Visual Image Digital Watermarking Embedding Algorithm Combining 3D Boolean CNN and Arnold Technology

Cun Shang, Ying Xue, Wen Xiang Liu, and Yang Liu

***Abstract*—As digital technology has been leaping forward over the past few years, its application in watermarking has become widespread. To enhance the effectiveness of this technology, a novel digital watermarking embedding algorithm based on a 3D Boolean cellular neural network and cat face transformation is proposed in this study. The proposed algorithm is capable of preprocessing the image using cat face transformation and then encrypting it using a three-dimensional (3D) Boolean cellular neural network for the confidentiality of the digital watermark confidentiality. As indicated by the performance comparison experiment, the information entropy and the correlation coefficient of adjacent pixels are better at 7.9993 and 0.0009. The result suggests that Algorithm 4 exhibits strong robustness. Subsequently, in the empirical analysis, the result reveals that the maximum signal-to-noise ratios of R, G, and B in the HSI color space watermark images reach 76.6621, 80.6228, and 77.4841, all at a high level. The above results suggest that this algorithm exhibits good encryption performance. Accordingly, applying this algorithm to the field of visual images can facilitate the development of color image-level authentication and copyright identification.**

***Index Terms*—CNN, Arnold technology, Visual images, Digital watermarking, Embedding algorithm**

I. INTRODUCTION

Digital watermarking technology (DWT) is capable of embedding specific information into multimedia data to achieve copyright protection and digital content protection [1]. The watermark should be hidden, such that it cannot be detected and removed and that the watermark is robust [2]. In the field of visual images, DWT has been introduced in copyright protection and digital content security. However, early digital watermarking techniques have largely embedded grayscale images in carrier images [3-4]. Its disadvantage is that the embedded image hinders our understanding of color. Thus, finding a digital watermark embedding algorithm for color images is of great practical significance [5]. The Arnold transform is a nonlinear mapping that is one of the most common strategies for position scrambling of two-dimensional (2D) matrices [6]. Cellular Neural Network (CNN) is analog signal processing with local interconnections and dual output. It is capable of boasting continuous real-time operation, high-speed parallel computing, and suitability for VLSI implementation. Its application has penetrated a considerable number of fields (e.g., pattern recognition, image processing, global optimization) [7]. Based on the Cellular Automata Theory, this type of ANN makes it possible for the neighboring units of the network to interact with each other. Each unit or "cell" is a non-linear dynamic system [8]. A visual image digital watermark embedding algorithm based on 3D Boolean CNN and Arnold transform is proposed to more effectively protect the security of copyright information and digital content. This study aims at providing certain reference and reference values for DWT application in visual images. The main contributions are presented as follows. The first point is that the original visual image falls into 8×8 grids. DWT and coefficient quantization processing are performed on the respective grid. The second point is to extract the brightness component I from the visual image based on the HSI color space, and then perform DWT processing. The third point is integrating 3D Boolean CNN with Arnold technology to improve its security. A variety of parts of the research are presented as follows. In Section 1, the relevant research on Arnold technology, CNN algorithm, and digital watermark embedding algorithm is mainly introduced. In the second section, the digital watermark embedding algorithm that integrates 3D CNN and Arnold technology is mainly explained. In the third section, the comparative and empirical results of the fusion algorithm are described in detail. Lastly, in Section 4, the conclusion of this study is drawn.

II. RELATED WORKS

With the gradual advance of CNN, its optimized methods have been introduced in multiple fields. To facilitate the current electronic nose detection of volatile components in citrus, Cao's team proposed an image feature extraction model based on an optimized CNN method. Empirical analysis has been conducted on the model. As indicated by the results, the model exhibits favorable feature extraction ability, such that the detection accuracy of the electronic nose can be increased [9]. Ji et al. proposed an optimized

Manuscript received November 30, 2021; revised August 21, 2023.

This work was supported in part by the Xinyang Agriculture and Forestry University under Project for Core Teacher Training Plan and Academic Backbone Plan under Grant 20210005, Xinyang Key Research and Promotion Special under Grant 20220046, Teaching Reform Research Project under Grant 2021XJGLX41, Philosophy and Social Science Planning Project in Henan Province (No.2022BYS038)

Cun Shang is a professor of the College of Planning and Design Xinyang Agriculture and Forestry University and a postdoctoral of Wuhan University of Technology, Wuhan, 430000 China. (e-mail: 2006230019@xyafu.edu.cn).

Ying Xue is an assistant professor of the College of Planning and Design, Xinyang Agriculture and Forestry University, Xinyang, 464000 China. (e-mail: 2020230006@xyafu.edu.cn).

Wen Xiang Liu is an assistant professor of the College of Forestry, Xinyang Agriculture and Forestry University, Xinyang, 464000 China. (e-mail: 2020290002@xyafu.edu.cn).

Yang Liu is an associate professor of the College of Planning and Design, Xinyang Agriculture and Forestry University, Xinyang, 464000 China.(Correspondence Author, phone: 8618203761792; e-mail: leadnat@163.com).

CNN by local binary constraints to tackle the issue of difficulty in recognizing image textures and constructed a texture feature extraction model based on it. As indicated by the result of performance testing of this method, its accuracy in recognizing image textures is 96.7%, superior to the comparison algorithm and has practicality [10]. Moreover, the application range of Arnold's transformation technology was also becoming wider and wider. For better security of the physical layer and the transmission function of the system, Bi's team proposed an encryption method following the chaotic Arnold transform and chaotic linear frequency modulation matrix technology. Empirical analysis was conducted on this method, and the results suggested that this method exhibits higher sensitivity and security [11]. Qu et al. addressed the issue of poor performance of the encryption methods for optical color images using pixel imaging and Arnold transform. Performance testing of this encryption method revealed that it is feasible and robust against certain types of attacks [12].

With the widespread application of color images, a wide variety of methods have been incorporated into digital watermark embedding schemes. Xu et al. proposed a novel blind color image watermark leveraging the tensor domain. The above-mentioned method can effectively account for the holistic features of color images and disperses watermark information across the red, green, and blue channels through tensor decomposition by incorporating a multi-dimensional perspective [13]. Byun et al. calculated the DCT coefficient at a specific position using discrete cosine transform(DCT). The full frame DCT was unnecessary as the watermark bit could be embedded by directly adjusting the pixel value, which ensured robustness and low computational complexity [14]. Makbol et al. presented a novel and dependable image watermarking method by SVD and integer wavelet transform. The vital innovation of the proposed method lies in the s and v matrices, where s was incorporated into the singular value of the host image. To bolster security, supplementary secret keys were acquired from the watermark image while embedding[15]. Hamidi et al. [16] introduced a robust and blind watermark for safeguarding digital image copyrights. Its security was reinforced by subjecting the watermark to Arnold transform before embedding. Its innovation lay in ensuring improved robustness by the size of discrete Fourier transform (DFT) coefficients.

The above-described research has fully confirmed that the CNN algorithm and Arnold transform technology have been applied in numerous fields, and multiple methods are currently applied in digital watermark embedding schemes. However, CNN and Arnold transform technology in digital watermark embedding have been rarely investigated. To fill this gap, their fusion is studied and applied to digital watermarking embedding. Hopefully, this method is capable of providing certain reference values for DWT applications in visual images [17].

III. A Digital Watermark Embedding Algorithm Integrating 3D CNN and Arnold Technology

To improve the security and accuracy of the digital watermark embedded algorithm of color images and protect the copyright of information and digital content, a digital watermark embedded algorithm is developed based on Arnold technology. Moreover, based on 3D Boolean CNN, a digital watermark embedded algorithm of 3D CNN and Arnold technology is developed.

A. Digital Watermark Embedding Algorithm by Arnold Technology

At present, most color images are expressed by RGB color space. Nevertheless, compared with RGB, the color described by HSI (brightness) is more intuitive and natural for humans [18]. The HSI color space describes color features through three parameters: H, S, and I, where H defines hue; S represents saturation; I represents intensity. Accordingly, H, S, and I can be used to combine and describe the color features of color images [19]. Due to the separation of H, S, and I parameters, the HSI color space has significant advantages in visual image segmentation [20]. Arnold Transform technique, i.e., an algorithm employed for image processing, is capable of rotating, scaling, and deforming an image. The technique conforms to the theory of a nonlinear dynamic system, and the image is transformed by iterating the image pixels. To be specific, Arnold transforms can rearrange the pixels of an image in accordance with certain rules, with the aim of achieving the rotation, scaling, and deformation of the image. Arnold transform technology has been extensively used in image encryption, image compression, image feature extraction, and so forth. It is capable of encrypting the image, such that the original image can be recovered only with the corresponding decryption key. Accordingly, its application in digital watermark embedding can significantly improve the security and transparency of watermark embedding. Fig. 1 presents the flow chart of the digital watermark embedding algorithm based on Arnold technology.

Fig.1 demonstrates that traditional visual images are typically represented in RGB color space. The researchers first convert the image from RGB to HSI to embed the watermark and back to RGB after embedding. Before embedding, the color image should be preprocessed. The original visual image is defined as K, with a size of $M \times N_{24}$, and the watermark is defined as WR, with a size of $\frac{M}{8} \times \frac{N}{8}$. When the preparation is made for embedding, the watermark image is preprocessed to achieve binary sequence conversion through Arnold transform. The position of image pixels varies with the variation of the pixel coordinates for process safety. The definition of the Arnold transform is presented as follows. Assuming that there is a point on a cell per unit area, the point (x, y) undergoes Arnold transformation to another point (x', y'), the transformation equation is shown in Equation (1).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod M \tag{1}$$

In Equation (1), (x, y) is the original pixel coordinate, (x', y') represents that of the converted new image, and M is the matrix order. After Arnold's transformation, the correlation between the pixel space and the original visual image is eliminated, and the digital watermark information security is improved. The results are shown in Fig. 1. After transformation, the watermark energy is evenly distributed. As a result, the extracted watermark remains str-

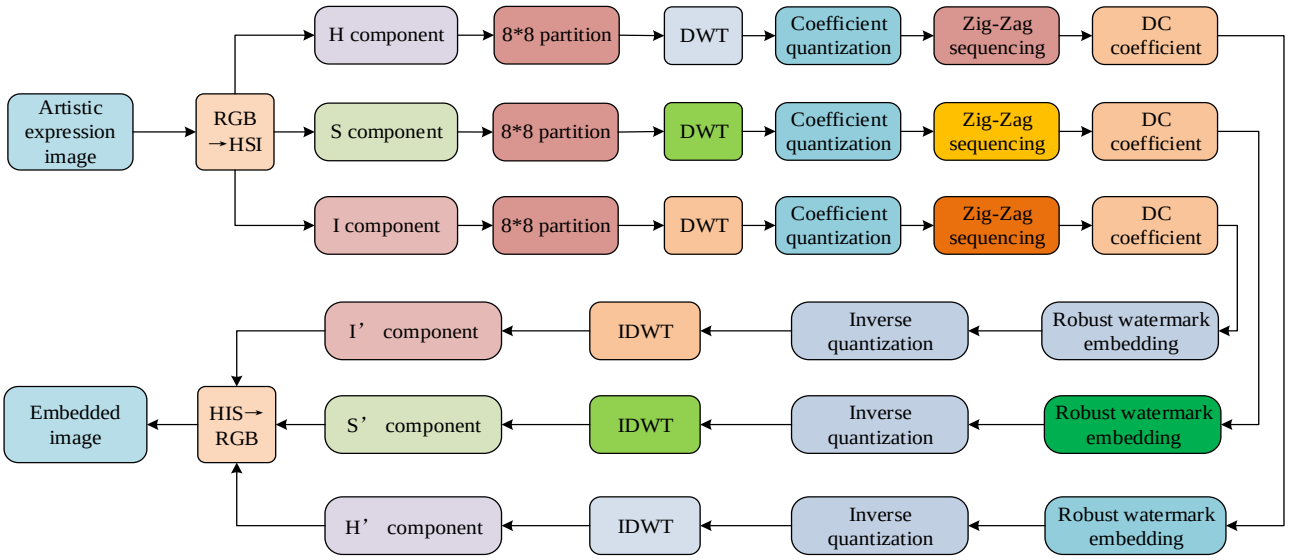


Fig. 1. Arnold Digital Watermark Embedding Algorithm Flowchart

ucturally intact when the host image is attacked. After completing the watermark preprocessing operation, color space conversion is performed from RGB to HSI on the watermark. The HSI color space transformation can fall into cylinder transformation, single hexagonal cone transformation, sphere transformation, or triangle transformation. Cylindrical transformations are employed in this study. The calculation equation for cylinder transformation is shown in Equation (2).

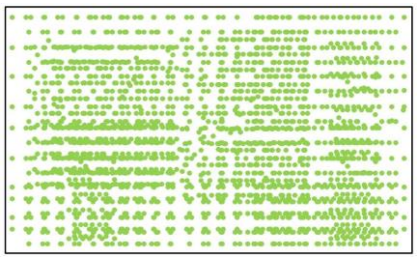
$$\begin{cases} I = \dfrac{1}{\sqrt{3}}(R+G+B), \\ S = 1 - \dfrac{\sqrt{3}}{I}\min(R,G,B) \\ H = \begin{cases} \theta, when\ G \geq B \\ 2\pi - \theta, when\ G < B \end{cases} \\ \theta = \cos^{-1}\left[\dfrac{\frac{1}{2}\left[(R-G)+(R-B)\right]}{\sqrt{(R-G)^2+(R-B)(G-B)}} \right] \end{cases} \tag{2}$$

Equation (2), I represents the brightness component, H and S represent the color difference component. Using Equation (2), the original image is conversed from RGB to HSI, and the conversion results are shown in Fig. 2.

In image color space transformation, regardless of whether the color image is 24-bit or 16-bit, the values of parameters H, I, and S parameters in the identical pixel are the same. Thus, the research on the conversion of images from RGB to HSI can effectively resist color depth conversion attacks. After the spatial color conversion of the image is completed, the extraction of the brightness component I is investigated. The principle of brightness segmentation I extraction is determined by image segmentation, and the expression for image segmentation is written in Equation (3).

$$f_k^I(x,y)(x,y=1,2,\ldots 8,k=1,2,\ldots\frac{M}{8}) \tag{3}$$

(a) Watermark before conversion



(b) Converted watermark

Fig. 2. Arnold Color Space Transformation Effect

In Equation (3), $f_k^I(x,y)$ represents partitioning; I represents the brightness component of the parameter, $\frac{M}{8}$ represents the image grid 8×8's length. In the flowchart, after image segmentation, DCT transformation and quantization processing are performed on the image segmentation. The processing equation is shown in Equation (4).

$$B_k^I(u,v) = \left[\frac{F_k^I(u,v)}{B \times Q(u,v)} = 0.5 \right](u,v=1,2,\ldots 8) \tag{4}$$

In Equation (4), u and v represent the grid lengths in the horizontal and vertical directions, respectively $F_k^I(u,v)$ represents the quantization coefficient, B is the quantization factor, $B_k^I(u,v)$ denotes the DWT coefficient, $Q(u,v)$

represents the numerical value in the standard quantization equation. Subsequently, a herringbone scan sequencing is performed, and the quantified DWT coefficients in the respective grid are sorted according to the herringbone scan order. At this point, the quantified DWT coefficients in all grids are defined, as expressed in Equation (5).

$$C_k^I(i)(i=1,2,\ldots,64) \tag{5}$$

To embed watermarks into visual images, the research first selects the DC coefficients to be embedded. The selection equation is shown in Equation (6).

$$C_k^{I'}(1)=C_k^I(1)+aWR_k \tag{6}$$

In Equation (6), WR_k represents the watermark information of the grid, $C_k^I(1)$ is the DC coefficient embedded in the grid, a represents the embedding strength. Subsequently, the watermark information is subjected to inverse quantization, and the inverse transformation calculation is shown in Equation (7).

$$\begin{cases} when 0^\circ \le H < 120^\circ, \\ \quad R=\dfrac{1}{\sqrt{3}}\left[1+\dfrac{S\cos(H)}{\cos(60^\circ-H)}\right], \\ \quad B=\dfrac{I}{\sqrt{3}}(1-S), G=\sqrt{3}I-R-B \\ when 120^\circ \le H < 240^\circ, \\ \quad G=\dfrac{1}{\sqrt{3}}\left[1+\dfrac{S\cos(H-120^\circ)}{\cos(180^\circ-H)}\right], \\ \quad B=\dfrac{I}{\sqrt{3}}(1-S), B=\sqrt{3}I-R-G \\ when 240^\circ \le H < 360^\circ, \\ \quad B=\dfrac{1}{\sqrt{3}}\left[1+\dfrac{S\cos(H-240^\circ)}{\cos(300^\circ-H)}\right], \\ \quad B=\dfrac{I}{\sqrt{3}}(1-S), R=\sqrt{3}I-B-G \end{cases} \tag{7}$$

To verify the scheme's effectiveness, different embedding factors are employed, and the normalized signal-to-noise ratio (NSNR) of the respective alpha channel serves as the test result data. On that basis, the normalized mean square error of the image is shown in Equation (8).

$$NSNR=\begin{cases} \dfrac{\sum_{m=0}^{H-1}\sum_{n=0}^{N-1}\left\{\phi\left[x(m,n)-y(m,n)\right]\right\}^2}{\sum_{m=0}^{H-1}\sum_{n=0}^{N-1}\left\{\phi\left[x(m,n)\right]\right\}^2} \\ -10\log(NMSE) \end{cases} \tag{8}$$

In Equation (8), $x(m,n)$ denotes the original image, $y(m,n)$ is the reconstructed image, H represents the height, N expresses the width, $\phi[\cdot]$ represents an arithmetic unit.

B. A Digital Watermark Embedding Algorithm Combining 3D CNN Model

Although the Arnold technology-based digital watermarking embedding algorithm exhibits high nondestructive, security, and robustness, it still has some disadvantages (e.g., high computational complexity and limited embedding capacity). The cellular neural network algorithm is integrated into the algorithm to enhance the performance of the proposed digital watermark embedding algorithm. Cellular Neural Network (CNN) is a type of nonlinear simulation dynamic system with structural regularity and infinitely expandable dimensions. In general, its dynamic characteristics comprise chaos, periodicity, almost periodicity, and stability, among which stability turns out to be prominent in the application of cellular neural network dynamic characteristics [21]. CNN cells are a locally interconnected, dual-valued output signal nonlinear simulation processor with continuous real-time, high-speed parallel computing capabilities, and suitability for implementation in markedly large-scale integrated circuits [22]. Its application scope has infiltrated numerous fields (e.g., pattern recognition, image processing, and global optimization) [23]. The CNN unit circuit diagram of the CNN unit is shown below [24].

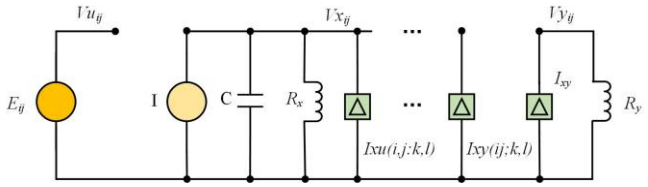


Fig. 3. CNN Unit Circuit Diagram

In Fig. 3, u_{ij} represents external input information, x_{ij} represents the state cell variable, y_{ij} represents the output result. CNN comprises multiple neural network units, as expressed in Fig. 3. cell $C(i,j)$ is only connected to its neighboring cell $C'(k,l)$. Their connection points are voltage-controlled current sources I_{xu} and I_{xy}. In the process of determining whether two cells are adjacent, it is necessary to use neighborhood N_r, and the expression of neighborhood N_r is shown in Equation (9).

$$N_r=\left\{C_{ij}:\max(|k-i|),|l-j|\le 1<k<N,1<l<M\right\} \tag{9}$$

The state expression of $C(i,j)$ can be obtained from Equation (9), as written in Equation (10).

$$C\frac{dx_{ij}}{dt}=\frac{1}{R_x}x_{ij}+\sum_{Ci,j\in Nr(i,j)}A(i,j;k,l)y_{kl}+\sum_{Ci,j\in N_r(i,j)}B(i,j;k,l)u_{kl}+I \tag{10}$$

Equation (10) is simplified to obtain the simplified state expression, as expressed in Equation (11).

$$\frac{dx_{ij}}{dt} = -x_j + a_j f(x_j) + G_0 + G_s + I_j \tag{11}$$

In Equation (11), a_j denotes a constant, $f(x_j)$ represents the output information of cells, G_0 expresses that of connected cells, and G_s denotes a linear combination of connected cell state variables, I_j is the threshold value. To improve cellular neural networks, a novel chaotic cellular neural network is constructed based on symbolic functions, and its dimensionless state equation is shown in Equation (12).

$$f(x_j) = \frac{1}{2}(|x_j + 1| - |x_j - 1|) \tag{12}$$

In Equation (12), $f(x_j)$ represents the information of the output cell x_j. Research into the construction of the 3D Boolean CNN network based on cellular neural networks, with the design scheme shown in Fig. 4.

In Fig. 4, the 3D Boolean CNN network first generates a chaotic sequence through the CNN network while selecting an encryption algorithm key through the chaotic sequence. Subsequently, it encrypts the image using the key and the plaintext signal. The decryption process of images is generating an identical chaotic sequence using the identical CNN network and obtains the decryption key according to the identical rules to decrypt the image. Their flowcharts are presented in Fig. 5.

In Fig. 5, the 3D Boolean CNN network encryption module includes two layers of the encryption process. First, the encryption key is pre-iterated to improve its sensitivity, and after preprocessing, the key is the initial value for the first convolution to determine the CNN convolution kernel of the first layer. Subsequently, the image processed by Arnold's digital watermark embedding algorithm is iterated to generate eight convolutional matrices, which are combined with the input image to build a CNN input matrix.

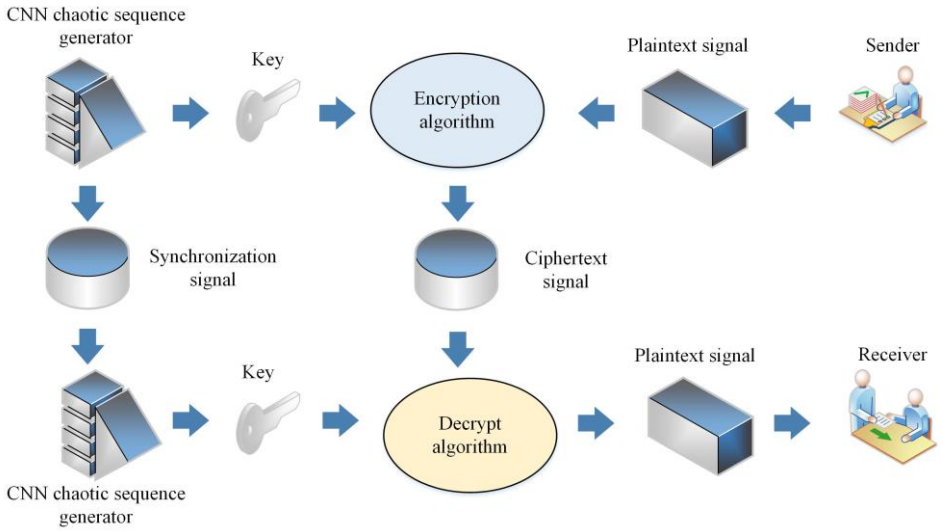
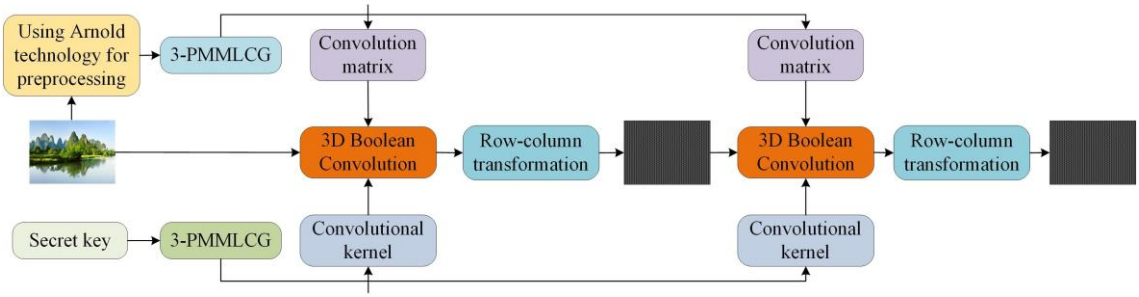
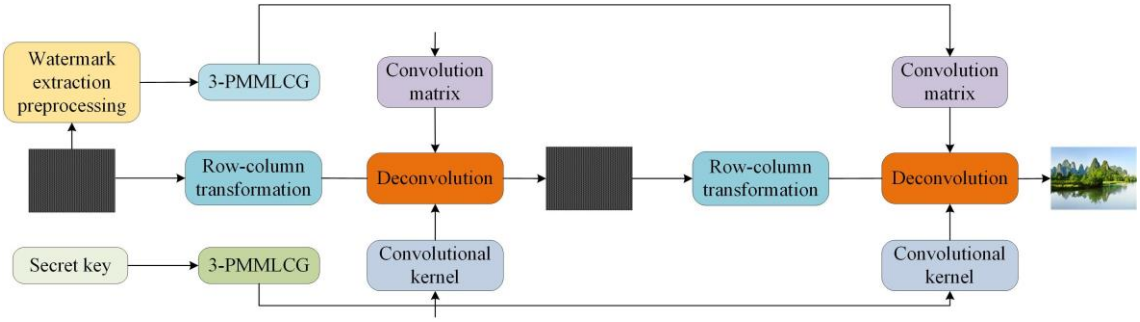


Fig. 4. Design Scheme of 3D Boolean CNN Network



(a) Encryption flowchart



(b) Encryption flowchart

Fig. 5. Encryption and decryption process of 3D Boolean CNN

The input image, input matrix, and convolutional kernel are input into the 3D Boolean convolution, and row-column transformation is performed on them. The second layer encryption process is initiated, comprising inputting the convolutional matrix and kernel of the first layer into a 3D Boolean convolution, performing row and column changes on it, and finally outputting the image data after the row and column changes to obtain the image encryption result. As depicted in Fig. 4, the decryption module of the 3D Boolean CNN network acts as the inverse process of the encryption module. A hybrid digital image embedding algorithm can be obtained by combining 3D Boolean CNN and Arnold technology, which can effectively improve its security. To compare the performance of the hybrid digital image embedding algorithm, information entropy and adjacent pixel correlation serve as the evaluation indicators. In an image, information entropy is capable of indicating the chaos of its pixels. The information entropy of the image is expressed in Equation (13).

$$H(x)=\sum_{i=0}^{2^N-1} p(x_i)\frac{1}{\log_2 p(x_i)} \tag{13}$$

In Equation (13), x_i denotes the grayscale value of the image; $p(x_i)$ is x_i 's proportion in the image, 2^N represents the grayscale level. When 2^N is 2^8, the image confusion reaches its maximum, and its encryption performance is optimal. Cryptographic images' attack resistance is inversely proportional to the correlation between adjacent pixels, as expressed in Equation (14).

$$r=\frac{\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))}{\sqrt{D(x)D(y)}} \tag{14}$$

In Equation (14), x and y denote pixel values, $D(x)$ represents the number of pixel points, $E(x)$ and $E(y)$ express the average value of x and y, $D(x)$ and $D(y)$ denote the variance of x and y, r represents the correlation coefficient, and the closer r is to 1, the higher the correlation between adjacent pixels, the closer it is to 0, the lower the correlation will be.

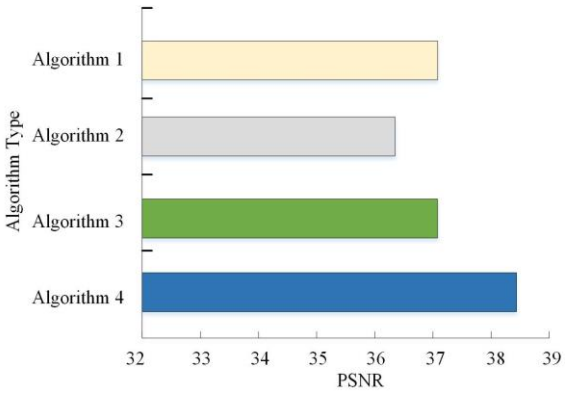
IV. Comparative Results and Empirical Analysis of Fusion Algorithms

To analyze the effectiveness of the algorithms, performance comparison experiments will be conducted on image encryption algorithms through chaos encryption, optical encryption, and frequency encryption, termed algorithm 1, 2, and 3. The proposed hybrid algorithm is termed Algorithm 4. The basic settings of the experimental environment settings are illustrated in Table I.

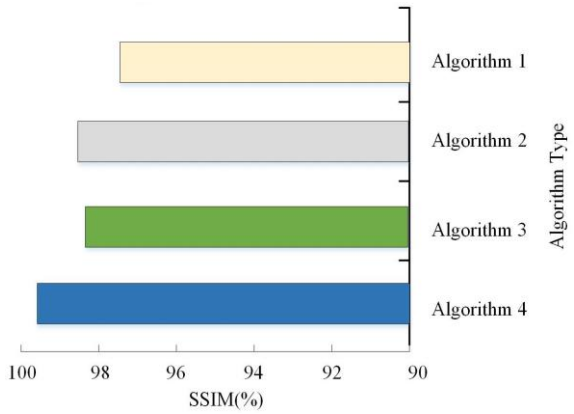
In this study, ImageNet is selected as the dataset for this experiment, containing 14197122 images. The performance of the four algorithms is compared with information entropy and the correlation coefficient of adjacent pixels as evaluation indicators, and the four algorithms are applied to different types of image recognition. The comparison results are presented in Fig 6.

TABLE I
The Experimental Basic Environmental Parameters

Parameter variables	Parameter selection
Operating system	Windows10
Operating environment	MATLAB R2019a
PC side memory	16G
CPU main frequency	1.10GHz
Global procurement unit	RTX-2070
Central Processing Unit	i7-10710
Data storage	ImageNet



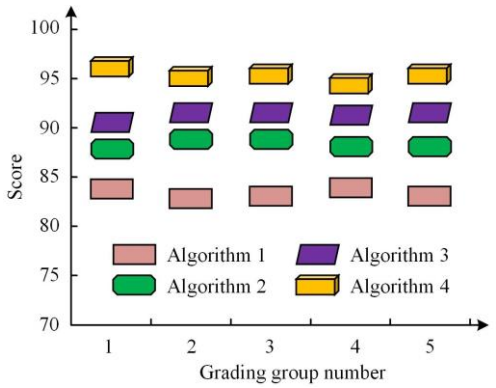
(a) Comparison of PSNR values for different watermarks



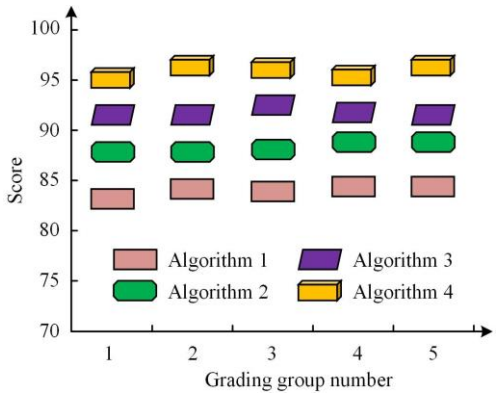
(b) Comparison of PSNR values for different watermarks

Fig. 6. Information entropy comparison

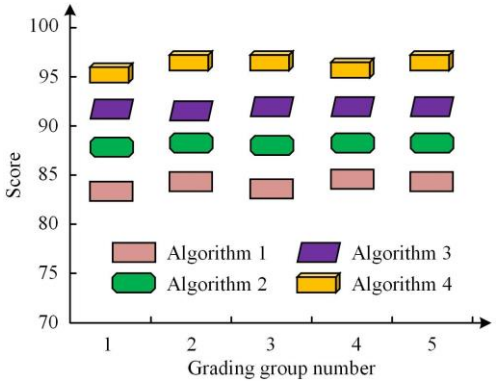
Fig. 6 (a) presents the comparison of the first five image types. The information entropy spread of Algorithm 4 is notably higher, and its average information entropy in the first five image types is 7.9993, higher than 7.9998 of Algorithm 1, 7.9973 of Algorithm 2, and 7.997 of Algorithm 3. Fig. 6 (b) illustrates the comparison of the last five image types. Besides, the information entropy scatter of Algorithm 4 is markedly higher than that of the other three algorithms, its average information entropy in the last five types of images is 7.9994, higher than 7.9967 of Algorithm 1, 7.9972 of Algorithm 2, and 7.9973 of Algorithm 3. In the experiment of this study, the optimal information entropy is 8. Thus, the algorithm's performance is considered superior when the resulting information entropy approaches 8. In brief, Algorithm 4 outperforms similar comparison algorithms. Relevant professionals have been selected to score the running speed, security, and resource consumption indicators of the four algorithms, and the score comparison results are shown in Fig. 7.



(a) Running speed score



(b) Security score



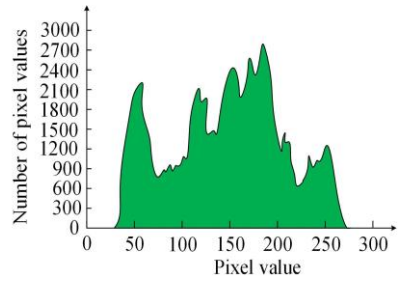
(c) Resource consumption score

Fig. 7. Score results of running speed, security, and resource consumption indexes of the four algorithms

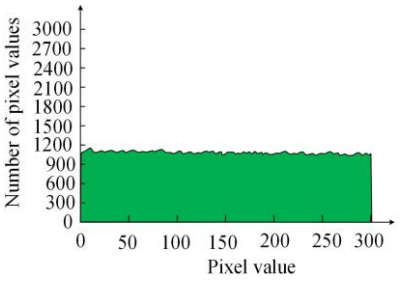
As depicted in Fig. 7 (a), the running speed scores of the four algorithms all exceed 80 points, and the average score of Algorithm 4 is the maximum among the four algorithms, with 95.3 points, higher than the 90.7 points of Algorithm 3, 87.9 points of Algorithm 2 and 84.1 points of Algorithm 1. As depicted in Fig. 7 (b), the security scores of the four algorithms all exceed 83 points, and the average score of Algorithm 4 is the maximum among the four algorithms, with 95.1 points, which is higher than the 91.2 points for Algorithm 3, 88.1 points of Algorithm 2 and 83.9 points of Algorithm 1. As depicted in Fig. 7 (c), the resource consumption scores of the four algorithms all exceed 84 points, and the average score of Algorithm 4 is the maximum among the four algorithms, with 94.8 points, higher than the 91.5 points of Algorithm 3, 88.2 points of Algorithm 2 and 84.6 points of Algorithm 1. As indicated by the above results, the proposed algorithm exhibits high performance in the dimensions of running speed, security, and resource consumption, and its performance is better than that of similar algorithms. Furthermore, cryptographic images are more susceptible to attack when neighboring pixels display a significant correlation [25]. Accordingly, to examine the performance of the four algorithms, different types of images processed by the four algorithms and 4000 pairs of adjacent pixel points are randomly selected for analysis. The correlation coefficient results of adjacent pixels under different algorithms are illustrated as follows.

TABLE II
ADJACENT PIXEL CORRELATION COEFFICIENTS FOR DIFFERENT ENCRYPTION SCHEMES

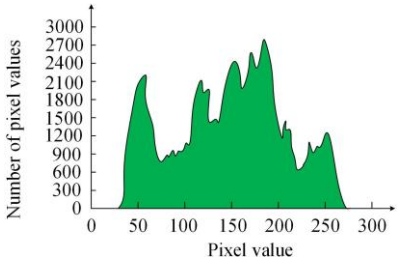
Image type	Man	Puppy	Kitty	Worker	Forest	Lakes	House	Tree
Plaintext	0.9708	0.9798	0.9806	0.9863	0.9725	0.9687	0.9637	0.9817
Algorithm 1	0.0053	0.0058	0.0057	0.0049	0.0063	0.0047	0.0055	0.0046
Algorithm 2	0.0044	0.0042	0.0048	0.0047	0.0045	0.0038	0.0037	0.0045
Algorithm 3	0.0039	0.0047	0.0053	0.0049	0.0045	0.0051	0.0038	0.0041
Algorithm 4	0.0024	0.0031	0.0024	0.0035	0.0015	0.0021	0.0032	0.0009



(a) Plaintext image



(b) Ciphertext image



(c) Decrypting images

Fig. 8. Clear text, ciphertext, and decryption histograms before and after processing with Algorithm 4

As depicted in Table II, the correlation coefficients in the original plaintext image exceed 0.96, and those in the processed image are below 0.007. the above-mentioned result suggests that the images processed by the four

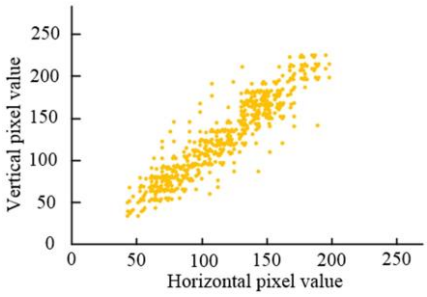
algorithms can effectively resist external attacks. Vertically, the correlation coefficients in the images processed by the four algorithms can reach the minimum for all types of images processed by Algorithm 4. And its neighboring pixel correlation coefficient in tree-like images reaches its minimum, at 0.0009, lower than 0.0046 in Algorithm 1, 0.0045 in Algorithm 2, and 0.0041 in Algorithm 3. As revealed by the above results, from the perspective of the correlation coefficient dimension, Algorithm 4 exhibits better performance in resisting attacks compared with the comparative algorithm. To verify its real effectiveness, a comparative analysis was then carried out using histograms of plaintext, ciphertext, and decrypted images, as well as specific distribution maps of adjacent pixels in plaintext and ciphertext images. Furthermore, an image is randomly selected from the ImageNet dataset, and the plaintext, ciphertext, and decryption histograms before and after processing with Algorithm 4 are presented in Fig. 8.

Fig. 8 (a) is the histogram of the plaintext image, Fig. 8 (b) is the histogram of the ciphertext image, and Fig. 8 (c) presents the histogram of the decrypted image. Histograms can visually represent the statistical features of image data. In Fig. 8 (a), the histogram of the plaintext image shows clear statistical features, and its pixel values fluctuate more strongly in the [30-270] range. In Fig. 8 (b), the histogram of the ciphertext image effectively hides statistical features, and its distribution is relatively uniform on the [0300] interval. As depicted in Fig. 8 (c), the statistical features of the histogram of the decrypted image are very similar to those of the plaintext image. From the above results, Algorithm 4 can effectively resist statistical attacks based on image histograms. Fig. 9 presents the specific distribution of Algorithm 4.

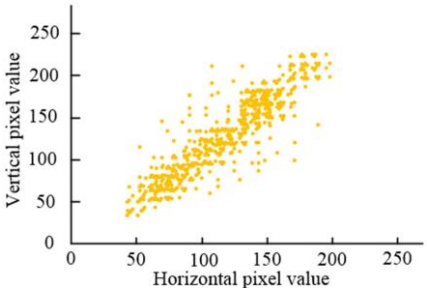
Fig. 9 (a) shows the distribution of adjacent pixels in the plain image in the horizontal direction, and Fig. 9 (b) shows the distribution of adjacent pixels in the vertical direction. From Fig. 9 (a) and (b), the adjacent pixels in the horizontal and vertical directions tend to be linear, with a strong correlation. Fig. 9 (c) shows the distribution of adjacent pixels in the ciphertext image in the horizontal direction, and Fig. 9 (d) shows the distribution of adjacent pixels in the vertical direction. As depicted in Fig. 9 (c) and (d), the adjacent pixels of the ciphertext images in the horizontal and vertical directions fill the whole space and are randomly distributed. As indicated by the above results, the image encrypted by Algorithm 4 exhibits prominent attack resistance. The practical performance of the visual image digital watermark embedding algorithm is investigated following the performance tests on the proposed algorithm. Thus, the algorithm is tested with different embedding factors, and the normalized signal-to-noise ratio (NSNR) of the respective alpha channel serves as the resulting test data. The results are presented below.

TABLE III
EVALUATION OF EMBEDDING RESULTS IN HSI COLOR SPACE

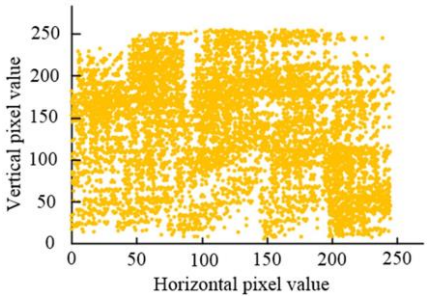
Coefficient (Alpha 1 to Alpha 14)				NSNR(R)	NSNR(G)	NSNR(B)
0.1	0.1	0.1	0.1	76.6621	80.6228	77.4841
0.1	0.1	0.2	0.2	76.1837	80.1752	77.2843
0.2	0.2	0.2	0.2	62.7994	66.5711	63.8854
0.2	0.2	0.3	0.3	62.5971	66.5712	63.6893
0.3	0.3	0.3	0.3	54.6900	58.6507	63.6891
0.3	0.3	0.4	0.4	54.5638	58.5328	55.6534
0.4	0.4	0.4	0.4	48.9362	52.8974	50.0227



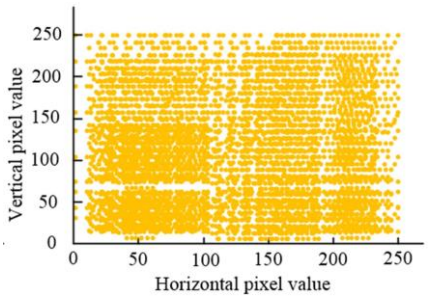
(a) Clear text image horizontal direction



(b) Clear text image vertical direction



(c) Ciphertext image horizontal direction



(d) Vertical direction of ciphertext image

Fig. 9. Specific distribution of adjacent pixels in plaintext and ciphertext images

In Table III, NSNR (R), NSNR (G), and NSNR (B) represent the alpha channel NSNR, corresponding to the NSNR of R, G, and B watermark images in HSI. As depicted in Table III, the maximum signal-to-noise ratios of NSNR (R), NSNR (G), and NSNR (B) are 76.6621, 80.6228, and 77.4841, respectively. This result suggests the favorable practical application effect of the visual image digital watermark embedding algorithm. In addition, the practical embedding and extraction results of the algorithm are compared, which are implemented in MATLAB 2019a. The carrier image is shown in Fig 10.

(a) Watermark

(b) Carrier image

(c) Embedding watermark into carrier image

Fig. 10. Watermark, carrier image, and carrier image after embedding watermark

In Fig. 10, no significant visual change exists after the watermark is embedded in the carrier image, suggesting that the image watermarking embedding algorithm is a good agnostic method. Watermark extraction requires the original and the embedded image. During extraction, two layers of wavelet decomposition are performed, one layer is the original image, and the other layer is the watermark image whose low-frequency coefficients are generated by those of the second layer decomposition of the original image and the digital watermark image, while the high-frequency coefficients are generated by those of the first layer decomposition. Similar to the embedding process, the wavelet coefficients of the original image are subtracted from those of the watermark image. Lastly, an inverse wavelet transform is performed to extract the watermark. The original and the extracted watermark image are depicted as in Fig 11.

The comparison of Fig. 11 (a) and (b) indicates that the extracted watermark image does not show any significant difference, and it has a high resolution. This result shows a good practical application. In brief, the proposed watermark embedding algorithm that integrates the 3D Boolean CNN network and Arnold technology has good performance, such that it can be applied to visual image authentication and copyright recognition. To further analyze the practical application effect of the image watermarking embedding algorithm proposed in this study, 15 images are taken as samples, and the algorithm is adopted to embed watermarking. In the above-mentioned process, the security, robustness, and transparency of the embedding algorithm are evaluated. The full score is 1, the higher the score, the better the performance of the index will be. Table IV lists the actual application results of the proposed watermarking embedding algorithm in 15 images.

(a) Original digital watermark

(b) Extracted digital watermark

Fig. 11. Comparison between the extracted watermark image and the original watermark image

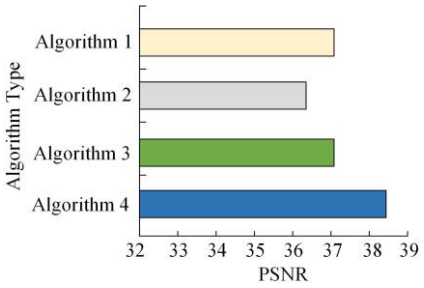
TABLE IV
STUDIES THE ACTUAL APPLICATION RESULTS OF THE PROPOSED IMAGE WATERMARKING EMBEDDING ALGORITHM IN 15 IMAGES

Class No	Security	Robustness	Transparency
1	0.93	0.95	0.94
2	0.92	0.93	0.92
3	0.91	0.94	0.93
4	0.91	0.92	0.92
5	0.93	0.91	0.91
6	0.94	0.94	0.93
7	0.91	0.93	0.92
8	0.92	0.91	0.93
9	0.94	0.93	0.92
10	0.93	0.92	0.91
11	0.91	0.91	0.93
12	0.91	0.95	0.94
13	0.92	0.94	0.93
14	0.92	0.93	0.91
15	0.93	0.93	0.94

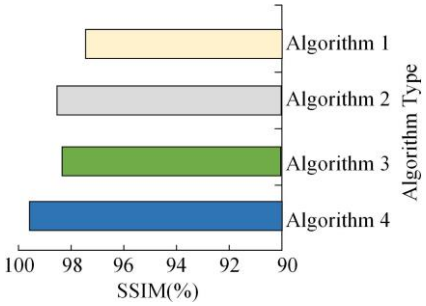
As depicted in Table IV, the security, robustness, and transparency scores of the proposed watermark embedding algorithm all exceed 0.9 points the in practical application of the algorithm, and the maximum score of security is 0.94 points, the maximum score of robustness is 0.95 points, and the maximum score of transparency is 0.94 points in the 15 images. As indicated by the above results, the watermark embedding algorithm proposed in this study has a good effect in practical applications. Then, the image quality of the watermark added by each algorithm is objectively evaluated, and the Peak Signal-to-Noise Ratio (PSNR) and structural similarity (SSIM) is selected as the evaluation index for image comparison, and the encrypted watermark is embedded in the image. The results of the extracted watermark image PSNR and SSIM values of each algorithm are compared and the comparison results are shown in Fig. 12.

Fig. 12 (a) shows the comparison of PSNR values after each algorithm. As shown in Fig. 12 (a), the PSNR value of the images after adding the watermark in the proposed Algorithm 1 is 38.4, which is higher than the other comparison algorithms, indicating that it has more similarity to the image before adding the watermark. Fig. 12 (b) shows the comparison of SSIM values after each algorithm. As shown in Fig. 12 (b), the SSIM value of the pictures

after adding the watermark in Algorithm 1 is 99.2%, which is higher than the other comparison algorithms, indicating that it has more similarity to the pictures before adding the watermark. In summary, the results show that the watermark extraction performance of the proposed Algorithm 1 is higher than other comparison algorithms, which preserves the original watermark image structure while ensuring a certain resolution.



(a) Comparison of PSNR values for different watermarks



(b) Comparison of PSNR values for different watermarks

Fig. 12. PSNR and SSIM results for each algorithm

V. Conclusion

With the rapid advance of information technology, the security of digital watermarks turns out to be increasingly difficult to ensure. To enhance the overall performance of existing digital watermark embedding algorithms, a fusion algorithm is investigated by combining the 3D Boolean CNN algorithm with Arnold transform technology. To be specific, Algorithm 4 is compared with Algorithm 1, Algorithm 2, as well as Algorithm 3. As indicated by the result, the information entropy of Algorithm 4 is 7.9993, higher than 7.9998 of Algorithm 1, 7.9973 of Algorithm 2 and 7.997 of Algorithm 3. The correlation coefficient of adjacent pixels in Algorithm 4 is 0.0009, lower than 0.0046 in Algorithm 1, 0.0045 in Algorithm 2, and 0.0041 in Algorithm 3. The above result suggests that Algorithm 4 exhibits strong robustness. In addition, the practical application effect of the watermark embedding algorithm is also analyzed, and the results suggest that the maximum NSNR (R), NSNR (G), and NSNR (B) of the image processed using the algorithm reach 76.6621, 80.6228, and 77.4841. The above results suggest that the proposed algorithm exhibits better encryption performance and the practical application effect of the visual image digital watermark embedding algorithm is good as well. At present, the applicability of this algorithm is relatively small, and its applicability will be improved in subsequent research.

Reference

[1] Q. L. Liu, S. Q. Yang, J. Liu, P. C. Xiong, and M. C. Zhou, "A discrete wavelet transform and singular value decomposition-based digital video watermark method - ScienceDirect," *Applied Mathematical Modelling*, vol. 85, pp. 273-293, 2020.

[2] Hamilton. J, Danicic. S, "An Evaluation of the Resilience of Static Java Bytecode Watermarks Against Distortive Attacks," *IAENG International Journal of Computer Science*, vol.38, no.1, pp. 1-15, 2011.

[3] Tambo. T, Filtenborg. J, "Digital services governance: IT4IT for management of technology," *Journal of Manufacturing Technology Management*, vol. 30, no. 8, pp. 1230-1249, 2019.

[4] X. H. Chen, J. S. Wang, Y. L. Ruan, and S. Z. Gao, "An Improved Iris Recognition Method Based on Discrete Cosine Transform and Gabor Wavelet Transform Algorithm," *Engineering Letters*, vol. 27, no. 4, pp676-685, 2019.

[5] Cao. Y, Yu. F, and Tang. Y, "A Digital Watermarking Encryption Technique Based on FPGA Cloud Accelerator," *IEEE Access*, vol. 8, pp. 11800-11814, 2020.

[6] Berens. M. J, Hofstetter. T. B, and Bolotin. J, "Arnold W A. Assessment of 2,4-Dinitroanisole Transformation Using Compound-Specific Isotope Analysis after In Situ Chemical Reduction of Iron Oxides," *Environmental Science & Technology: ES&T*, vol. 54, no. 9, pp. 5520-5531, 2020.

[7] Islam. A, Othman. F, Sakib. N, et al, "Prevention of Shoulder-Surfing Attack Using Shifting Condition with the Digraph Substitution Rules," *Artificial Intelligence and Applications*, vol. 1, no. 1, pp. 58-68, 2023.

[8] Juan A. Ramírez-Quintana, Mario I. Chacon-Murguia, and Jose F. Chacon-Hinojos, "Artificial Neural Image Processing Applications: A Survey," *Engineering Letters*, vol. 20, no. 1, pp68-80, 2012.

[9] Cao. H, Jia. P, Xu. D, Jiang. Y, and Qiao. S, "Feature Extraction of Citrus Juice During Storage for Electronic Nose Based on Cellular Neural Network," *IEEE Sensors Journal*, vol. 20, no.7, pp. 3803-3812, 2019.

[10] Ji. L, Chang. M, Shen. Y, and Zhang. Q, "Recurrent convolutions of binary-constraint Cellular Neural Network for texture recognition," *Neurocomputing*, vol. 387,no.28, pp. 161-171, 2020.

[11] Bi. M, Zhuo. X, Yang. G, Hu. M, and Hu. W, "Chaotic Arnold transform and chirp matrix encryption scheme for enhancing the performance and security of OFDM-PON," *Optical Fiber Technology*, vol. 51, pp. 64-70, 2019.

[12] Qu. G, Meng. X, Yin. Y, Wu. H, and He. W, "Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation," *Optics and Lasers in Engineering*, vol. 137, no.20, pp. 1-11, 2021.

[13] Xu. H, Jiang. G, Yu. M, and Luo. T, "A color image watermarking based on tensor analysis," *IEEE Access*, vol. 6, pp. 51500-51514, 2018.

[14] Byun. S.W, Son. H. S, and Lee. S. P, "Fast and robust watermarking method based on DCT specific location," *IEEE Access*, vol. 7, pp. 100706-100718, 2019.

[15] Makbol. N. M, Khoo. B. E, Kassem. T. H, and Loukhaoukha. K, "A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection," *Inf. Sci*, vol. 417, pp. 381–400, 2017.

[16] Hamidi. M, El Haziti. M, Cherifi. H, and El Hassouni. M, "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. Multimedia," *Tools Appl*, vol. 77, pp. 27181-27214, 2018.

[17] Q. Zheng, X. Tian, M. Yang, and H. Wang, "Differential Learning: A Powerful Tool for Interactive Content-Based Image Retrieval," *Engineering Letters*, vol. 27, no. 1, pp. 202-215,2019.

[18] Wang. W, Yao. M, and N. M. K, "Color image multiplicative noise and blur removal by saturation-value total variation," *Applied Mathematical Modelling*, vol. 90, no. 1, pp. 240-264, 2021.

[19] Kamiyama. M, Taguchi. A, "Color Conversion Formula with Saturation Correction from HSI Color Space to RGB Color Space," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. 104, no. 7, pp. 1000-1005, 2021.

[20] Chen. B, Shi. S, Sun. J. Chen, and B.G. W, "Using HSI Color Space to Improve the Multispectral Lidar Classification Error Caused by Measurement Geometry," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 4, pp. 3567-3579, 2020.

[21] Muruganandhan. S. G, Manian. R, "Computational and artificial neural network based study of functional SNPs of human LEPR protein associated with reproductive function," *Journal of Cellular Biochemistry*, vol. 120, no. 4, pp. 18910-18926, 2019.

[22] Cao. H, Jia. P, Xu. D, Jiang. Y, and Qiao. S, "Feature Extraction of Citrus Juice During Storage for Electronic Nose Based on Cellular Neural Network," *IEEE Sensors Journal*, vol. 20, no. 7, pp. 3803-3812, 2019.
[23] Ji. L, Chang. M, Shen. Y, and Zhang. Q, "Recurrent convolutions of binary-constraint Cellular Neural Network for texture recognition," *Neurocomputing*, vol. 387, no.28, pp. 161-171, 2020.
[24] Chen. D. D, Lin. Y. C, and Wu. F, "A design framework for optimizing forming processing parameters based on matrix cellular automaton and neural network-based model predictive control methods," *Applied Mathematical Modelling*, vol. 76, pp. 918-937, 2019.
[25] Andrea. R, Galli. M, Bianchi. M, Parisi. E, and Wang. H. L, "Clinical outcomes of short implants (≤6 mm) placed between two adjacent teeth/implants or in the most distal position: A systematic review and meta-analysis," *European Journal of Oral Implantology*, vol. 14, no.3, pp. 241-257, 2021.