Medical Image Watermarking Based on Visual Secret Sharing and Cellular Automata Transform for Copyright Protection

Tzuo-Yau Fan[1], Her-Chang Chao[2*], and Bin-Chang Chieu[1]
[1]Department of Electronic and Computer Engineering, National Taiwan University of Science and Technology, Taipei, 10607, Taiwan, R.O.C.
[2]Department of Computer Science and Information Engineering, Ming Chuan University, Taoyuan, 33348, Taiwan
[e-mail: yaufan0625@gmail.com, herchang@mail.mcu.edu.tw, chu@mail.ntust.edu.tw]
*Corresponding author: Her-Chang Chao

Received October 8, 2017; revised January 13, 2018; revised March 15, 2018; revised July 14, 2018; accepted August 8, 2018; published December 31, 2018

Abstract

In order to achieve the goal of protecting medical images, some existing watermark techniques for medical image protection mainly focus on improving the invisibility and robustness properties of the method, in order to prevent unnecessary medical disputes. This paper proposes a novel copyright method for medical image protection based on visual secret sharing (VSS) and cellular automata transform (CAT). This method uses the protected medical image feature as well as VSS and a watermark to produce the ownership share image (OSI). The OSI is used for medical image verification and must be registered to a certified authority. In the watermark extraction process, the suspected medical image is used to generate a master share image (MSI). The watermark can be extracted by combining the MSI and the OSI. Different from other traditional methods, the proposed method does not need to modify the medical image in order to protect the copyright of the image. Moreover, the registered OSI used to verify the ownership and its appearance display meaningful information, facilitating image management. Finally, the results of the final experiment can prove the effectiveness of our method.

Keywords: Medical watermarking, copyright protection, visual secret sharing, cellular automata transform

1. Introduction

Most medical-related applications at present, such as telemedicine, hospital information systems, and Teleconsultation [1, 2], are made possible by the rapid development of the Internet. The creation of these medical applications enables people to seek treatment convenient. In addition, improvements in technology transform hospitals and medical research centers into computerized environments. This change draws attention to the digitization process, storage, and transmission of medical images, which has given rise to general standard protocol digital imaging and communications in medicine (DICOM). DICOM is based on TCP\IP communication. The purpose of this protocol is to set standards for the data processing, storage, printing, and communication transmission of medical imaging and related facilities, so that medical devices from different manufacturers can transmit and utilize patient information through a common network. This makes it possible for physicians and medical research units in different locations to store and access medical images and related information of a patient through the Internet from the image server, in order to perform immediate and convenient diagnosis, treatment, and research of the symptoms.

The standard file format of DICOM can be divided into two parts: The header and the data set. The header mainly documents important information provided by medical devices. The data set is comprised of a number of data elements, which generally include patient history, check-up information, parameters, device information, and video information. However, content in both the header and the data set is subject to attack, tampering, or misplacement during the transmission or storage process, which may lead to unnecessary medical disputes during the follow-up diagnosis and treatment of a disease. Malicious entities have had ample attack opportunities against remote medical applications, such as an open transmission channel that facilitates the sending of DICOM-formatted medical images. As such, it is important to ensure the safety and copyright protection of the data when transmitted through the open transmission channel, and this cannot be overlooked [3, 4]. For the abovementioned reasons, the development of cryptography, steganography, and watermarking technologies can provide a robust solution to the security and protection of digital content [5, 6].

Based on the embedding domain, the watermarking techniques can be classified into the spatial domain and the frequency domain. The spatial domain technique [7] is the direct method. This method directly modifies the image pixels to embed the watermark, and the processing speed is rapid. However, this method cannot resist processing attacks of various images [8] and it is mainly suitable for fragile watermarking methods. The frequency domain technique transforms the image into a frequency domain. The watermark is embedded by modifying the coefficient of the frequency domain. The transformation approaches employ a discrete Fourier transform (DFT) [9], discrete cosine transform (DCT) [10] and discrete wavelet transform (DWT) [11] to generate the frequency coefficient. In contrast to the spatial domain technique watermarking, transform domain techniques have a more robust ability to resist attacks and are mainly suited to robust watermarking methods. In addition, the technology of cellular automata transformation (CAT) [12] also has the same multi-resolution characteristic as DWT. It is only necessary to use fixed-point operations rather than floating-point operations, making calculation simple. Therefore, as long as the initial value and rule number are properly set, CAT can be used for image compression [13], data encryption [14], and digital watermarking [15-18].

The proposed watermarking techniques in recent years [15-21] needs to achieve four distinct characteristics in order to have an effective design: security, invisibility, robustness, and capacity. Lin et al. [19] proposed a watermarking method based on significant difference of wavelet quantization. In this study, the host image is decomposed using the 3-level DWT and obtain the mid-frequency sub-band LH3. The DWT coefficients in LH3 are divided into groups of seven non-overlapping blocks, and the two coefficients of the highest amplitude in each block are considered the significant coefficients. The pixel values of the watermark are individually embedded in the difference values of all significant coefficients. Even though this method maintains good visual quality of the watermarked image, it does not make the image fully resistant to most of the image processing attacks. A robust watermarking technique using inter-block coefficient differencing in DCT domain is presented by S. A. Parah et al. in [20]. The host image is divided into 8 × 8 pixel blocks and each block is computed to obtain the DCT coefficients. A pair of DCT coefficients are then selected in two adjacent blocks to embed the watermark in its difference. The advantage of this method is to satisfy the invisibility characteristic of the watermark, since only the DCT coefficients of some of the blocks in the image are moderately modified. However, this method does not necessarily resist strong malicious attacks. In addition, in recent years, some watermark methods use CAT [15-18] to achieve the invisibility and robustness characteristics and enhance the security of the watermark. In [15], Shiba et al. proposed a watermarking method based on CAT, which provides the same multi-resolution ability as does DWT, so in the beginning of Shiba's method it obtains the low-frequency coefficients of the host image through CAT, and directly embeds the watermark there. The advantage of using CAT is that the initial value and rule number need to be set when the image goes through the CAT conversion, and the two parameters can be regarded as confidential keys; in the recovery of the watermark, the exact settings have to be used to be able to successfully retrieve the watermark. The safety of the watermarking method is therefore improved. In addition, though Shiba's method has good imperceptibility, there is still room for improvement in the resistance to certain geometric attacks. Li et al. [17] and Sung et al. [18] have both implemented a three-dimensional (3D) image copyright protection method based on CAT. Their method uses 3D image as a watermark and embeds the 3D watermark into mid-frequency coefficients in the 2-level CAT domain. Although these methods retain the advantages of security and imperceptibility and can resist most of the signal processing, their resistance to rotation and shifting attacks can still be improved.

Where watermark is applied to medical images, Li et al. [16] offered a watermarking method for medical images based on CAT. The mid-frequency sub-band is extracted from the host image through CAT, and the watermark is embedded here. In addition to maintaining good quality of the watermarked image, this method also has sufficient resistance against destruction. In [22], Rahimi and Rabbani mentioned that for current picture archiving and communication systems, the digital storage and transmission of medical images are advantageous, but there is also a need to pay attention to medical image privacy and security. Thus, in Rahimi's method, the medical image is divided into ROIs (regions of interest) and RONIs (regions of non-interest), and then watermarks with different embedding intensities are embedded respectively. The advantage this system has is that it can maintain good imperceptibility and can also be applied to medical images in the DICOM format. In order to make the function of watermark embedding in medical images more effective, Cedillo-Hernandez et al. [23] proposed a watermarking method based on DFT-based effective management. In this method, the electronic patient record (EPR) data is converted to binary data, and encrypted with a confidential key as a watermark. In addition to verifying the

copyright of the protected medical image, this method can also facilitate management according to the embedded EPR data.

Whether the watermark information is embedded in the spatial domain or the frequency domain, risks of image quality in modification still exist. A number of scholars have started to focus on zero-watermarking methods [3, 24-30] based on a combination of visual secret sharing (VSS) [31, 32] and watermarking. These methods use the protected image feature as well as visual secret sharing and digital watermarks to produce the public image called ownership share image (OSI) and register the image with a certified authority. In the watermark extraction process, the protected image is used to generate the secret image, called the master share image (MSI). The watermark can be extracted by stacking the MSI and the OSI. This method will not affect image quality. The advantages of this method are: (1) the pixel values of the image will not be modified, so as to ensure that the image quality is not affected; (2) the size of the watermark that protects the image is not limited by the size of the image; (3) the method can be combined with cryptographic technology, which enhances the security of the watermarking method. From the above advantages, it can be seen that the zero-watermarking method can effectively achieve the security, invisibility, robustness, and capacity characteristics, and is therefore a research topic worthy of attention.

Wang and Chen [24] suggested a copyright protection method that adopts DCT to obtain the DC value of each non-overlapping block, as well as a feature matrix consisting of the DC value for each block. In the feature matrix, the relationship between the coefficient of each non-overlapping block and the mean value of the blocks is used to produce the OSI for image verification, and a codebook is not required. The OSI generated by the aforementioned image copyright protection methods has a black-and-white color method. Management of the OSI is difficult when the legal owner or creator owns more than one image. Rawat and Raman [25] proposed a copyright protection method based on visual cryptography techniques and fractional Fourier transform (FrFT) to achieve the OSI. In this method, the suitable image features are extracted by FrFT and singular value decomposition (SVD). The security of Rawat's method is ensured by using VSS. In regard to robustness, this method is not resistant to some attacks, such as those exploiting cropping and rotation. Fan et al. [3] described an approach using error control codes (ECC), VSS, and DWT. In their method, two different views were put forth. First, because zero watermarking does not embed the watermark into the host image, the size of the watermark is not limited by the size of the host image. Therefore, before this method generates the OSI, the watermark first goes through ECC encoding, giving the watermark the ability of error correction. Besides that, Fan's method also mentioned that because OSI's external appearance is a seemingly noisy image, the management of these images would be difficult if they are unintentionally mixed up. Therefore, the external appearance of the resulting OSI presents a meaningful message to improve the convenience of management. However, the clarity of the message presented by OSI still needs to be strengthened. Thanh and Tanaka [26] proposed a copyright protection method that splits a protected image into non-overlapping blocks, and each block is deconstructed into an upper triangular matrix by QR decomposition. The DCT is applied to these matrices and the significant DC coefficients of each matrix are obtained. Finally, the two consecutive DC coefficients are compared to produce the OSI for image verification. A hybrid domain method for image copyright protection based on the VSS technique was proposed by Amiri and Moghaddam [27]. The robustness of this method has been enhanced by using DWT, SVD, and the scale-invariant feature-transform technique. Dong and Li [28] proposed a zero-watermarking algorithm for medical images in the DWT-DFT domain to achieve the OSI. The method has the advantage that it does not modify the medical image, which prevents

medical disputes when protecting it. However, the robustness of this method has a tendency to decrease as the rotation ratio increases. Shao et al. [29] proposed a copyright protection method based on the Arnold transform and VSS, which has a high degree of robustness: in addition to obtaining valid host image features through the quaternion-type moment invariants, the robustness of this method, also breaks up the watermark through the Arnold transform method, so that if attacked, the watermark will not have concentrated distortion, which would otherwise make it impossible to identify the contents of the watermark.

Medical images are special images that are used to assist in the diagnosis of unusual medical conditions. A special degree of care is therefore required in the protection of medical images. In conventional watermarking methods for medical images, watermark data (which protect the image) are embedded into a medical image, with certain limits to the amount of watermark data that is embedded in the image. Although these methods can ensure the protection of medical images, they will also affect the quality of the protected medical images, and the degradation of a medical image is directly determined by the amount of watermark data that is embedded in the image. Conventional watermarking processes could therefore affect the accuracy of diagnoses based on protected medical images, thus leading to unnecessary medical disputes. To address this problem, many researchers have investigated the use of zero-watermarking techniques to protect medical images. These techniques ensure that the quality of the medical image will not be affected by the watermarking process, and they alleviate constraints on the amount of watermark data that can be used to protect an image. Despite the strengths of current zero-watermarking techniques, the robustness and manageability of these techniques still leaves much to be desired. In this paper, a novel copyright method for medical image protection based on the VSS and CAT is proposed. In order to give our proposed method sufficient safety and robustness, the pixels of the watermark are first mixed up before the implementation, and the verification information with error correction capability is obtained through ECC encoding. The ECC used in this paper is BCH code. Then, the low-frequency coefficient is obtained through CAT from the protected medical image, which is used as important feature to generate MSI. Next, the verification information, MSI, and stamp image are used to generate the OSI to verify the copyright of the medical image. The external appearance of the OSI is a clear presentation of the information of the stamp image, in order to facilitate the management of OSI. In the security aspect, because the initial value and rule number are set before CAT, these two parameters will be regarded as a confidential key. Furthermore, VSS encoding is used when generating OSI, so the overall watermark has excellent security. Lastly, the proposed mechanism does not modify any pixel values of the medical image to achieve the purpose of copyright protection, so that the medical image can retain the original quality.

The remainder of this paper is organized as follows. Section 2 presents the cellular automata transform, Section 3 describes the method; Section 4 discusses the experimental results; and Section 5 offers the conclusion.

2. Cellular Automata Transform

Cellular automata (CA) are dynamic systems in discrete time-space domains whose cells are arranged in lattice structures with each cell in a finite number of states. The states will evolve in unison according to the rule applied to a specified continuous space. CA thus processes the following three features: (a) Parallel computation: each cell can be synchronized in operation as parallel processors, and therefore, can perform parallel computations. (b) Locality: changes in cell states are affected only by cells within a certain distance. Global effects need to be

effected by setting cell values and rules of operation. (c) Homogeneity: cells operate and interact by the same operational rule. As pointed out in [12], appropriate CA generation rules and initial values will produce cellular spaces that can act as the basis functions for cellular automata transform (CAT). These functions can have orthogonal, semi-orthogonal, bi-orthogonal, and non-orthogonal bases, in which the orthogonal basis function can effectively extract CAT coefficients from the target signal, and can thus be used in data compression and information encryption.

One-dimensional (1D) cellular spaces provide the simplest environment for generating 1D CAT bases. It is defined by Eq. (1).

$$A_{ik} = 2a_{ik}a_{ki} - 1,\ 0 \le i,k \le N-1, \tag{1}$$

where N represents the total number of initial CA cells and $a_{ik} \in \{0,1\}$ represents the state of the CAs at a node i at time $a_{ik} \in \{0,1\}$. The 1D CAT and ICAT (inverse CAT) are defined by Eq. (2) and Eq. (3).

$$c_k = \frac{1}{N}\sum_{i=0}^{N-1} f_i A_{ik} \tag{2}$$

$$f_i = \frac{1}{N}\sum_{k=0}^{N-1} c_k A_{ik} \tag{3}$$

where c_k, $k = 0,1,\cdots,N-1$, is the CAT coefficient; and f_i, $i = 0,1,\cdots,N-1$, is the 1D signal that can be transformed into the CAT frequency space by the basis function A_{ik}, $i,k = 0,1,\cdots,N-1$. The image can be considered a two-dimensional signal. Therefore, 2D CAT basis functions were used for analysis, which was constructed based on Eq. (4).

$$A_{ijkl} = A_{ik}A_{jl} \tag{4}$$

where $0 \le i,\ j,k,l \le N-1$. Different 2D CAT basis functions are formed from different initial values and rule numbers, such as the one in **Fig. 1** constructed from the initial value 11011000_2 and rule number 158.

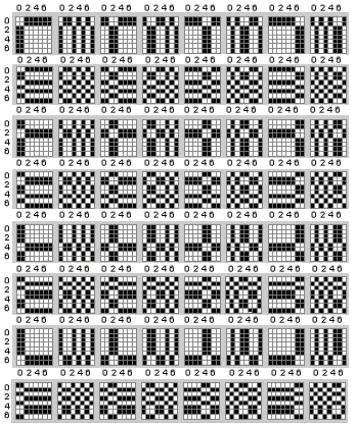


Fig. 1. 2D CAT basis function. The black and white pixels represent -1 and 1, respectively, with $N = 8$.

Using the as-obtained 2D CAT basis function, the 2D CAT and ICAT for an $N \times N$ input image f_{ij}, $0 \le i, j \le N-1$ are defined by Eq. (5) and Eq. (6).

$$c_{kl} = \frac{1}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f_{ij} A_{ijkl} \tag{5}$$

$$f_{ij} = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} c_{kl} A_{ijkl}, \tag{6}$$

where c_{kl}, $0 \le k, l \le N-1$ is the 2D CAT coefficient, and A_{ijkl}, $0 \le i, j, k, l \le N-1$ is the corresponding basis function.

After the 2D CAT processing of the image, the coefficient c_{kl} can be obtained and the frequency division can be performed according to the positions of *k* and *l*. If both *k* and *l* are even numbers, c_{kl} is the low-frequency component of the image block f_{ij}, which is collected and rearranged to obtain the low-low (LL) frequency sub-band. If *k* is even and *l* is odd, c_{kl} is the low-high frequency component of f_{ij}, which yields the low-high (LH) frequency sub-band. If *k* is odd and *l* is even, c_{kl} is the high-low frequency component of f_{ij}, which gives the high-low (HL) frequency sub-band. If both *k* and *l* are odd, c_{kl} is the high-frequency component, which forms the high-high (HH) frequency sub-band. As shown in **Fig. 2**, the frequency-divided image is split into LL, LH, HL, and HH sub-bands analogous to the frequency band decomposition. The CAT described in references [12-18] is capable of frequency decomposition, data hiding, and parallel processing, which makes them practical conversion methods in addition to DFT, DCT, and DWT.

(a) (b) (c)

Fig. 2. Illustrations of the CAT decomposition.
(a) Original image; (b) 2D CAT coefficients; and (c) four sub-band division.

3. Proposed Method

The proposed medical image protection method flow is illustrated in **Fig. 3**. It is divided into two phases: ownership share image construction and watermark extraction. In the ownership share image construction phase, BCH code encodes a watermark into the verification information. Next, the MSI is produced by CAT deconstructing the protected image into image features. Finally, verification information, MSI, and VSS can help generate an OSI that is registered to a certified authority. In the watermark extraction phase, a MSI can be produced

from a suspected medical image. The verification information can be extracted by stacking the MSI and the OSI. BCH code decrypts the verification information to the watermark. The ownership of the suspected medical image can be verified by observing watermark. The method is described hereinafter.

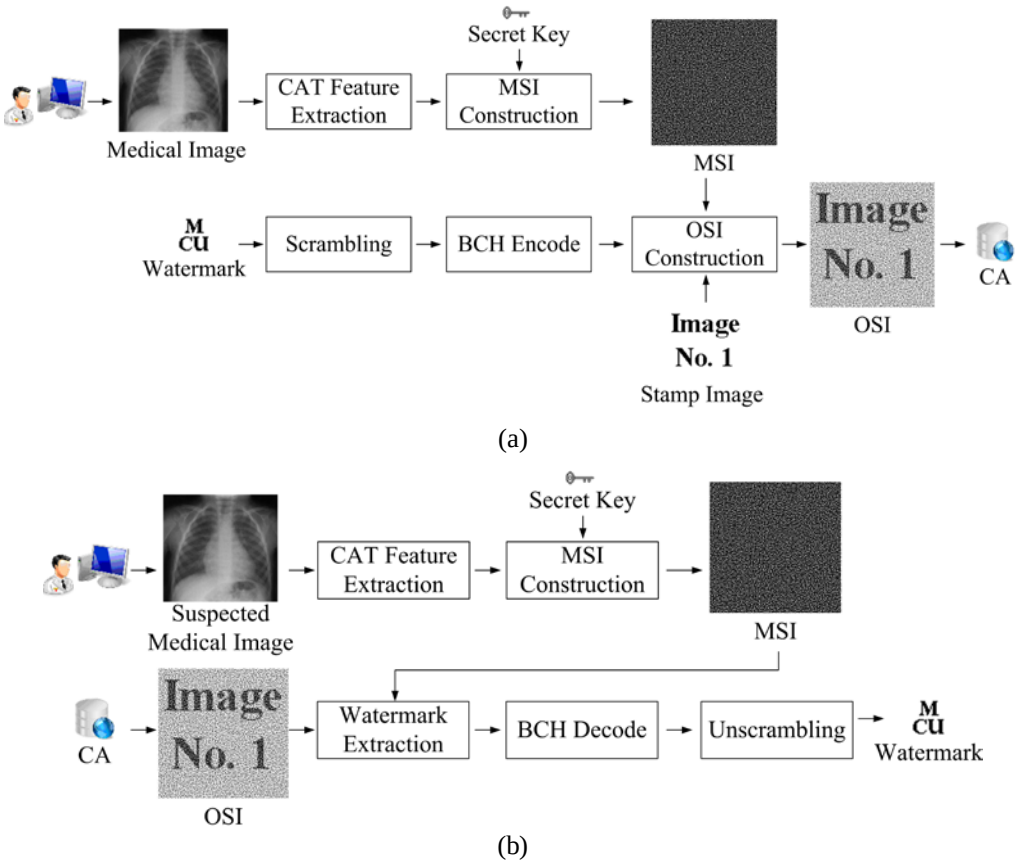


Fig. 3. Proposed method flow diagram.
(a) OSI construction phase and (b) watermark extraction phase.

3.1 OSI Construction

This section describes the generation of OSI process, which verifies medical image copyright. To increase the security of watermarks, torus automorphism (TA), proposed by Voyatzis and Pitas [33], is an effective method to scramble the pixel arrangement of a watermark. The n^{th} iteration of the TA function is defined by Eq. (7).

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \mod N \tag{7}$$

where k is an integer between 1 and N, and is a parameter that can be adjusted. N denotes the size of the image, (x_0, y_0) denotes the initial coordinate position of some pixels, and (x_n, y_n)

denotes the new coordinate position of (x_0, y_0) after n iterations. There is a quantity T that is referred to the automorphism period. This means the initial coordinates of all pixels are restored after the T^{th} iteration. The watermark W with a size of $m \times \ell$ is scrambled using TA and obtain the scrambled watermark W'. In order to give our proposed method sufficient robustness, each q pixel of scrambled watermark W' is encoded by $BCH(p,q)$ along the column and row to produce verification information V with a size of $(pm/q)\times(p\ell/q)$.

The protected medical image H with a size of $h \times h$ can be divided into 16×16 non-overlapping blocks entitled H_i, $i = 1, \cdots, (h/16)^2$, where i is the block index. A CAT coefficients H_i^c in LL_n (low-low sub-band) can be obtained by 2-level CAT deconstructing H_i. The maximum coefficient of each block H_i^c forms the feature coefficient matrix F_c with a size of $(h/16)\times(h/16)$. Next, the user prepares a secret key K that is used to seed a pseudorandom number generator, which subsequently facilitates random coefficient selection from the feature coefficient matrix F_c to form the feature matrix F. The width and height of feature matrix F are both two times the size of verification information V. In the feature matrix F, the maximum coefficient of each non-overlapping 2×2 block is set to white; the others are set to black, forming a binary image. Each pixel is white when the coefficient value is equal to 1 and is black when the coefficient is 0. Then the feature matrix is called MSI M.

In order to cause the OSI to have a specific pattern of stamp image C, the stamp image C pixel c_r, $r = 1, 2, \cdots, (pm/q)(p\ell/q)$, is referenced. The non-overlapping 2×2 block M_r and pixel v_r are respectively extracted from the MSI M and verification information V to map the rules, shown in **Table 1** and **Table 2**, to produce 2×2 block O_r of the OSI, in which r is the index of the block or pixel. Assuming that the pixel v_r is black, block O_r can be selected from the four-block M_r pattern and pixel c_r according to the rule shown in **Table 1**. One of the pixels in the gray region of the selected O_r is randomly defined as white with the others black. Assuming the pixel v_r is white, block O_r can be selected by the rule shown in **Table 2**. One of the pixels in the gray region of the selected O_r is randomly defined as black and the others are white. After each block is mapped with the pixel v_r, all of the O_r blocks can form OSI O. The OSI O is registered to certified authority. The OSI effectively acts as a secret key in image form when it is stored in a certified authority. Hence, the OSI is stored as raw data by the certified authority. When an image ownership dispute occurs, the image ownership can be verified by extracting the watermark from the OSI and the disputed image. The OSI construction algorithm is as follows:

Table 1. Generation rule of the block O_r.

(Pixel v_r is black)

M_r	c_r	Stacking Result
	■ □	

Table 2. Generation rule of the block O_r.

(Pixel v_r is white)

M_r	c_r	Stacking Result
	■ □	

Algorithm 1: OSI Construction

Input: Protected medical image *H*, watermark *W*, stamp image *C*, and secret keys *K*.

Output: OSI O.

Step 1: Use TA function to scramble the watermark *W* and generate the scrambled watermark W'.

Step 2: Use $BCH(p,q)$ to encode the scrambled watermark W' and generate a verification information V.

Step 3: Divide protected medical image H into 16×16 non-overlapping block H_i, $i=1,\cdots,(h/16)^2$. Each block is decomposed by 2-level CAT, and the entire decomposed maximum coefficient H_i^c, $i=1,\cdots,(h/16)^2$, form feature coefficient matrix F_c.

Step 4: Use secret key *K* to randomly select coefficients from the feature coefficient matrix F_c to form feature matrix *F*, where the width and height are two times the size of verification information V.

Step 5: In feature matrix *F*, the maximum coefficient of each non-overlapping 2×2 block is set to 1 and the others are set to 0. This can generate the MSI M.

Step 6: In the MSI M, extract non-overlapping 2×2 block M_r, $r=1,2,\cdots,(pm/q)(p\ell/q)$, according to M_r blocks, the pixel value of c_r, v_r, and the rules of **Table 1** and **Table 2** to produce O.

Step 7: The OSI O is registered to certified authority.

3.2 Watermark Extraction

This section explains the watermark extraction process. When the image owner wants to verify ownership of suspected medical image $\hat{H}$, the watermark $\hat{W}$ is extracted as follows: Steps 3 to 5 of the OSI construction algorithm are performed to produce the MSI $\hat{M}$ for verifying suspected medical image $\hat{H}$. Based on Eq. (8), pixel value $\hat{m}_i$ of MSI $\hat{M}$ and pixel value o_i of OSI O can generate the pixel value d_i of stacked image D, $i=1,2,\cdots,(2pm/q)(2p\ell/q)$.

$$d_i=\hat{m}_i\wedge o_i \tag{8}$$

where $\hat{m}_i$ and o_i are the i^{th} of the pixel value of MSI $\hat{M}$ and OSI O, respectively. $\wedge$ represents the Boolean AND operation. In the stacked image *D*, each non-overlapping 2×2 block D_r, $r=1,2,\cdots,(pm/q)(p\ell/q)$, is used to generate the pixel value $\hat{v}_r$ of verification information $\hat{V}$, according to Eq. (9).

$$\hat{v}_r=\begin{cases}1 & ,\text{if } \sum_{x=1}^{2}\sum_{y=1}^{2}D_r(x,y)=1\\ 0 & ,\text{otherwise}\end{cases} \tag{9}$$

In Eq. (9), if the $\hat{v}_r$ pixel value is equal to 1, the pixel is white; otherwise, black. Finally, $BCH(p,q)$ decrypts the verification information $\hat{V}$ to the scrambled watermark $\hat{W}'$. The scrambled pixel position can be restored by TA, and the watermark $\hat{W}$ can be deduced from

the scrambled watermark $\hat{W}'$. The ownership of suspected medical image $\hat{H}$ can be verified by observing watermark $\hat{W}$. The watermark extraction algorithm is as follows:

Algorithm 2: Watermark Extraction

Input: Suspected medical image $\hat{H}$, OSI O, and secret keys K.

Output: Extracted watermark $\hat{W}$.

Step 1: Perform step 3 to step 5 of the OSI construction algorithm to produce MSI $\hat{M}$.

Step 2: Use Eq. (8), the MSI $\hat{M}$ and OSI O can generate the stacked image D.

Step 3: Use Eq. (9), the stacked image D can construct the verification information $\hat{V}$.

Step 4: Apply $BCH(p,q)$ to decrypt the verification information $\hat{V}$ and generate the scrambled watermark $\hat{W}'$.

Step 5: Through TA, the watermark $\hat{W}$ can be restored by reordering the pixel position of scrambled watermark $\hat{W}'$.

4. Experimental Classification Results and Analysis

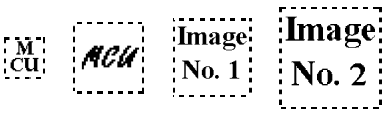
Herein we describe the performance of the proposed watermarking algorithm. Our method is tested by supplying medical images of different modalities, such as computed tomography (CT), magnetic resonance (MR), X-Ray, computed radiography (CR), and other (OT), each of size 512×512 as shown in **Figs. 4(a)~(e)**. In **Fig. 5**, the nature images acquired in experiments have a size of 512×512, and are named Baboon, Lena, and Peppers. The medical images and nature images are 8-bit grayscale images. **Figs. 6(a)** and **(b)** shows two binary watermark with size 35×35 and 70×70. **Figs. 6(c)** and **(d)** illustrate the stamp images with size 105×105 and 150×150 for verification of medical images. The program development tool was MATLAB and the computation platform was a personal computer with 2.67 GHz of Intel i5 CPU and 3 GB of RAM. The original medical images were damaged and attacked in the experiment, and then the attacked medical images were used for image verification. Subsequently, in **Figs. 7** and **8** experiments, the initial value and rule number of CAT are 10000001_2 and 11. **Fig. 7** shows simulation results of the proposed scheme obtained by using **Fig. 4(a)**, **Fig. 6(a)**, **Fig. 6(c)**, and $BCH(15,5)$. **Figs. 7(a)** and **(b)** show the MSI and OSI with size 210×210, respectively, and **Fig. 7(c)** shows the hidden watermark revealed by combining **Fig. 7(a)** with **Fig. 7(b)**. Similarly, **Fig. 8** shows simulation results of the proposed scheme obtained by using **Fig. 4(b)**, **Fig. 6(b)**, **Fig. 6(d)**, and $BCH(15,7)$. **Figs. 8(a)** and **(b)** show the MSI and OSI with size 250×250, respectively, and **Fig. 8(c)** shows the hidden watermark revealed by combining **Fig. 8(a)** with **Fig. 8(b)**. From the simulated test results in **Fig. 7** and **Fig. 8**, it can be seen that from the OSI generated by the method we proposed, the information displayed by stamp image can be clearly distinguished from its external appearance. Even when the OSI is unclear, management is still tenable according to the information displayed by its external appearance. In addition, from the steps in Algorithm 2, we can see that the watermark can be retrieved by combining MSI and OSI with a size of $N\times N$. During this processing, there were N^2 Boolean AND operations, $N^2/4$ comparators, and $3N^2/4$ adders. After retrieving the scrambled watermark, the extracted watermark can be deduced from the scrambled watermark. The overall operation does not consume a lot of time.

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

Fig. 4. Experimental medical images. (a) CT, (b) MR, (c) X-Ray, (d) CR, and (e) OT.

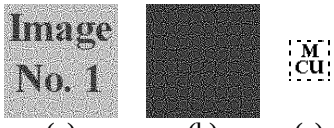
(a) (b) (c)

Fig. 5. Experimental nature images. (a) Baboon, (b) Lena, and (c) Peppers.



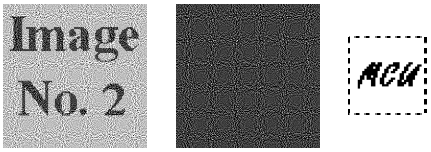
(a) (b) (c) (d)

Fig. 6. Two simulated watermark and stamp images, respectively. (a) Logo1 (35×35), (b) Logo2 (70×70), (c) stamp image1 (105×105), and (d) stamp image2 (150×150).



(a) (b) (c)

Fig. 7. Simulation results obtained by performing the proposed scheme on CT image. (a) OSI (210×210), (b) MSI (210×210), and (c) Retrieved watermark (35×35).



(a) (b) (c)

Fig. 8. Simulation results obtained by performing the proposed scheme on MR image. (a) OSI (250×250), (b) MSI (250×250), and (c) Retrieved watermark (70×70).

In this paper, we employed the *PSNR* (peak signal to noise ratio) and *NC* (normalized correlation) to test the indicators of the attack degree of the medical image and the basis of the watermark robustness. *PSNR* is defined by Eq. (10) and Eq. (11).

$$PSNR = 10\times 1\log\left(\frac{MAX^2}{MSE}\right) \quad \text{(dB)} \tag{10}$$

$$MSE = \frac{1}{h\times h}\sum_{x=1}^{h}\sum_{y=1}^{h}(H(x,y)-\hat{H}(x,y))^2 \tag{11}$$

MSE is the mean square error of the $h \times h$ image, *MAX* is the maximum pixel of the original medical image, $H(x, y)$ is the gray value of the original medical image, and $\hat{H}(x, y)$ is the gray value of the medical image under attack. A smaller *PSNR* indicates that the medical image under attack and the original medical image are more dissimilar. Conversely, a larger *PSNR* means that the distortion of the attacked medical image is smaller. *NC* is defined by Eq. (12).

$$NC = \frac{\sum_{i=1}^{J} \overline{w_i \oplus \hat{w}_i}}{J} \tag{12}$$

where w_i and $\hat{w}_i$ are the pixel value of original watermark W and extracted watermark $\hat{W}$, respectively, i is the index of the watermark pixel, J is the total number of watermark pixels, and $\oplus$ represents the Exclusive-OR logical operation. The *NC* value ranges from 0 to 1. The closer the *NC* value is to 1, the smaller the distortion of the watermark. **Table 3** and **Table 4** lists the attack parameters and *PSNR* values of the attacked medical images for CT, MR, X-ray, CR, and OT. The CT medical images between the test images we have prepared were subjected to the image processing attacks listed in **Table 3**. The resulting images (attacked CT medical images) are shown in **Figure 9**. **Table 4** and **Figure 9** show the generation of a strong distortion in the test medical image when subjected to various attacks, such as an increase in noise, blurring attacks, cropping, and rotation. Such a distortion can cause the attacked medical image to differ from the original medical image. Thus, there is a certain degree of distortion between the image features extracted from the attacked medical image and the original medical image.

Table 3. Medical image attack parameters.

Attacks	Parameter	Attacks	Parameter
JPEG-30	quality factor = 30%	Gaussian Blurring-4	radius = 4
JPEG-10	quality factor = 10%	Gaussian Blurring-8	radius = 8
JPEG 2000-2	compression ratio = 2	Brightness (25)	increased brightness of 25%
JPEG 2000-8	compression ratio = 8	Brightness (-25)	decreased brightness of 25%
Gaussian Noise-0.1	mean = 0, variance = 0.1	Median Filtering	window size = 4×4
Gaussian Noise-0.5	mean = 0, variance = 0.5	Average Filtering	window size = 4×4
Salt-pepper Noise-10	noise density = 10%	Rotation-3	rotate 3 degrees
Salt-pepper Noise-50	noise density = 50%	Rotation-7	rotate 7 degrees
Scaling	reduced 1/16	Cropping	cropped area of 25%
Mixed	JPEG and Gaussian noise	Histogram Equalization	Matlab function

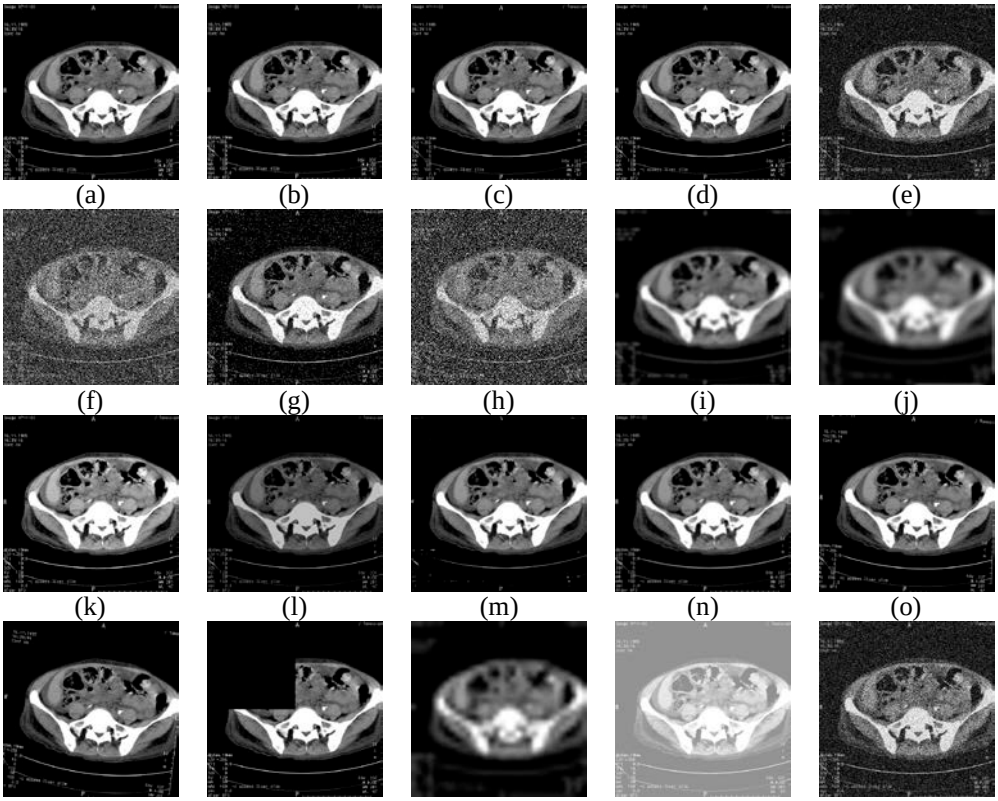


Fig. 9. Attacked CT medical image. (a) JPEG-30, (b) JPEG-10, (c) JPEG 2000-2, (d) JPEG 2000-8, (e) Gaussian Noise-0.1, (f) Gaussian Noise-0.5, (g) Salt-pepper Noise-10, (h) Salt-pepper Noise-50, (i) Gaussian Blurring-4, (j) Gaussian Blurring-8, (k) Brightness (25), (l) Brightness (-25), (m) Median Filtering, (n) Average Filtering, (o) Rotation-3, (p) Rotation-7, (q) Cropping, (r) Scaling, (s) Histogram Equalization, and (t) Mixed.

Table 4. *PSNR* of the medical images after various attacks.

Attacks	*PSNR*				
	CT	MR	X-Ray	CR	OT
JPEG-30	31.0987	41.8754	41.6192	41.7853	32.7993
JPEG-10	26.1302	35.8029	35.6538	35.8618	29.8464
JPEG 2000-2	58.1398	55.7231	55.0572	53.3118	56.1610
JPEG 2000-8	41.6341	55.6213	54.3154	51.8127	38.1865
Gaussian Noise-0.1	12.3631	12.4622	11.8063	11.2398	11.9350
Gaussian Noise-0.5	7.4847	7.5236	7.6951	7.8968	7.6738
Salt-pepper Noise-10	13.6939	13.7042	14.5042	15.575	14.3644
Salt-pepper Noise-50	6.6995	6.7394	7.5406	8.5681	7.3927
Gaussian Blurring-4	18.4557	30.9948	30.1453	38.8137	25.5466
Gaussian Blurring-8	16.9669	26.7036	26.0336	34.5178	23.8515

Brightness (25)	24.2837	25.6799	20.2392	17.9653	18.7489
Brightness (-25)	20.7875	25.7545	20.0713	17.7050	18.5294
Median Filtering	18.7095	39.7234	37.6072	34.004	28.4890
Average Filtering	19.9368	39.1097	36.3919	32.4550	27.9638
Rotation-3	14.5925	23.0825	26.3203	18.3678	20.1127
Rotation-7	12.7900	19.5875	22.0201	14.7301	16.9179
Cropping	17.4920	17.3249	12.2764	11.6974	13.2651
Scaling	16.9339	26.8446	29.6069	34.6447	23.2134
Histogram Equalization	6.2134	6.7832	12.0877	17.3079	14.6603
Mixed	12.2296	12.36	11.7178	11.1094	11.8232

The simulated results in the various attacks for CT and MR are shown in **Table 5**. The BCH code used in this simulation is $BCH(15,5)$. The watermark and stamp images are **Fig. 6(a)** and **Fig. 6(c)**, respectively. From **Table 5**, it can be seen that the extracted watermark could preserve the complete watermark information after various attacks, especially in compression, noise, median filtering, and histogram equalization attacks. In noise, rotation, and cropping attacks, a perfect watermark could not be extracted, but the watermark information could still be identified.

Table 5. The simulated results of CT and MR by *BCH*(15, 5).

Attack	CT		MR	
	NC	Retrieved watermark	*NC*	Retrieved watermark
JPEG-30	1		1	
JPEG-10	1		1	
JPEG 2000-2	1		1	
JPEG 2000-8	1		1	
Gaussian Noise-0.1	1		0.9992	
Gaussian Noise-0.5	0.9984		0.9853	
Salt-pepper Noise-10	1		1	
Salt-pepper Noise-50	0.9959		0.9584	
Gaussian Blurring-4	1		1	
Gaussian Blurring-8	1		1	
Brightness (25)	1		1	
Brightness (-25)	1		1	
Median Filtering	1		1	
Average Filtering	1		1	
Rotation-3	1		1	
Rotation-7	0.9927		0.9927	

Cropping	1		0.9412	
Scaling	1		1	
Histogram Equalization	1		1	
Mixed	1		0.9992	

Next, we carried out simulation experiments with different initial values and rule numbers for the CAT used for extraction of image characteristics, and the results were compiled in **Table 6**. In these experiments, two different initial values and rule numbers of CAT used in all simulation experiments are respectively 01011001_2 and 14, as well as 11000000_2 and 15. **Fig. 4(c)** and **4(d)** are the medical images used in the simulation, while the watermark and stamp images are **Fig. 6(a)** and **Fig. 6(c)**, respectively, and the BCH code used in this simulation is $BCH(15,5)$. From the experiment in **Table 6**, we can see that regardless of which group of CAT initial value and rule number is used for protection of medical images, the destruction-resistance of the watermark demonstrated good results. Even if a different CAT initial value or rule number was used, the extracted image characteristics still possessed resilience as the watermark was effectively retrieved when protected medical images underwent malicious image processing attacks. This is particularly so for compression attacks, scaling, histogram equalization, and median filtering, where the watermark was retrieved perfectly.

Table 6. The simulated results of X-Ray and CR by different initial value and rule number of CAT.

Attack	X-Ray				CR			
	C1		*C2*		*C1*		*C2*	
	NC	*Rw*	*NC*	*Rw*	*NC*	*Rw*	*NC*	*Rw*
JPEG-30	1		1		1		1	
JPEG-10	1		1		1		1	
JPEG 2000-2	1		1		1		1	
JPEG 2000-8	1		1		1		1	
Gaussian Noise-0.1	1		1		1		0.9967	
Gaussian Noise-0.5	0.9959		0.9959		0.9722		0.9535	
Salt-pepper Noise-10	1		1		1		1	
Salt-pepper Noise-50	0.9943		0.9976		0.9600		0.9673	
Gaussian Blurring-4	1		1		1		1	
Gaussian Blurring-8	1		1		1		1	
Brightness (25)	1		1		1		1	
Brightness (-25)	1		1		1		1	
Median Filtering	1		1		1		1	
Average Filtering	1		1		1		1	
Rotation-3	1		1		1		0.9967	
Rotation-7	0.9976		0.9984		0.9396		0.9453	

Cropping	0.9029		0.9143		0.9976		0.9967	
Scaling	1		1		1		1	
Histogram Equalization	1		1		1		1	
Mixed	1		1		1		1	

Note. *Rw* = Retrieved watermark; *C1* = initial value as 01011001_2 and rule number as 14; *C2* = initial value as 11000000_2 and rule number as 15.

Using BCH codes with different error-correcting capabilities, the watermark data extracted for verification of the attacked OT image are shown in **Table 7**. Although *BCH*(15,7) and *BCH*(15,5) have different error-correcting capabilities, the information on the watermark extracted could be identified after various attacks. From this, the watermark information extracted using the proposed method presented a high level of robustness after various attacks.

Table 7. Simulated result of OT by different BCH codes.

Attack	*BCH*(15,7)		*BCH*(15,5)	
	NC	Retrieved watermark	*NC*	Retrieved watermark
JPEG-30	1		1	
JPEG-10	1		1	
JPEG 2000-2	1		1	
JPEG 2000-8	1		1	
Gaussian Noise-0.1	0.9976		1	
Gaussian Noise-0.5	0.9290		0.9869	
Salt-pepper Noise-10	1		1	
Salt-pepper Noise-50	0.9567		0.9967	
Gaussian Blurring-4	1		1	
Gaussian Blurring-8	1		1	
Brightness (25)	1		1	
Brightness (-25)	1		1	
Median Filtering	1		1	
Average Filtering	1		1	
Rotation-3	0.9976		1	
Rotation-7	0.9747		1	
Cropping	0.9682		1	
Scaling	0.9976		1	
Histogram Equalization	1		1	
Mixed	0.9935		1	

In order to demonstrate the application flexibility of our mechanism, a simulation experiment of a grayscale nature image is provided in **Table 8**. In this experiment, the

watermark used is **Fig. 6(a)**, the stamp image is **Fig. 6(c)**, the BCH code used is $BCH(15,5)$ and the initial value and rule number of CAT is 11010100_2 and 147, respectively. The nature image and the medical image itself have different image characteristics. However, we can see from **Table 8** that our mechanism yields good results in protecting nature images as the watermark can be effectively retrieved from protected images after undergoing many types of image processing attacks, with *NC* values above 0.9. This shows that the content of the watermark can be clearly identified.

Table 8. Simulated result of nature images.

Attacks	Baboon		Lena		Peppers	
	PSNR	*NC*	*PSNR*	*NC*	*PSNR*	*NC*
JPEG-30	26.4758	1	34.2648	1	33.6933	1
JPEG-10	23.4774	1	30.3760	1	30.4571	1
JPEG 2000-2	45.5768	1	54.2959	1	52.8087	1
JPEG 2000-8	29.078	1	40.2888	1	38.2474	1
Gaussian Noise-0.1	11.2338	0.9804	11.3258	0.9992	11.4465	0.9992
Gaussian Noise-0.5	7.902	0.9271	7.8767	0.9322	7.8597	0.9445
Salt-pepper Noise-10	15.5696	1	15.4663	1	15.3239	1
Salt-pepper Noise-50	8.5823	0.9561	8.4564	0.9714	8.2726	0.9371
Gaussian Blurring-4	20.1904	1	25.0707	1	25.1541	1
Gaussian Blurring-8	19.3880	0.9992	22.0836	1	21.6252	1
Brightness (25)	17.4784	1	17.8728	1	17.8647	1
Brightness (-25)	17.5284	1	17.7603	1	17.8190	1
Median Filtering	21.6838	1	28.9218	1	29.0390	1
Average Filtering	21.6914	1	28.3642	1	28.2798	1
Rotation-3	15.7564	0.9706	16.2678	0.9878	15.3879	0.9339
Rotation-7	14.2158	0.9184	13.4035	0.9243	12.2813	0.9241
Cropping	11.9229	0.9951	11.9812	1	11.9537	0.9878
Scaling	19.3501	0.9804	21.9871	0.9935	21.5879	0.9804
Histogram Equalization	17.5701	1	19.0995	1	20.6591	1
Mixed	11.1231	0.9878	11.2388	0.9992	11.3003	0.9992

It can be observed from the obtained experimental results that the performance of the proposed scheme has sufficient robustness. Image processing attacks such as compression and blurring can cause the removal of several high frequency features. However, during image feature extraction in the proposed scheme, CAT was employed for extracting the low frequency image features while the OSI was constructed. The low frequency feature of CAT represents the image part having the strongest energy. Therefore, during watermark recovery, there is lesser damage to the image features, which in turn allows high quality reconstruction of retrieved watermarks. In attacks involving an increase in noise, noise addition in the image can damage the overall features of the image. The extent of distortion increases with

increasing amount of noise. Hence, the proposed scheme relies on the features extracted by CAT and the error-correcting ability of BCH to withstand noise attacks. Regarding the aspect of geometric attacks such as rotation and cropping, it may be possible that the extracted features are not in the same positions as the original positions owing to the deformation of the image content, thereby causing the watermark retrieval to be unsuccessful. In the proposed scheme, the images were segmented into 16×16 non-overlapping blocks during the extraction of image features. Thus, even if the image is damaged, content close to the original features can still be extracted. Furthermore, before the watermark was embedded, the pixel values of the watermark were first scrambled. Such scrambling was performed so that even if the pixel values of the watermark became distorted and damaged, it would not be overly focused and unidentifiable. This corroborates that the proposed scheme has a good performance efficiency.

For performance comparisons, four copyright protection methods, proposed by [24], [25], [26], and [30] were implemented in this study. We use the gray-scale images CT and MR in **Fig. 4(a)** and **(b)** as the test images. The watermark shown in **Fig. 5(a)** is used for the experiment, and the stamp image shown in **Fig. 6(a)** is used for proposed scheme. As shown in **Table 9**, Wu's scheme is able to sustain different compression attacks such as JPEG compression and JPEG 2000. However, Wu's scheme is vulnerable to geometric attacks such as cropping, scaling, rotation, and histogram equalization, whereas our scheme is able to withstand such attacks. Moreover, it is obvious that the performance of our scheme is much better than the algorithms in [24, 25, 26, 30]. A feature of our scheme is that it can extract the watermark perfectly in the case of some image processing attacks such as median filtering, scaling, histogram equalization, and compression attacks. Simulated curves of *NC* from the extracted watermarks after JPEG compression, Gaussian noise, and rotation attacks with different parameters are respectively shown in **Figs. 10(a)**, **(b)**, and **(c)**. From these figures, the proposed method is more capable of resisting JPEG compression, Gaussian noise, and rotation image processing attacks than two related methods. It can thereby be seen that the low-frequency coefficient extracted from the image through CAT is suitable for constructing OSI. Moreover, the watermarks are ECC-encoded. These two factors mitigate and resist damage to the image in this proposed method.

Table 9. Comparison of the simulation results of CT.

Attack	*NC*				
	Proposed Scheme	[30] Method	[26] Method	[25] Method	[24] Method
JPEG-30	1	1	1	1	1
JPEG-10	1	1	0.9824	0.9907	0.9992
JPEG 2000-2	1	1	1	0.9995	0.9845
JPEG 2000-8	1	1	0.9936	0.9980	0.9820
Gaussian Noise-0.1	1	0.9896	0.9812	0.9912	0.9869
Gaussian Noise-0.5	0.9984	0.9118	0.9334	0.9568	0.9633
Salt-pepper Noise-10	1	0.9837	1	0.9726	0.9886
Salt-pepper Noise-50	0.9959	0.9322	0.9551	0.9312	0.9535
Gaussian Blurring-4	1	0.9967	0.9853	0.9656	0.9780
Gaussian Blurring-8	1	0.9935	0.9774	0.9182	0.9755

Brightness (25)	1	0.9992	1	1	1
Brightness (-25)	1	1	0.9915	1	1
Median Filtering	1	0.9927	1	0.9839	0.9796
Average Filtering	1	0.991	1	0.9829	0.9886
Rotation-3	1	0.9878	0.9792	0.9515	0.9616
Rotation-7	0.9927	0.9600	0.9491	0.9122	0.9257
Cropping	1	0.9420	0.9594	0.9438	0.9404
Scaling	1	0.9935	0.9806	0.9966	0.9739
Histogram Equalization	1	0.8890	0.9851	0.9634	0.9992
Mixed	0.9992	0.9731	0.9812	0.9177	0.9614

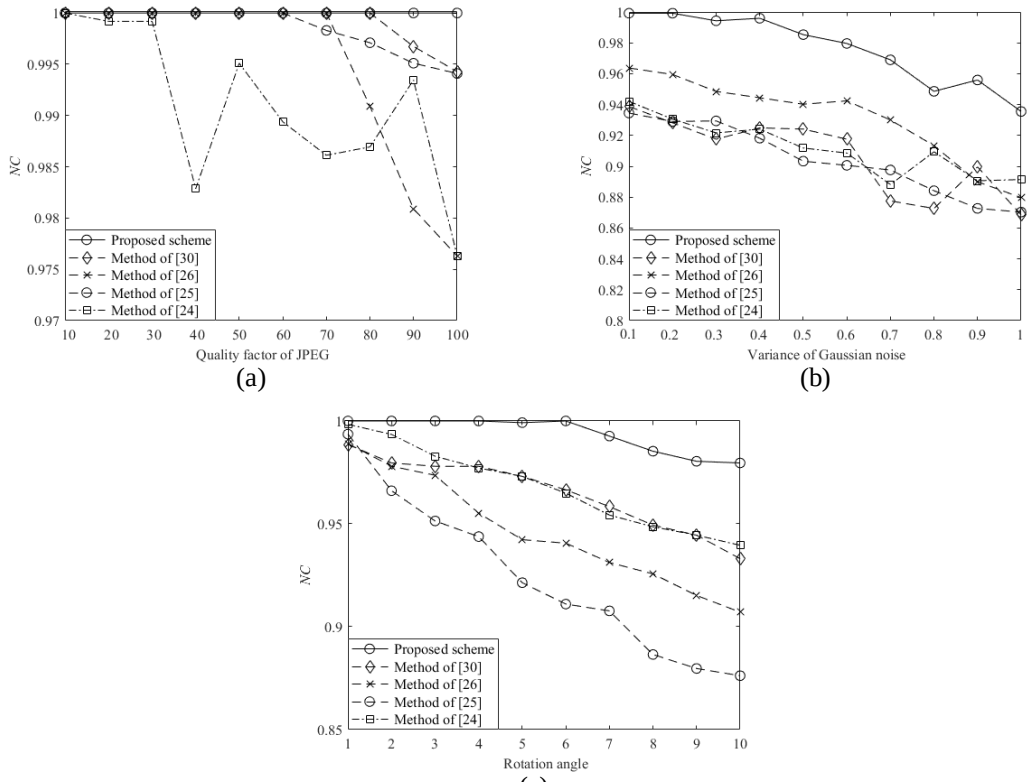
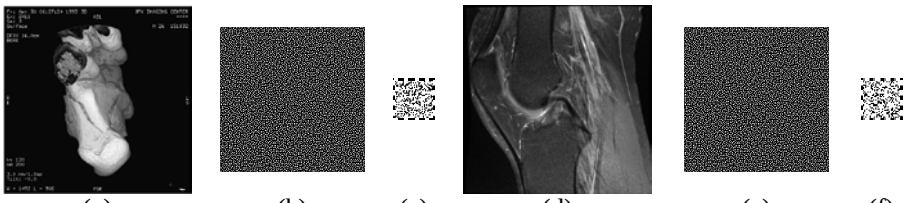


Fig. 10. Simulated curves of the *NC* with different attack parameters. (MR) (a) JPEG、(b) Gaussian noise and (c) Rotation.

Lastly, the unregistered medical images in **Fig. 11(a)** and **Fig. 11(d)** are used to test whether our scheme is practical and whether unambiguity will occur. **Fig. 11(b)** and **Fig. 11(e)** are the extracted MSI of unregistered images, which was used in combination with the registered OSI in **Fig 7(a)** to extract the watermark. From **Fig. 11(c)** and **Fig. 11(f)**, we can see that the unregistered medical images cannot produce a meaningful watermark with registered OSI, while other content were all noise. This proves that the proposed scheme cannot extract watermarks from unregistered images, resulting in unambiguity and sufficient safety.



(a) (b) (c) (d) (e) (f)

Fig. 11. Simulation results obtained by performing the proposed scheme on an unregistered medical image. (a) and (d) unregistered medical images, (b) and (e) MSI of unregistered medical images, (c) and (f) retrieved watermarks, respectively.

5. Conclusion

Due attention must be given to the digitization, process, storage, and transmission of medical images together with this change. In this paper, we proposed a novel copyright method for image protection based on VSS and CAT. The main purpose of this method is to protect the copyright of medical images. The advantages of the proposed method are as follows: first, this method does not need to modify a protected medical image and can maintain the quality of a protected medical image. The proposed method can effectively achieve the invisibility. In other words, this prevents medical disputes when protecting medical images with our method. Secondly, the proposed method employs VSS and CAT to enhance the requirements of security. The watermark can be resistant to intentional attacks that attempt to remove the watermarks. Thirdly, because the watermark size in our method is not limited to the protected medical image, it is possible to generate verification information through ECC-encoding before implementing the watermark. Even though malicious damage to protected medical images can degrade features in the image and affect the verification information, the watermark for protection has error-correcting capability after using BCH code, and the resistance of the watermark to attacks can be enhanced. In addition, the OSI for medical image verification is no longer an irregular black-and-white image, and it can display meaningful pattern and information to facilitate OSI management. The experiment results indicated that a perfect watermark can be extracted after common image processing, such as JPEG compression, noise attacks, rotation, cropping, or histogram equalization. The unregistered images cannot generate a meaningful watermark with the registered OSI, and thus, there will be no unambiguous situations. Based on the above experimental results, the proposed method illustrates better robustness and feasibility than other related methods.

References

[1] M. Abo-Zahhad, S. M. Ahmed and O. Elnahas, “A wireless emergency telemedicine system for patients monitoring and diagnosis,” *International Journal of Telemedicine and Applications*, vol. 2014, pp. 1–11, 2014. Article (CrossRef Link)

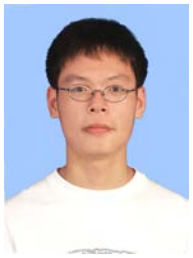
[2] Y. C. Weng and S.L. Hsieh, “Design and implementation of a web-based medical drawing management system,” *Journal of Intelligent Information Systems*, vol. 49, no. 3, pp. 391–405, 2017. Article (CrossRef Link)

[3] T. Y. Fan, B. C. Chieu and H. C. Chao, “Robust copyright-protection scheme based on visual secret sharing and Bose–Chaudhuri–Hocquenghem code techniques,” *Journal of Electronic Imaging*, vol. 21, no. 4, pp. 043018, 2012. Article (CrossRef Link)

[4] M. P. Turuk and A. P. Dhande, “A novel reversible multiple medical image watermarking for health information system,” *Journal of Medical Systems*, vol. 40, pp. 269, 2016. Article (CrossRef Link)

[5.] H. Nyeem, W. Boles and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of Digital Imaging*, vol. 26, no. 2, pp. 326–343, 2013. Article (CrossRef Link)
[6] S. A. Parah, F. Ahad, J. A. Sheikh and G. M. Bhat, "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique," *Journal of Biomedical Informatics*, vol. 66, pp. 214–230, 2017. Article (CrossRef Link)
[7] R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2, pp. 86–90, 1994. Article (CrossRef Link)
[8] C. C. Chang and P. Y. Lin, "Adaptive watermark mechanism for rightful ownership protection," *Journal of Systems and Software*, vol. 81, no. 7, pp. 1118–1129, 2008. Article (CrossRef Link)
[9] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, 2011. Article (CrossRef Link)
[10] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997. Article (CrossRef Link)
[11] X. G. Xia, C. G. Boncelet and G. R. Arce, "A multiresolution watermark for digital images," in *Proc. IEEE Int. Conf. Image Process.*, vol. 1, pp. 548–551, 1997. Article (CrossRef Link)
[12] O. Lafe, *Cellular Automata Transforms: Theory and Applications in Multimedia Compression, Encryption and Modeling*, Kluwer Academic Publishers, Norwell, MA, 2000. Article (CrossRef Link)
[13] R. J. Chen, C. F. Tai and J. L. Lai, "Novel CAT Wavelets-based image coding system," in *Proc. IEEE Int. Symp. Consum. Electron.*, pp. 1–6, 2007. Article (CrossRef Link)
[14] Z. Eslami, S. H. Razzaghi and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognition*, vol. 43, no. 1, pp. 397–404, 2010. Article (CrossRef Link)
[15] R. Shiba, S. Kang and Y. Aoki, "An image watermarking technique using cellular automata transform," in *TENCON 2004. 2004 IEEE Region 10 Conf.*, pp. 303–306, 2004. Article (CrossRef Link)
[16] X. W. Li, S. J. Cho and S. T. Kim, "2-D CAT-based medical image watermarking algorithm," *International Journal of Computer Theory and Engineering*, vol. 4, no. 5, pp. 722-725, 2012. Article (CrossRef Link)
[17] X. W. Li, S. T. Kim and I. K. Lee, "3D image copyright protection based on cellular automata transform and direct smart pixel mapping," *Optics Communications*, vol. 329, pp. 92–102, 2014. Article (CrossRef Link)
[18] M. Sung, X. Li and I. K. Lee, "Visual perception based robust watermarking with integral imaging," *Optik-International Journal for Light and Electron Optics*, vol. 127, no. 24, pp. 11828–11839, 2016. Article (CrossRef Link)
[19] W. H. Lin, S. J. Horng, T. W. Kao, P. Fan, C. L. Lee and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp. 746–757, 2008. Article (CrossRef Link)
[20] S. A. Parah, J. A. Sheikh, N. A. Loan and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Digital Signal Processing*, vol. 53, pp. 11–24, 2016. Article (CrossRef Link)
[21] C. Kavitha and S. Sakthivel, "An effective mechanism for medical images authentication using quick response code," *Cluster Computing*, pp. 1–8, 2018. Article (CrossRef Link)
[22] F. Rahimi and H. Rabbani, "A dual adaptive watermarking scheme in contourlet domain for DICOM images," *Biomedical Engineering Online*, vol. 10, no. 1, pp. 53, 2011. Article (CrossRef Link)
[23] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake and H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging," *Signal, Image and Video Processing*, vol. 9, no. 5, pp. 1163–1178, 2015. Article (CrossRef Link)
[24] M. S. Wang and W. C. Chen, "Robust copyright protection scheme based on discrete cosine

transform and secret sharing techniques," *Journal of Electronic Imaging*, vol. 17, no. 2, pp. 023006, 2008. Article (CrossRef Link)
[25] S. Rawat and B. Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," *Signal Processing*, vol. 92, no. 6, pp. 1480–1491, 2012. Article (CrossRef Link)
[26] T. M. Thanh and K. Tanaka, "An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13455–13471, 2017. Article (CrossRef Link)
[27] T. Amiri and M. E. Moghaddam, "A new visual cryptography based watermarking scheme using DWT and SIFT for multiple cover images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8527–8543, 2016. Article (CrossRef Link)
[28] J. Dong and J. Li, "A robust zero-watermarking algorithm for encrypted medical images in the DWT-DFT encrypted domain," in *Innov. in Med. Healthc.*, pp. 197–208, 2016. Article (CrossRef Link)
[29] Z. Shao, Y. Shang, R. Zeng, H. Shu, G. Coatrieux and J. Wu, "Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography," *Signal Processing: Image Communication*, vol. 48, pp. 12–21, 2016. Article (CrossRef Link)
[30] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Applied Soft Computing*, vol. 13, no. 2, pp. 1170–1182, 2013. Article (CrossRef Link)
[31] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology-EuroCrypt94, Lect. Notes in Comput. Sci.*, vol. 950, pp. 1–12, 1995. Article (CrossRef Link)
[32] H. C. Chao and T. Y. Fan, "XOR-based progressive visual secret sharing using generalized random grids," *Displays*, vol. 49, pp. 6–15, 2017. Article (CrossRef Link)
[33] G. Voyatzis and I. Pitas, "Digital image watermarking using mixing systems," *Computer & Graphics*, vol. 22, no. 4, pp. 405–416, 1998. Article (CrossRef Link)



Tzuo-Yau Fan received the B.S. and M.S. degrees, both in Department of Computer Science and Information Engineering, from Ming Chuan University, Taoyuan, Taiwan, in 2008 and 2010, respectively. He is currently a Ph.D. student of Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. His research interests are in the area of image processing, digital signal processing, and computer vision.

Her-Chang Chao received the B.S. degree and Ph.D. degree, both in electronic engineering, from National Taiwan University of Science and Technology, Taipei, Taiwan, in 1991 and 1998 respectively. He is now Associate Professor at the Department of Computer Science and Information Engineering, Ming Chuan University, Taoyuan, Taiwan. His research interests are in the area of image processing, digital signal processing, multimedia information security, data hiding, digital watermark, and computer vision.

Bin-Chang Chieu received the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, U.S.A., in 1989. He is now Professor at the Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan. His current research interests are in image processing, digital signal processing, neural networks, and computer vision.