)$$

According to the above formula, the gradient of image can be defined as Formula 4:

$$\nabla f(a,b) = [G_a, G_b]^T = [f_a(a,b), f_b(a,b)]^T \quad (4)$$

Because gradient operators have a variety of sizes and element values, gradient operators with different performance can be used in different situations [10]. Roberts operator uses local forward difference for edge detection, and its calculation formula is shown in Formula 5:

$$G[a,b] = \sqrt{f[a,b] - f[a+1,b+1]^2 + (f[a+1,b] - f[a,b+1])^2} \quad (5)$$

After simplification, it is shown in Formula 6:

$$G[a,b] = |G_a| + |G_b| \quad (6)$$

The matrix expression of Roberts operator is shown in formula 7:

$$G_a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, G_b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad (7)$$

Sobel operator puts the gradient calculation point in the center of the template, which has a certain anti noise ability. The calculation and matrix expression of the gradient amplitude are shown in Formula 8 and Formula 9 respectively:

$$G[a,b] = \sqrt{S_a^2, S_b^2} \quad (8)$$

$$G_a = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}, \quad G_b = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \quad (9)$$

Prewitt operator also realizes edge detection by computing difference and has certain image smoothing ability. The calculation and matrix form of the gradient amplitude are shown in Formula 10 and Formula 11 respectively:

$$G[a,b] = \sqrt{G_a^2 + G_b^2} \quad (10)$$

$$G_a = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix}, \quad G_b = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad (11)$$

Laplacian is a classical second-order differential edge detection operator, which can well highlight the texture details in the image, and has the characteristics of advance and rotation invariance. Its mathematical expression is shown in Formula 12:

$$\nabla^2 f = \frac{\partial^2 f}{\partial a^2} + \frac{\partial^2 f}{\partial b^2} \quad (12)$$

Gaussian Laplacian operator is the optimization of Laplacian operator. Before using Laplacian operator, the image is smoothed by Gaussian filtering, which can enhance the detection effect and anti noise ability. The Gaussian function $G(a,b)$ is shown in Formula 13:

$$G(a,b) = \frac{1}{2\pi\varpi} \exp\left(-\frac{1}{2\pi\varpi}(a^2 + b^2)\right) \quad (13)$$

Where ϖ is the standard deviation of the Gaussian function. After smoothing, Laplace operator is used for edge detection. The detection formula is as follows:

$$g(a,b) = f(a,b) * G(a,b) \quad (14)$$

$$h(a,b) = \nabla^2(f(a,b) * G(a,b)) \quad (15)$$

$$h(a,b) = f(a,b) * \nabla^2 G(a,b) \quad (16)$$

2.1.3. Evaluation criteria of edge detection performance

The basic requirements of edge detection include: it must be able to detect the real edge of the image correctly; the positioning accuracy of the edge must reach a certain standard; the detected edge width cannot be too wide; and it must have certain anti-noise performance. These requirements cannot be met at the same time, some of the performance is good, others will be poor. Therefore, the evaluation

of image detection performance needs to be carried out from both subjective and objective aspects.

Subjective evaluation depends on human eyes to judge the quality of edge extraction, and the main indicators of observation include continuity, smoothness, width and positioning accuracy [11]. Objective evaluation standard evaluates the performance of edge detection in quantitative form, avoiding the influence of subjective factors on the evaluation results. The performance indicators of objective evaluation include signal-to-noise ratio, edge positioning accuracy and unilateral response distance [12]. If the impulse response of the edge detection filter is $h(x)$, the edge function is $b(x)$, and the edge occurs at $x=0$, then the noise in the image is $z(x)$ and its variance is z_0^2 . The mathematical expressions of the above three performance indicators are as follows:

$$SNR = \frac{\left| \int_{-\infty}^{+\infty} b(-x)h(x)dx \right|}{z_0 \sqrt{\int_{-\infty}^{+\infty} h^2(x)dx}} \quad (17)$$

$$L = \frac{\left| \int_{-\infty}^{+\infty} b'(x)h'(x)dx \right|}{z_0 \sqrt{\int_{-\infty}^{+\infty} h'^2(x)dx}} \quad (18)$$

$$M = \pi \sqrt{\frac{\int_{-\infty}^{+\infty} h'^2(x)dx}{\int_{-\infty}^{+\infty} h''^2(x)dx}} \quad (19)$$

2.2. Digital watermarking technology

2.2.1. Classification of digital watermarking

Digital watermarking can effectively maintain the security of digital products, and its basic framework includes watermark embedding, extraction and detection [13]. Digital watermarking can be divided into visible watermark and invisible watermark according to people's subjective feeling. Digital watermarking can be divided into robust watermarking and fragile watermarking according to the characteristics of watermarking. Robust watermarking can withstand conventional image processing operations, and fragile watermarking is very sensitive to signal changes.

Digital watermarking can be divided into space domain watermark and change domain watermark according to the embedding domain of watermark. The change domain watermark can resist certain image attacks and ensure the imperceptibility of watermark, which is the development trend of digital watermarking [14]. According to the detection process, digital watermarking can be divided into blind detection and non blind detection, public key and private key watermarking. According to the type of original carrier, it can be divided into still image, audio, video, software and document watermark.

2.2.2. Related technologies and attack methods of digital watermarking

Modern information hiding technology can effectively hide the existence of secret information by embedding image, sound, video, text and other information into the host information, without causing people's doubt and attention. Information hiding technology is the same as cryptography technology to prevent malicious attacks and protect the integrity of information technology. The form of information hiding changes with the emergence of digital media. Various information can be embedded into all kinds of digital media information.

Image encryption technology can make digital watermarking algorithm have better effect and security. The image scrambling operation is carried out on the digital image, and the pixel points are disturbed by the characteristics of the image point array [15]. The core of image encryption technology is to control the intensity of encryption and the difficulty of decryption. These operations can randomize the watermark signal. Without weakening the correlation between signal pixels, the watermark signal has stronger anti attack ability.

The attack methods of digital watermark will threaten its security. Several common attack methods include embedding one's own watermark into others' products or embedding others' watermark into their own products without authorization, detecting or even extracting watermarks without authorization, removing digital watermarks from products without authorization, and attacks from systems and laws [16].

2.2.3. Performance evaluation of digital watermarking

When evaluating the performance of digital watermarking, watermark robustness is an important evaluation index. Watermark with good robustness can withstand various conventional attacks, and the robustness of watermark is affected by many factors. The watermark should be embedded in the high information area of the image, and the intensity coefficient and data volume should be well controlled. The original size and type of image also affect the invisibility and robustness of the watermark. The robustness of the watermarking algorithm is inversely proportional to the watermark information and the number of embedding [17]. The stronger the watermark is embedded, the more robust it is, but the invisibility of watermark will be sacrificed. In addition, the addition of secret key information can enhance the robustness of the watermark without affecting its performance.

The invisibility of digital watermarking can be evaluated by subjective testing and quantitative testing. The subjective test is judged by the naked eye, the distorted images are arranged in order, and the invisible degree of watermark is described after observation. This method is easy to be affected by the subjective factors of observers, and can not accurately analyze the performance.

The measurement indicators of quantitative test methods include signal-to-noise ratio, peak signal-to-noise ratio, mean square error and mean absolute difference, etc., which can be used to measure the differential distortion [18].

2.3. Watermark copyright protection algorithm

2.3.1. Zero watermarking algorithm for documents

Document zero watermarking technology does not modify any data in the original document,

which can effectively avoid the problem of excessive dependence on the original document format and destruction of the original expression, and improve the robustness of the watermark. Document zero watermarking algorithms can be divided into two categories based on Chinese character features and those based on word and sentence features [19].

The zero watermarking algorithm based on Chinese character features records the required text in the document according to its order of occurrence, and uses it as the key. This kind of algorithm depends on the appearing order of words, which is easy to change, so it can not solve the problem of robustness to delete, add and tamper attacks at the same time.

The zero watermarking algorithm based on the features of words and sentences can not solve the problem of robustness to delete, add and tamper attacks at the same time, but the algorithm is based on the classification and recognition of words and sentences. By calculating and selecting the entropy of words or sentences, selecting key words or key sentences, zero watermark is embedded in them.

2.3.2. Digital watermarking algorithm in spatial domain and transform domain

Bit plane replacement algorithm is one of the common spatial domain algorithms. It uses 8-bit binary to represent a pixel in gray-scale image, and the least significant one is defined as the last bit [20]. Then watermark information is used to replace the last bit to realize information hiding and reduce distortion. The algorithm has the advantages of simple operation and poor robustness. The patching method is also one of the common spatial domain algorithms. Based on the statistical characteristics, it selects multiple pairs of pixels in the carrier to adjust their relative brightness values [21]. The algorithm has high robustness, but its capacity is very small, so it is difficult to calculate.

The transform domain algorithm can distribute watermark evenly in the carrier, so as to improve the transparency and robustness. At present, the commonly used transform domain watermarking algorithms include Fourier transform (DFT), discrete cosine transforms (DCT) and discrete wavelet transform (DWT) [22,23].

DFT domain algorithm is based on the translation invariance and scaling of Fourier transform, which can better resist geometric attacks. DCT transform domain algorithm can change the watermark all over the whole image, which has strong robustness, but the local characteristics are poor, and may appear distortion. DWT transform domain algorithm has the characteristics of multi-resolution, which can better show the local characteristics, and can also spread the local distortion to the whole image, so it has better global characteristics.

2.3.3. JPEG image copyright protection algorithm

Still image compression standard (JPEG) images are widely used in various fields, and the authentication of its authenticity and integrity also depends on digital watermarking algorithm [24]. JPEG only supports the data processing of brightness signal and color difference signal, so these signals need to be divided into blocks, and then the image data is transformed and compressed by quantizing DCT coefficients. Only after entropy coding can JPEG images be generated.

JPEG image watermarking algorithm adjusts the strength of local hidden watermark according to HVS, and embeds watermark under the premise of invisibility. The frequency masking, brightness masking and edge masking of HVD can be reasonably utilized to improve the invisibility and robustness of the watermark [25].

JPEG image watermarking algorithm needs to preprocess the watermark information to ensure its insensitivity and security, and then embed the watermark into the image. The watermark information can be extracted after pseudo-random reverse scrambling. The standard of normalized similarity is used to determine whether there is watermark information in JPEG image, and the watermark is detected.

3. Experiments on construction of zero watermark copyright protection algorithm based on embedded intelligent edge computing detection

3.1. Design of embedded intelligent edge detection module based on Sobel operator

This paper designs an embedded intelligent edge detection module based on Sobel operator. Its sub modules include image line buffer module, convolution calculation module and threshold processing module. The system framework is as follows.

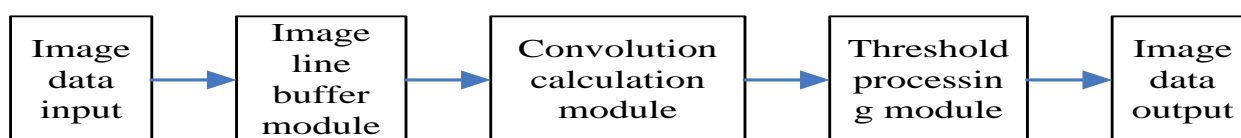


Figure 1. Embedded intelligent edge detection module.

As shown in Figure 1, the input serial image data is buffered and converted into 3 lines of parallel image data to form an image matrix of 3×3 pixels. Then, Sobel's horizontal and vertical operators are used to calculate the horizontal gradient and vertical gradient through the convolution calculation module. The combination of discrete D flip-flop, multiplier and adder is used to realize the convolution operation. After combining the horizontal gradient with the vertical gradient, the edge detection image can be obtained by threshold processing.

3.2. Design of zero watermark copyright protection algorithm based on embedded intelligent edge detection

3.2.1. Preprocessing of zero watermark

Before embedding the watermark into the image, it is necessary to preprocess the watermark. In this paper, Arnold transform of image scrambling technology is used to preprocess the watermark, and all pixels of the image are transformed to rearrange the pixel position of the image. When the image is attacked, the loss can be spread to the whole image by anti scrambling, and the robustness of the watermarking algorithm is also improved.

3.2.2. Zero watermark embedding

When embedding watermark, the invisibility and robustness of watermark should be considered, and the embedding position and method should be selected properly. In this paper, the watermark

embedding operation is as follows: firstly, the image is transformed, and then the Zig-Zag scanning transmitter is used to select the intermediate frequency coefficient as the watermark embedding position. The zero watermark is transformed by Arnold transform, and the scrambling watermark image is embedded in the position determined in the previous step. The watermark image can be obtained by inverse transformation of the modified image.

3.2.3. Algorithm robustness attack test and performance evaluation

The robustness of the proposed zero watermark copyright protection algorithm, DFT transform domain algorithm, DCT transform domain algorithm and JPEG image copyright protection algorithm based on embedded intelligent edge detection module are tested respectively. The detection rate and signal-to-noise ratio of each algorithm are calculated.

The image quality of the proposed zero watermark copyright protection algorithm based on embedded intelligent edge detection module is evaluated subjectively and objectively. The quality level of subjective evaluation is divided into five levels. The image quality of 1–5 grades increases in turn. The higher the level, the better the image quality. The objective evaluation indexes include signal-to-noise ratio, peak signal-to-noise ratio, mean square error and mean absolute difference.

4. Discussion on the performance of the algorithm

4.1. Detection rate of watermark protection algorithm under different attacks

4.1.1. Algorithm performance under image clipping attack

This paper proposes a zero watermark copyright protection algorithm based on embedded intelligent edge detection module, hereinafter referred to as TPA, DFT transform domain algorithm, DCT transform domain algorithm and JPEG image copyright protection algorithm. The performance of these four algorithms under different clipping ratio is compared. The clipping attack experiment is carried out with two pictures, P1 and P2.

Table 1. Algorithm detection rate in clipping attack.

Cut Scale		5%	10%	15%	20%	25%
P1	TPA	0.89	0.89	0.87	0.85	0.80
	DFT	0.58	0.55	0.50	0.42	0.25
	DCT	0.76	0.71	0.63	0.53	0.46
	JPEG	0.75	0.74	0.68	0.60	0.55
P2	TPA	0.87	0.85	0.84	0.81	0.75
	DFT	0.59	0.52	0.42	0.31	0.19
	DCT	0.75	0.73	0.65	0.54	0.50
	JPEG	0.71	0.64	0.55	0.43	0.32

As shown in Table 1, the detection rates of the four algorithms are different when the clipping ratio is different, and the detection rate decreases with the increase of the clipping ratio. The same algorithm will have different detection rate in different images. Among them, the detection rate of this

algorithm is the highest when P1 image is trimmed by 5% and 10%, which is 0.89. When P1 image and P2 image are subjected to different proportion of clipping attacks, the detection rate of the four algorithms changes as follows.

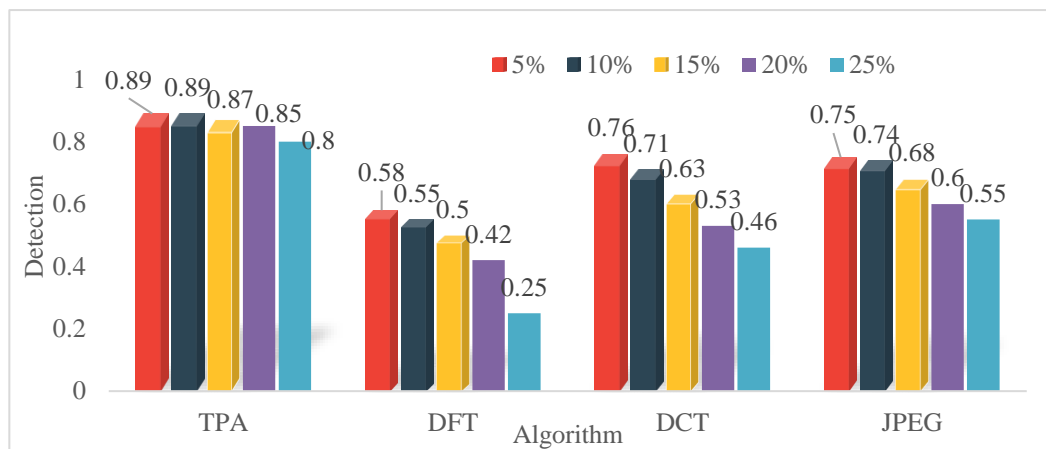


Figure 2. Algorithm detection rate change in P1 clipping attack experiment.

As shown in Figure 2, in the experiment of P1 image clipping attack, the algorithm in this paper has the best detection rate. The average detection rate of all clipping ratios is 0.86, followed by JPEG image copyright protection algorithm, with the average detection rate of 0.664. The lowest average detection rate is DFT transform domain algorithm, which is 0.46.

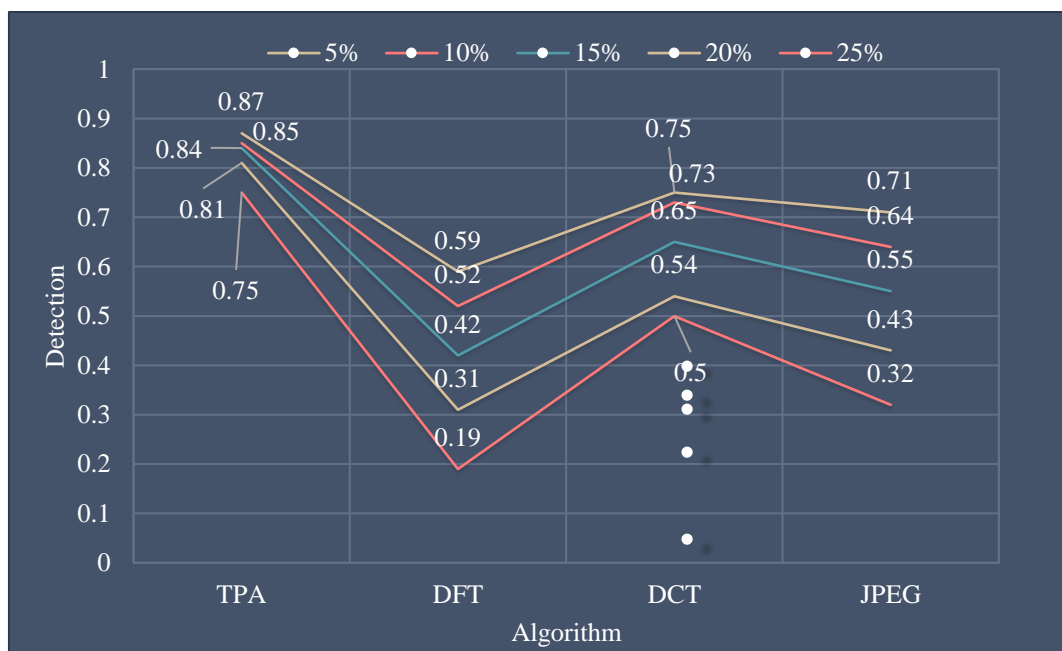


Figure 3. Algorithm detection rate change in P2 clipping attack experiment.

As shown in Figure 3, in P2 images, the algorithm in this paper has the best detection rate, with an average detection rate of 0.824, followed by the DCT transform domain algorithm, with an

average detection rate of 0.634. The lowest average detection rate is DFT transform domain algorithm, which is 0.406. This shows that the performance of the proposed algorithm is better than the other three algorithms when dealing with the clipping attack.

4.1.2. Algorithm performance under image scaling attack

The performance of the four algorithms in image scaling attack under different scaling ratio is compared. In the scaling attack experiment, three images are used, which are P3, P4 and P5.

Table 2. Algorithm detection rate in scaling attack.

Scaling scale		0.6	0.8	1.2	1.4
P3	TPA	0.41	0.49	0.37	0.31
	DFT	0.48	0.51	0.49	0.45
	DCT	0.18	0.39	0.31	0.30
	JPEG	0.15	0.27	0.15	0.14
P4	TPA	0.45	0.62	0.51	0.38
	DFT	0.49	0.52	0.45	0.39
	DCT	0.27	0.25	0.35	0.26
	JPEG	0.11	0.14	0.22	0.12
P5	TPA	0.39	0.54	0.57	0.55
	DFT	0.48	0.57	0.61	0.45
	DCT	0.16	0.32	0.33	0.16
	JPEG	0.10	0.14	0.18	0.13

As shown in Table 2, the detection rates of the four algorithms are different when the scaling ratio is different. If the scaling ratio is too large or too small, the detection rate will be reduced. The same algorithm will have different detection rate in different images. Among them, DFT transform domain algorithm has the highest detection rate of 0.61 when P5 image is magnified 1.2 times. When P3 image is attacked by different scale scaling, the detection rate of the four algorithms changes as follows.

As shown in Figure 4, in P3 images, the DFT transform domain algorithm with the best detection rate has an average detection rate of 0.483, followed by the algorithm in this paper, with an average detection rate of 0.395. The lowest average detection rate is JPEG image copyright protection algorithm, which is 0.178.

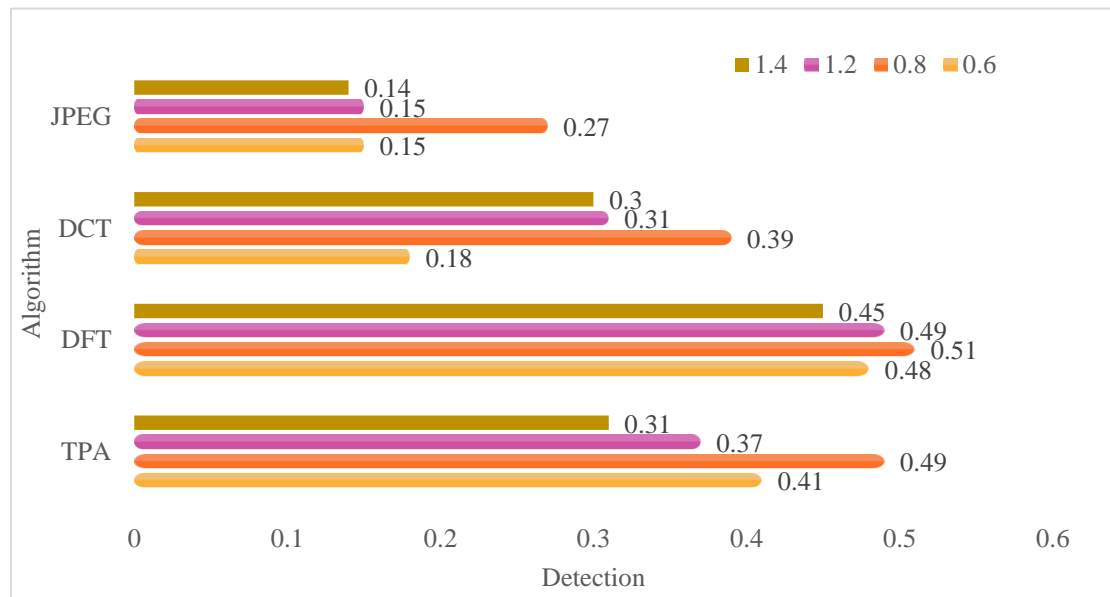


Figure 4. Change of detection rate in P3 scaling attack experiment.

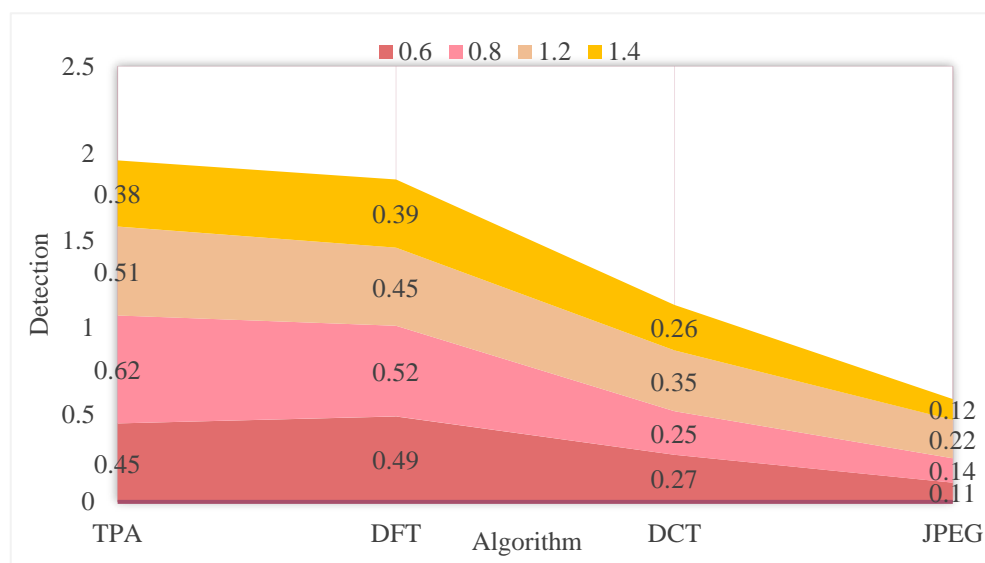


Figure 5. The change of detection rate in P4 scaling attack experiment.

As shown in Figure 5, in P4 images, the algorithm in this paper with the best detection rate has an average detection rate of 0.49, followed by the DFT transform domain algorithm, with an average detection rate of 0.463. The lowest average detection rate is JPEG image copyright protection algorithm, which is 0.148.

As shown in Figure 6, in P5 images, the DFT transform domain algorithm with the best detection rate has an average detection rate of 0.528, followed by the algorithm in this paper, with an average detection rate of 0.513. The lowest average detection rate is JPEG image copyright protection algorithm, which is 0.138. This shows that the performance of the proposed algorithm is slightly lower than that of the DFT transform domain algorithm when dealing with scaling attacks, but it is better

than the other two algorithms.

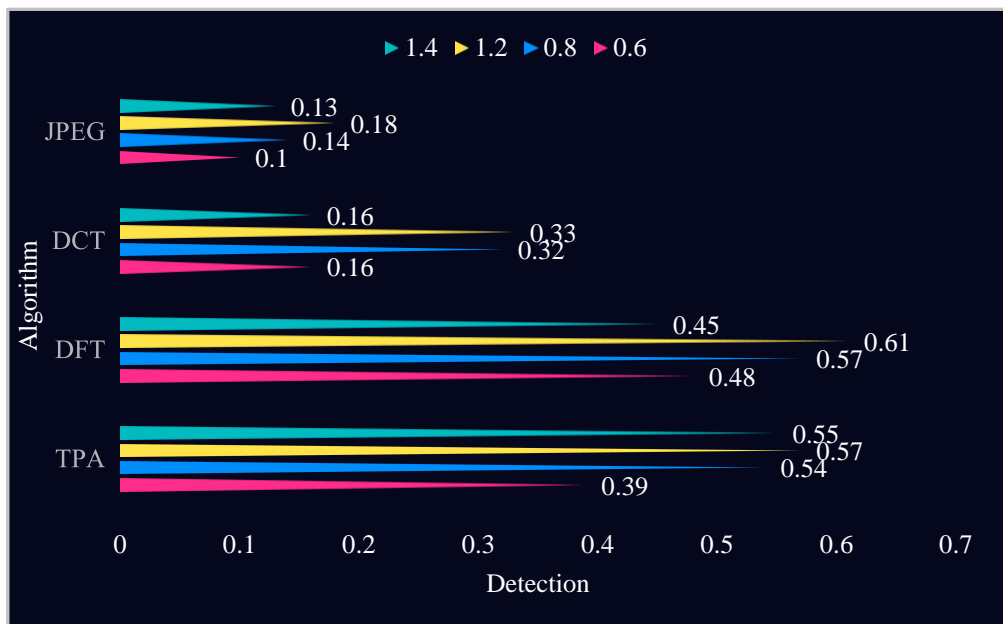


Figure 6. The change of detection rate in P5 scaling attack experiment.

As shown in Table 3, the algorithms under different noise attacks have different SNR, and the SNR of all algorithms under multiplicative noise is the highest. The highest signal to noise ratio (SNR) is 36.854% in P6 multiplicative noise attack. When P6 and P7 are attacked by different noises, the change trend of SNR is as follows:

Table 3. SNR of algorithm in noise attack.

Noise type	Multiplicative noise	Gaussian noise	Pepper noise	Gaussian random distribution 5%	Uniform distribution 5%	
P6	TPA	36.854	32.892	25.827	31.485	33.805
	DFT	21.458	18.515	18.750	19.482	20.725
	DCT	19.706	18.071	15.613	17.523	16.246
	JPEG	29.715	28.074	25.168	26.460	27.255
P7	TPA	38.487	31.325	22.884	29.381	30.712
	DFT	20.591	18.052	17.242	19.931	23.119
	DCT	22.753	19.373	16.665	20.584	21.310
	JPEG	30.716	32.644	20.351	33.413	28.312

4.2. SNR of watermark protection algorithm under different attacks

4.2.1. Algorithm SNR under noise attack

The signal-to-noise ratio (SNR) of the above four algorithms under noise attack is tested. The noise attacks are divided into five types: multiplicative noise, Gaussian noise, salt and pepper noise, Gaussian random distribution 5% and uniform distribution 5%. The noise attack experiment was

carried out with two pictures, P6 and P7. The results are as follows.

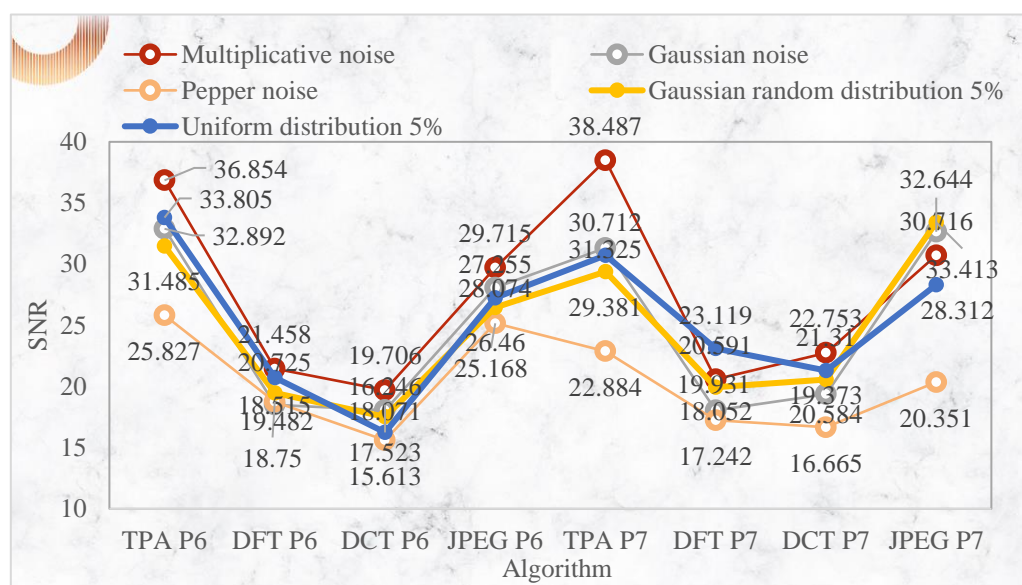


Figure 7. SNR variation in noise attack experiment.

As shown in Figure 7, in the noise attack experiment, the algorithm in this paper has the highest SNR. The average SNR of two images is 32.173% and 30.558%. The DCT transform domain algorithm has the lowest average detection rate, and the average SNR of P6 is 17.432%. This shows that the proposed algorithm can still maintain a high SNR and its robustness is high.

4.2.2. Algorithm SNR under sharpening and fuzzy attacks

The SNR of the above four algorithms under sharpening and fuzzy attacks is tested. Sharpening attack is divided into sharpening, further sharpening and sharpening edge, and fuzzy attack is divided into fuzzy and Gaussian blur. Sharpening attack and blurring attack are not carried out at the same time, but they are carried out with the same two pictures with the numbers of P8 and P9 respectively.

Table 4. SNR of algorithms in sharpening and blurring attacks.

Attack method	Sharpening	Sharpen more	Sharpen edges	Blur	Gaussian blur	
P8	TPA	35.646	28.851	39.638	41.285	33.835
	DFT	18.418	18.055	17.506	22.469	21.759
	DCT	22.366	20.031	17.693	23.253	22.291
	JPEG	25.245	23.032	27.166	26.840	24.215
P9	TPA	34.987	31.382	37.864	35.321	32.733
	DFT	21.511	19.052	20.243	19.931	18.149
	DCT	19.753	14.394	19.631	21.524	18.310
	JPEG	28.716	25.634	20.377	30.413	27.382

As shown in Table 4, the algorithm under different types of sharpening and fuzzy attacks has different signal-to-noise ratio, among which the highest is the signal-to-noise ratio of this algorithm in

the sharpening edge attack and fuzzy attack of P8, which are 39.638% and 41.285%, respectively. When P8 and P9 are attacked by different noises, the change trend of SNR is as follows:

As shown in Figure 8, in the sharpening attack experiment, the algorithm in this paper has the highest signal-to-noise ratio, and the average signal-to-noise ratio of the two images are 34.712% and 34.744%, respectively. In the experiment of fuzzy attack, the algorithm in this paper has the highest SNR, and the average SNR of two images is 37.56% and 34.027%, respectively. This shows that the proposed algorithm can still maintain high SNR and high robustness when dealing with different types of sharpening and fuzzy attacks.

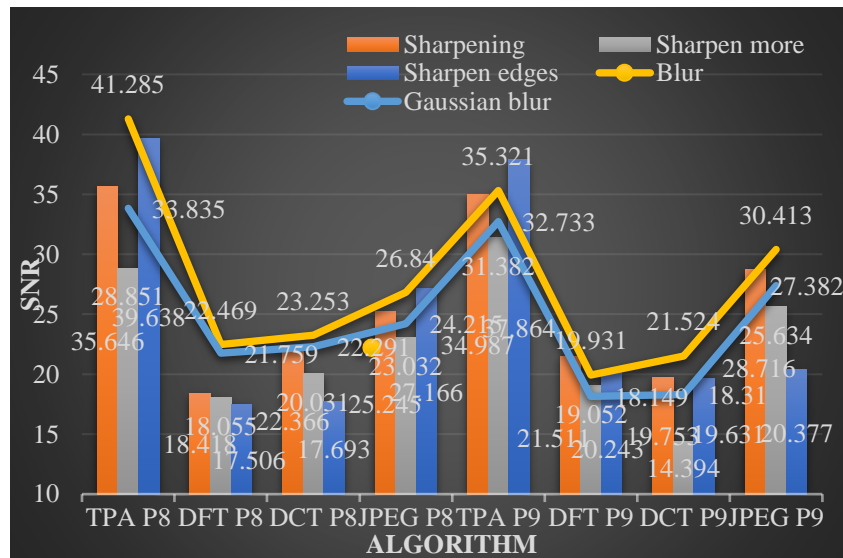


Figure 8. SNR variation in sharpening and blurring attack experiments.

4.3. Evaluation of image quality

4.3.1. Subjective evaluation of image quality

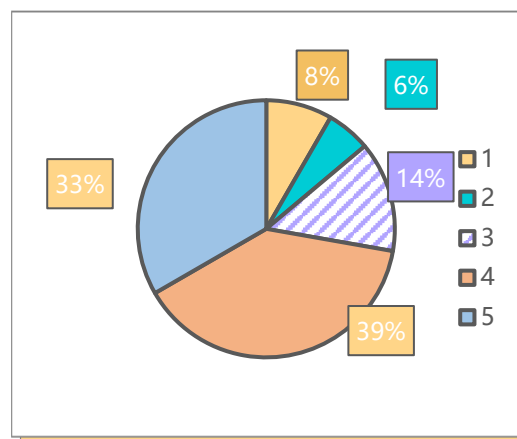


Figure 9. Subjective evaluation of image quality of the algorithm in this paper.

The quality of 36 images processed by this algorithm was evaluated by observers.

As shown in Figure 9, the subjective evaluation of 33% and 39% of the 36 images processed by the algorithm in this paper is level 5 and level 4, which indicates that the image processed by this algorithm has high quality.

4.3.2. Objective evaluation of image quality

The four objective evaluation indexes mentioned in the second chapter, namely SNR, PSNR, MSE and mean absolute difference, are used to evaluate the seven images processed by the algorithm.

As shown in Figure 10, the seven images processed by the algorithm in this paper have high performance in the four objective evaluation indexes: signal to noise ratio, peak signal-to-noise ratio, mean square error and average absolute difference. The mean values of SNR, PSNR, MSE and mean absolute difference of 7 images were 20.56, 25.13, 37.03 and 27.64, respectively.

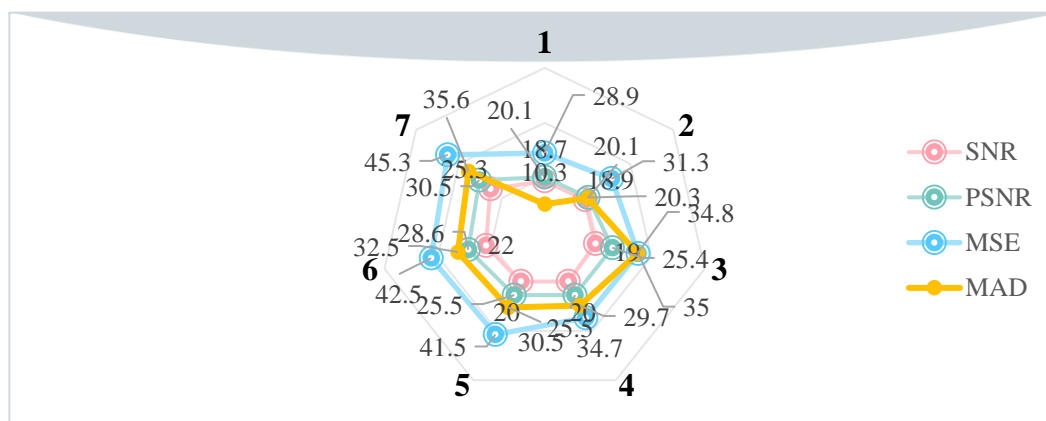


Figure 10. Objective evaluation of image quality of this algorithm.

5. Conclusions

Embedded image compression technology can reduce the amount of data in the calculation by compression algorithm, and then restore the data through reconstruction algorithm. This can save storage space and improve transmission efficiency. At the same time, there are a lot of redundant information in the image information. Image compression can reduce the redundancy, filter the objective information which is not sensitive, and increase the compression ratio. This paper designs an embedded intelligent edge detection module based on Sobel operator. Its sub modules include image line buffer module, convolution calculation module and threshold processing module, which can be used for image edge detection.

When evaluating the performance of digital watermarking, watermark robustness is an important evaluation index. Watermark with good robustness can withstand all kinds of conventional attacks. Therefore, in this paper, the zero watermark copyright protection algorithm based on embedded intelligent edge detection module is tested by cutting, scaling, sharpening and fuzzy attacks. It is concluded that the algorithm in this paper has better robustness against conventional attacks. The image processed by the algorithm presented good quality in both subjective and objective evaluation.

Therefore, this algorithm can well realize the copyright protection of digital media works.

Although the algorithm in this paper has a certain anti attack performance, but its related research is still in the primary stage, there are some deficiencies. In the zero watermarking algorithm, it is necessary to further optimize the embedding position and method of watermark, so as to improve the robustness of the algorithm against scaling attack. At the same time, the digital media has rich formats. The algorithm in this paper only focuses on the image format, which is far from enough. In the future research work, it is necessary to further study the transformation of watermark between various digital media formats.

Conflict of interest

There is no potential competing interest in our paper.

References

1. Q. Zhu, Digital watermarking technology based on relational database, *J. Interdiscip. Math.*, **21** (2018), 1211–1215.
2. Nasr addin Ahmed Salem Al-maweri, R. Ali, W. A. W. Adnan, A. R. Ramli, S. M. S. Ahmad, State-of-the-Art in Techniques of Text Digital Watermarking: Challenges and Limitations, *J. Comput. Sci.*, **12** (2016), 62–80.
3. C. Wang, X. Wang, Z. Xia, C. Zhang, Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm, *Inf. Sci.*, **470** (2019), 109–120.
4. Z. Xia, X. Wang, B. Han, Q. Li, T. Zhao, Color image triple zero-watermarking using decimal-order polar harmonic transforms and chaotic system, *Signal Process.*, **180** (2021), 107864.
5. X. Zhang, Z. Shen, Copyright protection method for 3D model of geological body based on digital watermarking technology, *J. Visual Commun. Image Representation*, **59** (2019), 334–346.
6. X. H. Wang, D. H. Wei, X. X. Liu, X. C. Ma, Digital watermarking technique of color image based on color QR code, *J. Optoelectron. Laser*, **27** (2016), 1094–1100.
7. X. Yang, W. Dai, G. Tang, L. Min, Deriving Ephemeral Gullies from VHR Image in Loess Hilly Areas through Directional Edge Detection, *ISPRS Int. J. Geo Inf.*, **6** (2017), 371–371.
8. H. Dadgostar, F. Afsari. Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB, *Inf. Secur. Tech. Rep.*, **30** (2016), 94–104.
9. R. Thankachan, R. Sethunadh, P. Ameer. Edge Detection in Polarimetric SAR Image based on Bandelet Transform, *Int. J. Comput. Appl.*, **181** (2019), 33–38.
10. P. M. Shakeel, S. Baskar, R. Sampath, M. M. Jaber, Echocardiography image segmentation using feed forward artificial neural network (FFANN) with fuzzy multi-scale edge detection (FMED), *Int. J. Signal Imaging Syst. Eng.*, **11** (2019), 270–270.
11. J. Jumanto. An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection, *Cybernetics Inf. Technol.*, **18** (2018), 74–88.
12. D. Nagarajan, M. Lathamaheswari, R. Sujatha, J. Kavikumar, Edge Detection on DICOM Image using Triangular Norms in Type-2 Fuzzy, *Int. J. Adv. Comput. Sci. Appl.*, **9** (2018), 462–275.
13. Y. Zhang, X. L. Ma. Research on image digital watermarking optimization algorithm under virtual reality technology, *Discrete Contin. Dyn. Syst.*, **12** (2019), 1427–1440.

14. H. Tan, P. Tang, C. Zhang, Digital Watermarking for Color Images Based on Compressive Sensing, *Nanoence Nanotechnol. Lett.*, **9** (2017), 724–729.
15. A. Q. M. Sabri, A. M. Mansoor, U. H. Obaidellah, E. R. M. Faizal, J. L. PC, Metadata hiding for UAV video based on digital watermarking in DWT transform, *Multimedia Tools Appl.*, **76** (2017), 16239–16261.
16. C. L. Song, L. Yang, X. Wang. Secure and Robust Digital Watermarking: A Survey, *J. Electron. Sci. Technol.*, **14** (2016), 57–68.
17. Nasr addin Ahmed Salem Al-maweri, R. Ali, W. A. W. Adnan, A. R. Ramli, S. M. S. Ahmad, State-of-the-Art in Techniques of Text Digital Watermarking: Challenges and Limitations, *J. Comput. Sci.*, **12** (2016), 62–80.
18. Z. Ling, Anti-tampering technology of digital watermarking in dynamic web page images, *Agro Food Ind. Hi Tech*, **28** (2017), 2195–2199.
19. Y. Zhang, C. Wang, X. Wang, W. Min, Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection, *Future Internet*, **9** (2017), 1–13.
20. C. Chongtham, M. S. Khumanthem, Y. J. Chanu, N. Arambam, D. Meitei, P. R. Chanu, et al., A Copyright Protection Scheme for Videos Based on the SIFT, *Iran. J. Sci. Technol., Trans. Electr. Eng.*, **42** (2018), 107–121.
21. Z. Xia, X. Wang, X. Li, C. Wang, S. Unar, M. Wang, et al., Efficient copyright protection for three CT images based on quaternion polar harmonic Fourier moments, *Signal Process.*, **164** (2019), 368–379.
22. X. W. Li, S. T. Kim, Q. H. Wang, Copyright protection for elemental image array by hypercomplex Fourier transform and an adaptive texturized holographic algorithm, *Opt. Express*, **25** (2017), 17076–17098.
23. R. Mancha, Adaptive Image Watermarking Scheme Using Fuzzy Entropy and GA-ELM Hybridization in DCT Domain for Copyright Protection. *J. Signal Process. Syst.*, **84** (2016), 265–281.
24. A. Lakshmi Priya, S. Letitia, Copyright Protection for Digital Colour Images Using Dual Watermarking Technique by Applying Improved DWT, DCT and SVD, *J. Electr. Electron. Eng.*, **4** (2016), 120–130.
25. A. E. Afify, A. Emran, A. Yahya, A Tamper Proofing Text Watermarking Shift Algorithm for Copyright Protection, *Arab J. Nuclear Sci. Appl.*, **52** (2019), 126–133.



AIMS Press

©2021 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>)