Original Article

A Highly Robust Medical Image Watermarking Method for Medical Real-time Applications

Mahdi Mehrabi[1], Vahdi Zarei[1], Mohammad Ghanbari[2]

[1]Department of Computer Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran, [2]School of Computer Science and Electronic Engineering University of Essex Colchester, UK

Abstract

Background: Watermarking such as other security concepts is an ongoing challenging research issue, especially for medical images, to protect patient privacy. Medical images need to be shared and transferred between hospitals and specialists as quickly as possible for better diagnosis. Fast and simple watermarking is needed as well as the robust transferring of channel noise, such as salt and pepper noise and robust cropping that may occur from specialists and signature encryption for patient privacy. **Methods:** In this article, a highly robust and simple watermarking method is introduced. The proposed method has very low computational complexity and at the same time, it is very robust to interference and uses simple computations such as (XORs) Exclusive ORs and rotations that can be done in real-time. The proposed method uses a combination of hidden neighboring signature information, Sudoku permutation, and noise pre-processing to achieve high robustness against salt and pepper noise and cropping. Simple signature encryption is also used. **Results:** The proposed method is examined in different medical image datasets. The experimental results indicate the proposed watermarking system is robust to salt and pepper noise density of up to 90% and about 70% cropping. The number of computations including encryption is five XOR per pixel and a rotation per block of signature size. **Conclusion:** A novel method for medical image watermarking is presented. The proposed method is in the spatial domain, has encryption, and uses only XOR computation. The proposed method is highly robust to noise and cropping which is necessary for medical uses. The proposed method can be used efficiently for real-time watermarking for medical and nonmedical image datasets.

Keywords: *Image crop noise, medical image watermarking, real-time watermarking, robust watermarking, salt and pepper noise*

Submitted: 01-Feb-2022 **Revised:** 15-Sep-2022 **Accepted:** 14-Mar-2023 **Published:** 12-Jul-2023

Introduction

Recently, widespread diseases like the COVID-19 pandemic increased the need for telemedicine, teleradiology, telediagnosis, and teleconsultation. Many of these medical technologies share and transfer medical information such as digital medical images between hospitals, specialists, or even patients to a specialist. When handling a person's document such as its medical image illegal copying, tampering or alerting digital images, and other security concepts need more attention.[1-3] Tampering and copyright protection are two challenging security issues for digital images. A common solution is image watermarking. Watermarking means hiding or embedding information such as a watermark (or signature) in a cover image (or carrier). Watermarking such as security concepts is an ongoing research issue.[4-7]

Medical image watermarking has no difference from public image watermarking, but there are some requirements and considerations in medical image watermarking. As indicated by Nyeem *et al.*,[8] encryption for privacy, robustness to noise and cropping, and low computational cost are some requirements of medical image watermarking. Salt and pepper noise may occur in medical images during transmission, faulty memory locations in hardware, and channel decoder damage.[9] Furthermore, cropping may be caused by a specialist to the bold or region of interest from other regions.[10] On the other hand, since time is critical in health systems, most medical applications need real-time algorithms. As a result, robust and not too complex watermarking methods are desired for medical images.

Address for correspondence:
Dr. Mahdi Mehrabi,
Department of Computer Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran.
E-mail: mahdi.mehrabi@iau.ac.ir; std.mehrabi@gmail.com

Access this article online

Website: www.jmssjournal.net

DOI: 10.4103/jmss.jmss_15_22

Quick Response Code:

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

For reprints contact: WKHLRPMedknow_reprints@wolterskluwer.com

How to cite this article: Mehrabi M, Zarei V, Ghanbari M. A highly robust medical image watermarking method for medical real-time applications. J Med Sign Sens 2023;13:199-207.

Historically, image watermarking techniques are carried out in the spatial domain. In this domain, data is embedded in pixels, blocks, bit streams, or code values.[11-19] In these methods, the signature (watermark) is embedded in the one to three least significant bits (LSBs) of pixels in a block. They may use pre-processing like hash or block processing. Spatial domain watermarking techniques are simple but are not very robust. Hence, transform domain watermarking techniques are introduced. Transform domain watermarking techniques are more complex but mostly robust.[20-26] In these methods, the signature is embedded in the transform of the cover image. Discrete wavelet transform (DWT), contourlet transform (CT), and discrete cosine transform are widely used in these approaches. As watermarking in frequency domains are robust they are more complex than spatial domain watermarking, some researchers attempted to design simple robust watermarking.[27-29] On the other hand, some research considers techniques that somehow fall between spatial and transform domains to benefit from both.[30-32]

In this article, a highly robust watermarking with low complexity method is proposed which can be used for real-time watermarking of medical or even nonmedical images. The proposed method uses a new strategy to use Sudoku permutation to tackle cropping attacks, and a novel approach to achieve robustness to salt and pepper noise by embedding neighboring signature information and preprocessing the cover image. Furthermore, the proposed method is simple and just uses XORs and rotations which made it suitable for real-time medical applications.

Subjects and Methods

Data and metrics

For evaluation, we used five medical image datasets as cover images.[9,34-36] The specifications of these datasets are mentioned in Table 1. We also used a public image dataset including famous images such as Avon, Baboon, Barbara, Birds, Boat, Bridge, Frymire, Girl, Goldhill, Lena, Monarch, Peppers, and Tulips. Signature images are binary images with 32 × 32, 64 × 64, and 128 × 128 pixels sizes. Furthermore different metrics and image quality assessment (IQM) are used for the evaluation and comparison of the proposed method. Peak signal-to-noise ratio (PSNR) and structural similarity index metric (SSIM) measure the effect of inserting a watermark in the cover image as the quality of the watermarked image. Normal cross correlation (NCC) measures the quality of the watermark extracted from the watermarked image, especially after attacking the watermarked image.[9,24,33] Increased PSNR, SSIM, and NCC mean better watermarking and robustness, respectively.

Table 1: Used cover image datasets

Dataset name	Content	Size	Format
DB. 1[9]	Medicine, CR	1760×1760 and over	DICOM
DB. 2[35]	Medicine, CT	512×512	DICOM
DB. 3[9]	Medicine, SC	1024×1024	DICOM
DB. 4[34]	Medicine, mixed	Mixed	Mixed
DB. 5[36]	Medicine, X-ray	299×299	PNG
DB. 6[9]	Public	512×512 and over	PNG

DB – Database; CT – Computerized Tomography, CR – Computed Radiography, DICOM – Digital Imaging and Communications in Medicine, PNG – Portable Network Graphic, SC – Scanned Chest

Embedding procedure

It is considered that both cover and signature images have rectangular dimensions, and the cover image is 4 × k (k = 1, 2,…) times greater than the signature. However, this condition may be reached by down-sampling or up-sampling the signature. A signature is a binary image or logo. The embedding procedure has three steps which are explained in the following steps.

Step 1

The first step to tackling salt and pepper noise is pre-processing. As salt and pepper noise changes pixel values to the lowest or highest ones (0 or 1), to distinguish pixels with these values from noisy ones, an addition/subtraction is carried out as in Eq. 1. If a pixel is corrupted by an attack, the signature is extracted from neighbors or distributed by Sudoku.

$$C_p(x,y) = \begin{cases} 2^n - 3 & \text{if } C(x,y) = (2^n - 1) \text{ or } (2^n - 2) \\ 2 & \text{if } C(x,y) = 0 \text{ or } 1 \\ C(x,y) & \text{otherwise} \end{cases} \quad (1)$$

Where in Eq. 1, $C\ (x,\ y)$ is the input cover image pixel and $C_p\ (x,\ y)$ is a pixel of the pre-processed cover image outputted from step one and n is the pixel bit depth.

Step 2

in this step robustness to cropping is considered and designed. To achieve robustness cropping a Sudoku puzzle-based permutation for embedding the signature is carried out. A Sudoku puzzle consists of the N × N grid of cells partitioned into N regions. Each region consists of N cells and must be filled in using a set of N distinct symbols. Sudoku enforces evenly spread numbers or symbols across the puzzle cells. A digit/symbol is assigned to each cell in the grid such that a given digit/symbol cannot appear twice in a row, in a column, or a region. Here the Sudoku puzzle is the cover image blocks and the signature represents the symbols and N is set to 4 (can be extended to more than 4). The cover image is arranged into 4 × 4 puzzles and four groups of blocks B (1) to B (4) are made while each group contains one kind of symbol or signature. The blocks in each group are selected in the cover image based on Sudoku as depicted in Figure 1a and b and shows the group of blocks with their row index in which B (k)(m) indicates block group k located in row m.

Sudoku-based block arrangement enforces evenly spread blocks of groups and spread signature across the cover image. This weakens the chance of corrupting the signature embedded in a group by cropping a region. For generating four different symbols or signatures, the original signature is rotated four times as in Eq. 2.

S (k)(1) = Rotate (S, (k-1) ×90) k = 1, 2, 3, 4. (2)

Where in Eq. 2, S is the original signature, S (k)(l) is the k-th rotated signature or symbol, and Rotate (x, y) is the rotating function that rotates matrix x by y degrees.

Now, four symbols or signatures say S(k)(1) for k = 1-4 are generated that will be embedded in four block groups in Figure 1a. To distinguish blocks of four groups in different rows the same notation and index as in Figure 1b is used for signatures such that S(k)(m) is the signature that will be embedded in block B(k)(m) in Figure 1b. However, it is worth noting that signatures S(k)(m) for the same k and m = 1-4 are the same version of the signature and so we use S(k)(m) as the k-th signature or rotated signature.

Step 3

In this step encryption and embedding four rotated signatures is proposed. The signature is embedded in the cover block pixel by pixel. As mentioned in the previous step, there are four groups of blocks say B(k)(m) (k = 1-4) and four rotated signatures say S(k)(m) (k = 1-4). Embedding in three groups are the same but the fourth is different. The rotated signature is first encrypted by a key and each bit (pixel) of it is embedded in the LSBs of the cover image pixels. Encryption is simple XOR of the rotated signature binary pixels by key bits. The key may be selected randomly, but we chose the second LSBs of the cover image pixels as the key values. Considering the k-th rotated signature image as S(k)(m), cover image block as B(k)(m), and output of encryption SE(k)(m), encryption can be formulated by Eq. 3.

SE(k)(m)(x, y) = (b[LSB-1]B(k)(m)(x, y)) XOR (S(k)(m)(x, y)) k, m = 1, 2, 3, 4. (3)

Where in Eq. 3, b[LSB-1]B(k)(m)(x, y), is the 2nd LSB bit of the binary form of B(k)(m)(x, y).

After encryption, the encrypted signatures SE(k)(m) are embedded in the cover image blocks. Each pixel of the encrypted signature (which is a bit) is embedded in the LSB of the corresponding pixel of the cover image block. The embedding is formulated in Eq. 4.

$$b_iW(k)(m)(x,y) = \begin{cases} SE(k)(m)(x,y) & if\ i == LSB \\ b_iB(k)(m)(x,y) & otherwise \end{cases} \qquad (4)$$

$$for\ k = 1,2,3, m = 1to4$$

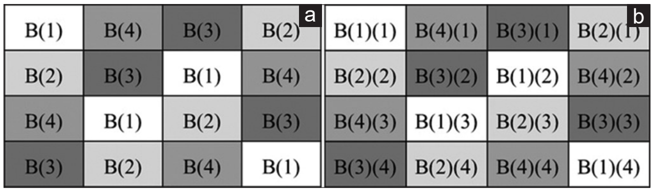
Where in Eq. 4 $b_iW(k)(m)(x, y)$ is i-th bit of output watermarked.

The embedding in the fourth group of blocks is like other groups but with a slight difference. The pixels of these blocks are not only embedding the corresponding signature pixels as before, but they also embed some information about neighboring signature pixels. This helps when pixels are corrupted by any attack, their signature may be extracted from its neighbors. If S(4)(m)(x, y) is a pixel of the signature S(4)(m) generated by (2) for the fourth group, its neighbors are S(4)(m)(x-1, y), S(4)(m)(x, y-1), S(4)(m)(x + 1, y), and S(4)(m)(x, y + 1). The pixels of S(4)(m) for each block of the fourth group deal with one neighboring position as illustrated in Figure 2 based on their block position in the group. It means each pixel embeds information of a neighbor where its block is available for all pixels. The signature pixel is first XORed with one of its neighbors as illustrated in Figure 2. In Figure 2a, blocks of the fourth group are marked as B(4)(1), B(4)(2), B(4)(3) and B(4)(4). Figure 2b shows a pixel of S(4)(m) and its neighbors marked as S(4)(m)(x, y), S(4)(m)(x-1, y), S(4)(m)(x, y-1) S(4)(m)(x + 1, y), and S(4)(m)(x, y + 1). Each pixel is first XORed with its neighboring pixels to make a new set of signatures that will be embedded in B(4)(i). This procedure is formulated in Eq. 5.

S`(4)(m)(x, y) =S(4)(m)(x, y) XOR S (4)(m)(x-((-1)^m) × (((m-1)%3 + 1)/2), y-((-1)^m) × (m%3%2)) m = 1, 2, 3, 4. (5)

Where in Eq. 5, S`(4)(m)(x, y) is a new signature pixel embedded in its neighbor's information, S(4)(m)(x, y) is the pixel of signature S(4)(m), "%" represents integer division reminder, "×" means integer multiply, and "/" means integer division. Each signature S`(4)(m) (m = 1-4) is then encrypted and embedded in the fourth group block B(4)(m) as other groups explained before as indicated in (2) and (4).

Table 2 summarizes the embedding procedure as pseudo code or algorithm. In this algorithm, *Sudpm* is a Sudoku permutation matrix in which its elements *Sudpm (x, y)*



B(1)	B(4)	B(3)	B(2)
B(2)	B(3)	B(1)	B(4)
B(4)	B(1)	B(2)	B(3)
B(3)	B(2)	B(4)	B(1)

B(1)(1)	B(4)(1)	B(3)(1)	B(2)(1)
B(2)(2)	B(3)(2)	B(1)(2)	B(4)(2)
B(4)(3)	B(1)(3)	B(2)(3)	B(3)(3)
B(3)(4)	B(2)(4)	B(4)(4)	B(1)(4)

Figure 1: (a) Block groups based on sudoku permutation, (b) block group with row index

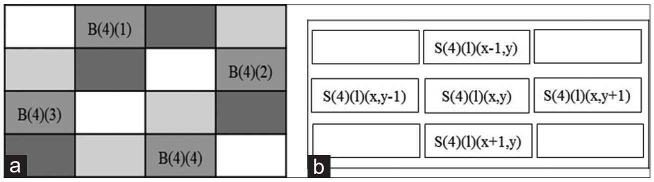


Figure 2: (a) Four blocks in group 4, (b) A signature pixel *S(4)(m)(x, y)* and its neighbours

Table 2: Watermark embedding pseudo code of the proposed method

```
//Input: Signature matrix 'S', cover image matrix 'C'
//Output: Watermarked image 'W'
//Matrix indices starts by 1
//Comments starts by '//'
//Preprocessing
For all x, y in range of pixels of C
{
Changing the pixels C (x, y) that are close to noise values
}
//Making new signature
For k=1:4
{
Rotating signature S to make new signature S (k) based on Eq. 2
}
//Embedding neighbors information for group 4
For all x, y in range of signature pixels
For m=1:4
Embed signature in Group 4 of blocks S (4) (m) (x, y) based on Eq. 5
//encryption and embedding to remaining blocks
For all x, y in range of cover pixels C
Embed signature based on Eq. 3 and 4
```

define the symbol or group block number in the x^{th} row and y^{th} column of Sudoku defined in Figure 1a.

Signature extraction

The proposed signature extraction is a no-reference method and is carried out in four phases. In each phase, several signature pixels are extracted. First, S(x, y) is considered as the pixel in position x (x-th row) and y (y-th column) of the signature, and all signature pixels get a value Eq. 2. Value 2 means they are not extracted. During extraction, if a pixel is detected as corrupted due to an attack or noise it is marked with a value equal to 3. Since in the first step of an embedding procedure all cover image pixels are tuned to not be 2n-1 or 0, if a watermarked image pixel takes these values it is considered corrupted and its embedded signature is marked as 3. Since the signature is a binary image, its pixels may be zero or one and during the signature extraction in each phase, several pixels are detected and take values of zero or one. The extraction continues until there is no pixel with values 2 and 3. The extraction phases are as follows.

Phase 1

Pre-processing: First of all, the cover image is partitioned into blocks and labeled as B(1)(m) to B(4)(m) belonging to groups 1-4 as depicted in Figure 1, where m is the row index. The embedded signature in each group is k × 90° rotated signature compared to the signature embedded in other groups. To have the same signature in different blocks, the blocks in each group are rotated back by 90° based on their group number as in Eq. 6.

B`(k)(m) = Rotate(B(k)(m),-(k-1) ×90) k = 1, 2, 3, 4 m = 1-4. (6)

In Eq. 6, B(k)(m) is a block of group k in row m in Figure 1, B`(k)(m) is a rotated block of group k and Rotate(x, y) is the rotation function that rotates matrix x by y degrees. After rotating each group every pixel of blocks B`(1)(m) to B`(4)(m) at the same positions contain information about the same pixels of signature.

Phase 2

In this phase, the uncorrupted signature pixels are extracted. To do this, block groups 1-3 say B`(1)(m) to B`(3)(m) are processed. Based on step one in embedding, pixel values attacked by salt and pepper and noise are changed to zero or one (highest or lowest pixel value). The signature pixel S (x, y) is extracted from any pixel B`(1)(m)(x, y) to B`(3)(m)(x, y) if one of them is not zero or one, otherwise, it is marked as value 3 or corrupted. The extraction including decryption is formulated in Eq. 7.

$$S(x,y)=\begin{cases} =3 \\ \quad if\ all\ B`(k)(m)(x,y)=0\ or\ 2^n-1 \\ \quad for\ all\ k,m=1\ to\ 3 \\ =b_{LSB}B`(k)(m)(x,y)\ XOR\ \ b_{LSB\text{-}1}B`(k) \\ \quad (m)(x,y)\ elsewhere \end{cases} \tag{7}$$

Where in Eq. 7 *b_{LSB}B`(k)(m)(x, y)* is the LSB bit of pixel *B`(k)(m)(x, y)* of block *B`(k)(m)*, and k is the group number.

Phase 3

In this phase signatures from corrupted pixels are extracted when at least one of their neighbors is uncorrupted. The corrupted pixels are marked as 3 in the previous phase. If one of the neighbors of those pixels in the position depicted in Figure 2a is not corrupted by attack or noise, the signature can be extracted from cover image blocks in group 4. This is because the signature in group 4 is encrypted and embedded with the neighbors' information as in Eq. 5. Using Figure 2a, if S(x, y) is a corrupted signature or pixel, based on embedding in group four and which the neighboring signature S(x ± 1, y ± 1) has not been corrupted, the signature is extracted from blocks B(4)(m) in Figure 2b. Using the notion in Figure 2a, the extraction including decryption is formulated in Eq. 8.

S(x, y) = B_{LSB}`(4)(m)(x, y) XOR $B_{LSB}$`(4)(m)(x, y) XOR S(x+ ((-1)^m) × (m%3%2), y+ ((-1)^m) × (((m-1)%3 + 1)/2) if B`(4)(m)(x, y) and S(x+ ((-1)^m) × (m%3%2) is available for any m = 1, 2, 3, 4. (8)

Where in Eq. 8: B` is block B in Figure 2 changed to B` by Eq. (6), B`(i)(j)(x, y) represent pixel row *x* and column *y* in bock B with index *i* and *j* in Figure 3, $B_{LSB}$`(4)(m)

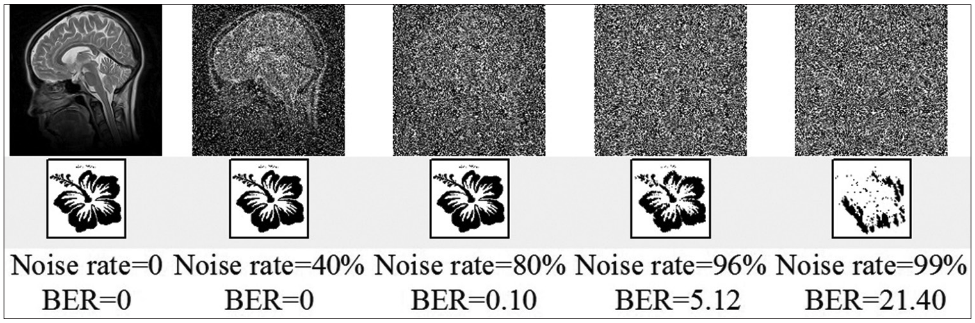


Figure 3: Robustness of the proposed method: from top row 1 watermarked noisy image, row 2 noise density rate, row 3 extracted signature, row 4 metrics for extracted signature

represents the LSB bit of block B`(4)(m), or cover image pixel, k is row index in Figure 2, “x^y” represent *x* power to *y*, “%” integer division remainder.

Phase 4

In previous phases extract signature pixels embed in cover image pixels that are not corrupted or at least one of its neighbors is not corrupted. In this phase signatures not extracted in the previous phases and marked as 3 are extracted by a statistical approach. The main idea is that a missed signature pixel can be predicted by the local and global distribution of signature pixels.

At first, MP is set to the majority of signature pixels extracted up to now, if the majority of the extracted signature pixels are 1 then MP = 1 and MP = 0 otherwise. For the signature pixels marked as 3 and not extracted in the previous phases, it is assigned to the most frequent bit in its eight surrounding neighbors as in Eq. 9.

$$S\left(x,y\right)=\begin{cases}1 & if\,freqN==1\\ 0 & if\,freqN==0\\ MP & otherwise\end{cases} \tag{9}$$

Where in Eq. 9, freqN is the most frequent signature pixel in 8 neighbors of S(x, y).

Table 3 summarizes the extraction procedure of the proposed method as a pseudo code or algorithm. Input is watermarked image *W* and output is signature *S*. *Sudpm* which is a permutation matrix as in Table 2, functions *zerosOf (S)* and *onesOf (S)* return the number of zeros and ones from matrix *S* respectively.

Results

In the first experiment the proposed method is used to embed signatures into all dataset images and the average quality of watermarked images are measured by PSNR and SSIM. The results are tabulated in Table 4.

The robustness of the proposed method against salt and pepper noise and cropping attacks are also evaluated. First, salt and pepper noise with different densities is applied to a watermarked image and then the signature is extracted. A sample of watermarked images by the

Table 3: Watermark extraction pseudo code of the proposed method

```
/Input: watermarked image matrix ‘C’
//Output: signature image matrix ‘S’
//Comments starts by ‘//’
//Permutation matrix
Sudpm=[1 4 3 2; 2 3 1 4; 4 1 2 3; 3 2 4 1]
//Initilizing signature S
For all x, y in range of Signature pixels
S (x, y)=3
//Mapping watermarked image to group blocks based on permutation matrix
For all x, y in range of watermarked image pixels
B (x/4+1) (sudpm (x/4+1) (y/4+1)) (x/4+1, y/4+1)=C (x, y)
//Rotating groups
For all k=1:4, m=1:4
B` (k) (m)=Rotate (B (k) (m), −(k−1)×90)
//Extracting signature pixels from group 1:3
For all x, y in range of signarure pixels
For k=1:3, m=1:3
If B (k) (m) (x, y)!=0 and B (k) (m) (x, y)!=$2^{n-1}$
{
Extract S (x, y) based on Eq. 7
}
//Extracting not extracted signature pixles from group 4
For all x, y in range of signature pixels
If S (x, y)==3
For m=1:4
If S (x + $((-1)^{m})$×(m% 3% 2), y + $((-1)^{m})$×(((m−1)%3+1)/2))!=3
If B`(4) (m) (x, y)!=0 AND B`(4) (m) (x, y)!=$2^{n-1}$
{
Extract S (x, y) based on Eq. 8
}
//Calculating MP
If ones of (S) > zeros of (S)
MP=1
Else
MP=0
For all x, y in range of signature pixels
If S (x, y)==3
{
Calculate S (x, y) based on Eq. 9
}
```

proposed method and corrupted by noise at different densities and their extracted signatures are illustrated in Figure 3. The robustness of the proposed method against salt and pepper noise is summarized in Table 5 as the maximum noise density of the proposed method can extract signature with NCC >0.99 and averaged over different datasets. The robustness of the proposed method was also evaluated against cropping attacks. For this purpose, the watermarked image is cropped by different kinds and different amounts, then the signature is extracted. The better-extracted signature, the more robust watermarking. Center Crop, Inverse (Inv.) Center Crop, Left/Right Edge Crop, and Corner (Cor.) Crops are different kinds of cropping attack that is applied to watermarked image. The NCC of extracted signatures is calculated as metr for robustness evaluation. The results of the proposed method for a sample DICOM image are depicted in Table 6. The samples of cropped watermarked images and extracted signatures are illustrated in Figure 4.

The quality of watermarking with the proposed method is also compared with the other recent robust methods in medical and public image datasets. The proposed method was compared with the methods by Su and Chen,[30] Ranjbar *et al*.,[23] and Etemad *et al*.[32] The results for public image datasets cover images are listed in Table 7.

Table 8 also reports the comparison of the proposed method with Vaidya.[29] This method converts the cover image to a lifting wavelet transform and then uses a DWT. Since transform domain robustness is poor, the method also uses the local binary pattern (LBP) of the cover image to produce an embedding factor. The watermark embeds in a transformed image based on the embedding factor. The combination of two transformations and LBP impose high complexity but makes the method robust. In Table 8, DB.4 is used as a cover image. The quality of watermarked images as PSNR and SSIM, and NCCs of extracted watermarks when watermarked images are attacked by different noise and crop are reported in Table 8.

Table 4: Average quality of watermarked image dataset by the proposed method

Dataset	PSNR (db)	SSIM	Signature size
DB. 1	115.9954	0.99999998	64×64
DB. 2	103.4837	0.99999788	64×64
DB. 3	105.5136	0.99999979	64×64
DB. 4	100.4427	0.99999841	64×64
DB. 5	96.4513	0.99999835	64×64
DB. 6	51.4550	0.99621428	128×128

DB – Database; PSNR – Peak signal-to-noise ratio; SSIM – Structural similarity index metric

Table 5: Robustness of the proposed method as maximum noise density to have normal cross correlation >0.99

Dataset	Salt and pepper noise density (%)
DB. 1	76
DB. 2	76
DB. 3	76
DB. 4	76
DB. 5	76
DB. 6	80

DB – Database

The proposed method is also compared with Zermi *et al*.[28] This method is in the transform domain and uses DWT to embed watermark; but to achieve robustness, it combined DWT with singular value decomposition. By this combination, it achieves a broad range of robustness but not high robustness. Table 9 reports the quality of watermarked images in terms of PSNR and SSIM for both methods when using DB.2 and DB.5 as cover images. The robustness of both methods is also compared in Table 10 as the NCC of extracted signatures.

Discussion

Medical image watermarking needs encryption for privacy, low-quality degradation, robustness to noise and cropping,

Table 6: Robustness of the proposed method against different cropping for 128×128 signature

Crop type	Crop percent	NCC
Center Crop 64	1.56	1
Center Crop 384	56.25	1
Center Crop 448	76.56	0.93
Inverse Center Crop 64	98.44	0.82
Inverse Center Crop 128	93.75	0.94
Inverse Center Crop 192	85.94	0.99
Inverse Center Crop 256	75.00	1
Inverse Center Crop 448	23.44	1
Inverse Left Corner Crop 64	98.44	0.85
Inverse Left Corner Crop 192	85.94	1
Inverse Left Corner Crop 448	23.44	1
Left Edge Crop 512×64	12.50	1
Left Edge Crop 512×320	62.50	1
Left Edge Crop 512×384	75.00	1

NCC – Normal cross correlation

Table 7: Quality comparison of watermarked public cover images by different methods

Method	Avion	Baboon	Lena	Peppers
	PSNR (dB)	PSNR (dB)	PSNR (dB)	PSNR (dB)
Su, Q. *et al*.[30]	49.86	49.89	49.98	50.08
Ranjbar, *et al*.[23]	35.95	38.16	38.72	38.95
Etemad *et al*.[32]	Not reported	48.25	48.99	48.35
Proposed method	51.16	51.16	51.15	52.9

DB – Database; PSNR – Peak signal-to-noise ratio

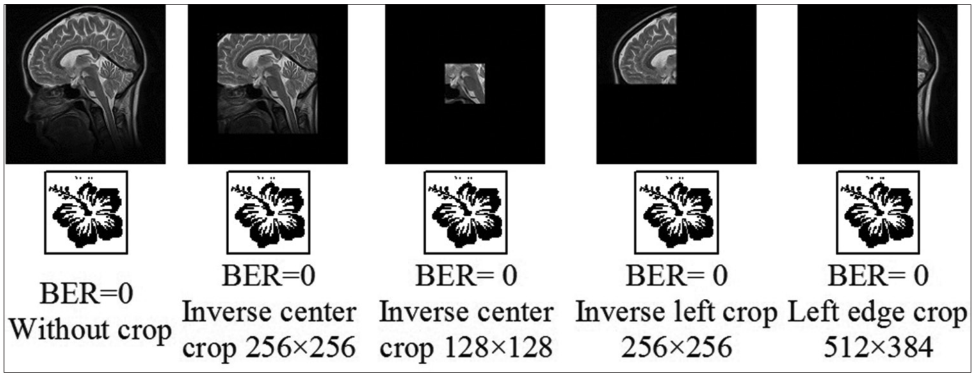


Figure 4: Robustness of the proposed method against cropping, from top: row one is cropped watermarked images with different, row two is signature extracted from above cropped watermarked image, row three is BERs of extracted signature and last row kind of cropping. BERs: Bit Error Rates

Table 8: Quality comparison of watermarked database 4 cover images

Watermarking method	PSNR (without attack)	SSIM (without attack)	NCC (1% salt and pepper attack)	NCC (2% salt and pepper attack)	NCC (10% cropping attack)
S.Prasanth Vaidya 1[29]	35.61	0.91	0.98	0.97	0.94
Proposed method	46.28	0.98	1	1	1

PSNR – Peak signal-to-noise ratio; NCC – Normal cross correlation; SSIM – Structural similarity index metric

Table 9: Quality comparison of different watermarked database

Watermarking method	PSNR (DB.2)	SSIM (DB 2)	PSNR (DB.5)	SSIM (DB.5)
Zermi *et al*.[28]	55.85	0.9997	57.04	0.9998
Proposed method	83.57	0.9985	51.39	0.9885

DB – Database; PSNR – Peak signal-to-noise ratio; SSIM – Structural similarity index metric

Table 10: Quality comparison of extracted signature as normal cross correlation

Watermarking method	2% salt and pepper	10% salt and pepper	25% cropping	50% cropping
Zermi *et al*.[28] DB.2	0.9549	0.9461	0.8906	0.6529
Proposed method DB.2	1	1	1	1
Zermi *et al*.[28] DB.5	0.9816	0.9517	0.7635	0.6035
Proposed method DB.5	1	1	1	1

and low computational cost. Spatial domain watermarking has low computation but is not very robust. In contrast, frequency-domain watermarking is robust but imposes more computations and complexity. The proposed watermarking method is designed in the spatial domain such that it can achieve robustness. On the other hand, a simple encryption is used but can be extended.

Different medical image datasets and public images are used to test the goals. The test results of proposed watermarking method indicates that it can embed a signature in a medical image with very low degradation of the cover image as depicted in Table 4. Furthermore, it has a superior quality compared to other robust medical images watermarking methods as depicted in Tables 7-10.

Robustness tests were carried out against salt and pepper attacks and cropping attacks which may occur in medical applications. The results as depicted in Table 5 indicate that with the proposed watermarking method, signatures can be extracted with very high quality in different metrics from watermarked images corrupted by noise with up to 70% densities. The highest noise density the proposed method can resist is 90%. The proposed method outperforms robust medical image watermarking methods in salt and pepper noise indicated in Tables 8 and 9.

The proposed method was also tested under different cropping attacks. The results reveal the proposed method is highly robust to any cropping applied to watermarked images. While other robust medical image watermarking methods in Table 10 have degraded performance, the proposed method has no degradation.

The main computational complexity of the proposed method includes only XORs and rotation. The number of XORs for embedding and extraction procedures is only 5 per pixel. The rotations can be done by memory mapping. Since there are no algebraic operations like add and multiply or divide, and the number of simple XORs is not heavy operations, the proposed method could be done easily in a real-time manner.

Conclusion

Medical image watermarking needs robustness, encryption, and a low computational cost. While spatial watermarking methods are simple and not robust, transform domain watermarking methods are robust but complex. We designed a spatial domain robust medical image watermarking method in this paper. The proposed method uses a novel embedding of signatures in pixel neighbors, a new strategy of Sudoku permutation for embedding, along with a simple encryption algorithm that is highly robust against salt and pepper noise and cropping attacks which are common in medical images. The experimental results show that the proposed method is robust to salt and pepper noise density to up to 90% and also robust to about 70% cropping and outperforms almost all the known robust medical image watermarking methods in terms of various quality metrics such as PSNR, SSIM, and NCC. The proposed method uses simple and low operations that can be easily afforded in the real-time applications.

Financial support and sponsorship

None.

Conflicts of interest

There are no conflicts of interest.

References

1. Mata-Mendoza D, Cedillo-Hernandez M, Garcia-Ugalde F, Cedillo-Hernandez A, Nakano-Miyatake M, Perez-Meana H. Secured telemedicine of medical imaging based on dual robust watermarking. The Visual Computer. 2022;38:2073-90.
2. Zheng L, Zhang Y, Thing VL. A survey on image tampering and its detection in real-world photos. J Vis Commun Image Represent 2019;58:380-99.
3. Atta R, Ghanbari M. A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set. J Vis Commun Image Represent 2018;53:42-54.
4. Singh OP, Singh AK, Srivastava G, Kumar N. Image watermarking using soft computing techniques: A comprehensive survey. Multimed Tools Appl 2021;80:30367-98.
5. Kumar S, Singh BK, Yadav M. A recent survey on multimedia and database watermarking. Multimed Tools Appl 2020;79:20149-97.
6. Anand A, Singh AK. Watermarking techniques for medical data authentication: A survey. Multimed Tools Appl 2021;80:30165-97.
7. Agarwal N, Singh AK, Singh PK. Survey of robust and imperceptible watermarking. Multimed Tools Appl 2019;78:8603-33.
8. Nyeem H, Boles W, Boyd C. A review of medical image watermarking requirements for teleradiology. J Digit Imaging 2013;26:326-43.
9. Mousavi SM, Naghsh A, Manaf AA, Abu-Bakar SA. A robust medical image watermarking against salt and pepper noise for brain MRI images. Multimed Tools Appl 2017;76:10313-42.
10. Mousavi SM, Naghsh A, Abu-Bakar SA. A Heuristic Automatic and Robust ROI Detection Method for Medical Image Warermarking. J Digit Imaging 2015;28:417-27.
11. Lin PL, Hsieh CK, Huang PW. A hierarchical digital watermarking method for image tamper detection and recovery. Pattern Recognit 2005;38:2519-29.
12. Shivani S. Verifiable medical images for E-healthcare: A novel watermarking approach using robust bit-wise association of self-mutating offsprings of pixels. Microprocess Microsyst 2022;90:104483.
13. Xiao D, Shih FY. An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing. Optics Commun 2012;285:2596-606.
14. Chen F, He H, Tai HM, Wang H. Chaos-based self-embedding fragile watermarking with flexible watermark payload. Multimed Tools Appl 2014;72:41-56.
15. Zhang X, Wang S. Statistical fragile watermarking capable of locating individual tampered pixels. IEEE Signal Process Lett 2007;14:727-30.
16. Zhang X, Wang S. Fragile watermarking scheme using a hierarchical mechanism. Signal Process 2009;89:675-9.
17. Zhang X, Wang S, Qian Z, Feng G. Self-embedding watermark with flexible restoration quality. Multimed Tools Appl 2011;54:385-95.
18. Bravo-Solorio S, Nandi AK. Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities. Signal Process 2011;91:728-39.
19. Hsu CS, Tu SF. Probability-based tampering detection scheme for digital images. Optics Commun 2010;283:1737-43.
20. Kumar C, Singh AK, Kumar P. A recent survey on image watermarking techniques and its application in e-governance. Multimed Tools Appl 2018;77:3597-622.
21. Singh SP, Bhatnagar G. A new robust watermarking system in integer DCT domain. J Vis Commun Image Represent 2018;53:86-101.
22. Moad MS, Kafi MR, Khaldi A. Medical image watermarking for secure e-healthcare applications. Multimedia Tools and Applications. 2022. p.1-21.
23. Ranjbar S, Zargari F, Ghanbari M. A highly robust two-stage contourlet-based digital image watermarking method. Signal Process Image Commun 2013;28:1526-36.
24. Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM. Information hiding in medical images: A robust medical image watermarking system for E-healthcare. Multimed Tools Appl 2017;76:10599-633.
25. Sinhal R, Sharma S, Ansari IA, Bajaj V. Multipurpose medical image watermarking for effective security solutions. Multimed Tools Appl 2022;81:14045-63.
26. Singh P, Devi KJ, Thakkar HK, Kotecha K. Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. IEEE Access 2022;10:8974-93.
27. Rohith S, Bhat KH. A simple robust digital image watermarking against salt and pepper noise using repetition codes. Int J Signal Image Process 2012;3:47-54.
28. Zermi N, Khaldi A, Kafi MR, Kahlessenane F, Euschi S. Robust SVD-based schemes for medical image watermarking. Microprocess Microsyst 2021;84:104134.
29. Vaidya SP. Fingerprint-based robust medical image watermarking in hybrid transform. The Visual Computer. 2022. p.1-6.
30. Su Q, Chen B. Robust color image watermarking technique in the spatial domain. Soft Comput 2018;22:91-106.
31. Nayak MR, Bag J, Sarkar S, Sarkar SK. Hardware implementation of a novel water marking algorithm based on phase congruency and singular value decomposition technique. AEU Int J Electron Commun 2017;71:1-8.
32. Etemad E, Samavi S, Soroushmehr SR, Karimi N, Etemad M, Shirani S, *et al*. Robust image watermarking scheme using bit-plane of hadamard coefficients. Multimed Tools Appl 2018;77:2033-55.

33. Vidya MJ, Padmaja KV. Affirmation of electronic patient record through bio-electric signal for medical data encryption authenticity. In TENCON 2017-2017 IEEE Region 10 Conference 2017. p. 1332-1336. IEEE.
34. Makhanov S. Medical Record Database; 2020. Available from: https://www.onlinemedicalimages.com/index.php. [Last accessed on 2020 Oct 03].
35. Mader K. CT Images from Cancer Imaging Archive with Contrast and Patient Age. Available from: https://www.kaggle.com/kmader/siim-medical-images. [Last accessed on 2020 Nov 07].
36. Rahman T, Chowdhury M, Khandakar A. COVID-19 Chest X-ray Database. Available from: https://www.kaggle.com/tawsifurrahman/covid19-radiography-database. [Last accessed on 2020 Nov 22].