# HILBERT-LSB-C as Authentication System for Color Medical Images

Syifak Izhar Hisham
Faculty of Computer Science and Software Eng.
Universiti Malaysia Pahang
Gambang, Malaysia
penawar85@gmail.com

Nurul Wahidah Arshad
Faculty of Electrical and Electronics Eng.
Universiti Malaysia Pahang
Pekan, Malaysia
wahidah@ump.edu.my

Jasni Mohamad Zain
Faculty of Computer Science and Software Eng.
Universiti Malaysia Pahang
Gambang, Malaysia
jasni@ump.edu.my

Liew Siau-Chuin
Faculty of Computer Science and Software Eng.
Universiti Malaysia Pahang
Gambang, Malaysia
liewsc@ump.edu.my

***Abstract*—This paper proposes a new numbering method for a fragile watermarking algorithm aimed at improving color medical image watermarking. The proposed method uses Hilbert pattern numbering before watermarking operations such as parity bits check and comparison between average intensities as the authentication data. The authentication data embedded in the same host image are utilized to localize any tamper using block-wise approach. The method is very effective since it only requires a secret key and public, chaotic mixing algorithm to recover the attacked image. We use the Hilbert mapping approach, which is more compatible with medical image modalities, which is not only specifically to the square shape of image but applicable to all kinds and modalities of the image. We propose the algorithm to match the criterion of having 3 planes in a color image. The peak-signal-noise-ratio value of the proposed scheme is very good, achieving up to 56 decibelf.**

***Keywords—authentication; Hilbert; localization; security; recovery***

## I. INTRODUCTION

Authentication method is seen as very important in medical images. A study of [1] has reported that the evaluation method for medical image watermarking techniques should be more stringent than regular image watermarking. One of the reasons is the medical images are available in different sizes and modalities such as CT, MRI, and X-ray. A watermarking scheme for medical image should invisibly embed data in the image without changing its size or format. The watermarking scheme should also compatible to all modalities of medical images. Among the criterion that is focused in medical image watermarking is the importance of not changing the meaning of even one pixel to ensure no misdiagnosis happens.

A watermarking method is considered good if it survives after being attacked by various kinds of noise. Medical images usually degrade when transmission because of Gaussian noise. Therefore, when developing a new watermarking method, the requirement is to be robust against Gaussian noise and speckle noise.

Another requirement of a quality watermarking method is to solve the problem of vector quantization (VQ) counterfeiting attack and collage attack. One popular way is by breaking block-wise independence as proposed by [2].

Chang (2007) [3] claims that modification to some blocks would be done effortlessly if malicious attackers know the block-mapping sequence in advance, which in this case, when we use the typical raster pattern. Hung (2013) [4] also states that a unique scan pattern is known as a secure method of encryption for having great compression before embedding, which can be further investigated in this research whether it is also good in watermarking or not.

The block numbering process is seen as critical as it also decides the location of the embedded watermark data when mapping. With the probability of getting the tamper attack in the middle of medical image is high, a unique numbering system is seen as helpful to protect the region of interest in the middle [5]. However, as we aim to develop schemes that is compatible with all types of modalities, we cannot say that the region of interest (ROI) is definitely only in the middle. As an example, a scanned femur in MRI will has the ROI as from top to the bottom of the image as that part of a body is long.

Lin et. al [2] proposed the idea of embedding the recovery data of original block into another block in cover block. This is to separate the block independency, which can optimize the security of original data. The method is very efficient and time saving since it only uses two simple operations for authentication, which are parity bits check and average intensities comparison. The embedding space is three least-significant-bits (LSBs) in every bit of pixels. The detection process is based on a hierarchical structure which three times of checking are done. Based on the approach in [6] which using unique and random mapping using two-dimensional transformation, [2] used public chaotic mixing algorithm to recover tampered images.

978-1-4673-6722-6/15/$31.00 ©2015 IEEE

This work is a start to more researches in digital watermarking [7-13]. Zain et. al [7] improved the method by embedding the recovery data into the most least significant bit (LSB) since the focus was on medical images, which carry crucial information in every pixel. To avoid any perceptible issue, only one LSB used to store watermark data is good for grayscale digital image.

Lin et. al [11] proposed a watermarking scheme for color images which also based on block-wise mechanism [8]. The watermark data are inserted in two LSBs in each plane, red, green and blue (RGB). It does not go through any process of color space transformation. The watermark data are the mean of each block and the quantization of them. The recovery results are excellent.

Liu (2012) [12] proposed an improved block-wise watermarking, which is developed for color image [9].The authentication data are achieved by using a dual-option parity-check method and morphological operations. The recovery data are the feature information of the host color image and its corresponding block-edge-pattern information. The block-edge-pattern consists of the gradient of the intensity and the pattern index of the block. The $YC^bC_r$ color space is adopted for the proposed design since the color pixel in this space is separated by luminance and chrominance components, which makes the embedding easier. The results of detection and recovery for this scheme are very promising.

A technique which integrates the embedding, localizing and recovering functions have been proposed by [13] as an authentication watermarking using spiral manner mapping for grayscale images. The authentication data are parity bits and average intensities, enlightened by [2] and [7]. However, the new numbering method used, the spiral pattern before embedding shows the results of detection and recovery is much better than using sequence mapping. The peak-signal-noise-ratio (PSNR) value is high, up to 70 decibel (dB) and the operating time is very fast. It is able to recover the valid digital image from various types of attacks such as changes in the pixels, changes of colors, block removal and various filter attacks. However, the images to be watermarked are limited to square shape image.

According to the review done, many researches of image watermarking were developed for square shape images [9-13]. While in researches of medical image watermarking, popular images to be samples of watermarking research are grayscale ultrasound, grayscale CT and MRI [6, 8, 13, 14]. We see this as the limitations in watermarking.

In this paper, we propose an algorithm of watermarking as an improved modification of the existing numbering and embedding technique [13] to protect all shapes and all types of grayscale and color images. We develop Hilbert manner numbering to fully cover up the watermarking area in the image, and embed it to all planes of RGB to recover any tamper of color medical image successfully.

## II. The Proposed Scheme

Based on the issue related to this research indicated in the previous section, the following research diagrams in Fig. 1 and 2 has been planned for this research to improve the models from [2, 7, 14]. The objective of this research is to develop a new technique for authentication, which appropriate for all medical imaging modalities, grayscale and color images.

Due to that, the samples in this research are from various modalities, CT, MRI, PET, ultrasound, mammogram, DTI and simple X-ray images. All these samples have different qualities, sizes, height and width. Some of them are 8 bits and some are 16 bits. The type of images is bitmap. There are many medical scanners that move forward to produce color images, and due to that, a watermarking that can work with grayscale images and also color images is competent to be integrated with current Hospital Information System or any clinical database.

Our proposed scheme can perform both tamper detection and recovery. Enlightened by [2], tamper detection is achieved through block-based, two-level inspection of authentication data in blocks. The recovery data is achieved through the feature data of original blocks hidden in other blocks in the cover image. The improvement in this scheme is significant. In spite of using sequence numbering like [2], this scheme uses Hilbert pattern to improve the results.

### A. Numbering Pattern

Before embedding, the blocks in the image should be numbered and mapped to decide the location of blocks as the watermark data. A unique style of numbering and mapping of pixels can guarantee the top performance of authentication system by spreading the numbered data as far as possible from the original location [14]. Hilbert is one of space filling curves and a unique style of scanning and numbering, such as shown in Fig. 2. Hilbert curve is a pattern developed by David Hilbert, a German mathematician in 1891 [15]. The proposed embedding technique starts with numbering by the Hilbert manner. It starts at random pixel and directly follows the generated iteration, which is +L, -L, +R and –R as stated in Table 1. This mapping can solve the withdraw faced by [10] because it covers all pixels as long as it is not being numbered yet.

For an M × N sized RGB cover image, each color plane is divided into non-imbricating blocks of size m_height × m_width. In this study, the blocks are set to 8 × 8 blocks when designing the HILBERT-LSB-C scheme. Then, numbering process takes place by applying the Hilbert path to get the non-sequential, unique order of image blocks of pixel before mapping.

Then, the mapping is done pseudo-randomly for all blocks generated by a one-dimensional transformation in (1),

$$B = [(k \times h) mod\ N_b] + 1, \quad (1)$$

where $B$ is the watermarked block, $h$ is Hilbert, $Nb$ is block numbers, and $k$ is the secret key; to ensure all blocks get the new location in the host image when embedding.

### B. Embedding

The embedded watermark in each sub-block is a 3-tuple ($v$, $p$, $r$), where both v and p are 1-bit authentication watermark, and r is a 7-bit recovery watermark for the corresponding sub-

block within the original block (block A) mapped to watermarked block (block C).

In this scheme, the watermark on the cover image is formed by authentication information of 2 bits and recovery information of 7 bits for each sub-block contained 16 pixels (4 x 4), which make the total of 21 bits from three planes for each 16 pixels. By using the block mapping sequence, the authentication and recovery information of the original or cover plane are generated and embedded into its mapping block of host plane of the image. The process is improved from HILBERT-LSB as follows:

*1)* Start with red plane, set the LSB of each pixel within the blocks, C to zero.

*2)* Calculate the average intensity of the block in R components, denoted by AvgC.

*3)* Calculate the average intensity of each four sub-blocks in a block, denoted by AvgCs. Generate the comparison between the average intensities of the blocks and sub-blocks as the authentication watermark, *v*, of each sub-block in the plane as:

$$v = \begin{cases} 0, & \text{if } \mathrm{AvgC_s} < \mathrm{AvgC} \\ 1, & \text{if } \mathrm{AvgC_s} > \mathrm{AvgC} \end{cases} \quad (2)$$

*4)* Generate the parity check bits, *p*, of each sub-block in the red plane as:

$$p = \begin{cases} 0, & \text{if the parity number is even} \\ 1, & \text{if the parity number is odd} \end{cases} \quad (3)$$

*5)* From the mapping sequence done in the first phase, obtain block C from the cover image whose recovery information will be stored in block H of the host image.

*6)* Compute the average intensity of each sub-block (Cs) within C, denoted by AvgCs.

*7)* Obtain the recovery intensity, *r*, of Hs by taking the seven most-significant-bit (MSBs) in AvgHs.

*8)* Embed the 3-tuple watermark (*v, p, r*), each in the LSB of each pixel in H in red plane.

*9)* Repeat the steps from 1 for green plane and blue plane, as shown in Fig. 1.

After the watermark bits are generated and embedded into its host color image, then the watermarked color image is formed. At this point, the image is ready to be stored, transmitted and shared. The process of validating whether the image is authentic or not is needed only after it is transmitted or shared, which is done by the tamper detection process.

For each sub-block Hrs of 4 x 4 pixels within the block Hr, perform the following steps:

*1)* Extract *v* and *p* from Hrs.

*2)* Set the LSB of each pixel within the red component of the Hrs to zero and compute the average intensity for each sub-block Hrs, denoted as Avg_Hrs.

*3)* Set the algebraic relation $\acute{v}$ = 1 if Avg_Hrs ≥ Avg_Hr, otherwise, set it to 0.

*4)* Count the total number of 1s in Avg_Hrs and denote it as Ps.

*5)* Set the parity check bit, $\acute{p}$ of Hrs to 1 if Ps is even, otherwise, set it to 0.

*6)* Compare $\acute{p}$ with *p* and compare $\acute{v}$ with *v*. If they are not equal, mark Hrs as tampered and complete the detection for Hrs; otherwise mark it as valid.

The valid sub-blocks will go through the next step while the tampered sub-blocks will continue with recovery phase.

*7)* For each valid block Hr of size 8 x 8 pixels, find the block number of block D, where block D is the one in which the intensity feature of block Hr is embedded.

*8)* Locate block D.

*9)* If block D is marked tampered, assume block Hr is valid and complete the test.

*10)* If block D is valid, obtain the 7-bit intensity of each Hrs by extracting the LSBs from each pixel in the corresponding block within block D, padding one zero at the end to make an 8-bit value. Compare with Avg_Hrs and mark Hr tampered if they are different.

*11)* Repeat steps for green, Hg, and blue, Hb, plane.

As shown in Fig. 2, the recovery of tampered image phase follows after the image is validated as tampered. For a tampered color image, the recovery data for each plane is stored in respective plane. The recovery procedure is described as follows (tampered block is named as block T and recovery bits block as block R):

*1)* Determine the block number of block R by using the secret key formula.

2) Trace block R.

3) Obtain the 7-bit intensity of each sub-block within block T, padding one zero to the 8th bit to make an 8-bit value.

4) Replace the new intensity of each pixel within the sub-block with this new 8-bit intensity.

5) Repeat step 3 and 4 for all sub-blocks within block T in red plane that have been tampered.

6) Repeat step 1 to 5 for green and blue plane.

## III. Results and Discussions

The metric used in this research is PSNR, one of metrics to determine the degradation in the embedded image with respect to the host image. A general rule of PSNR is the values over 36 dB in PSNR are acceptable in terms of degradation, which means no significant degradation is observed by human eyes [16].

The average PSNR value for watermark embedded images is satisfactory, 57.98 dB. As the PSNR value is high, there is no visual difference between the original image and the watermarked image, such as shown in Fig. 3.

While many researchers focusing in watermarking for color images use the approach of transforming the original color space to color space for the purpose of easy embedding without major changing in the image [8, 12, 17], this scheme promotes embedding in the original space of medical image. The medical scanner such as x-ray, MRI and CT scanner usually store the image in RGB, and for the purpose of protecting the originality and integrity of the medical information, the original space is kept untouched.

The performance evaluation of tamper proofing and recovery on different attacks is performed by detecting and restoring the changed content of the watermarked color image. In the experiments, cut-and-paste attack, collage attack and counterfeiting attack are performed to attack the watermarked image. These are the well-liked attacks of attackers to ruin the data in medical images [12]. Fig. 4 - 6 show the result after the images are being tested with several popular attacks.

To inspect the performance of the HILBERT-LSB-C, the same type of watermarking techniques that embed information into a host medical image in a block-wise trend are chosen for a reasonable comparison. The color medical image watermarking methods proposed by [18] as Adaptive Threshold (TMAP) method, [19] as ROI-based fragile watermarking and [20] as Region-based Watermarking for Robust and Fragile are chosen to compare. HILBERT-LSB-C uses a hierarchical structure to develop the watermarking method for color images, thus the accuracy of tamper localization can be ensured. Here, the method is separately applied to each color channel in the RGB color space for achieving color image watermarking.

In the method proposed by [18], the input image is also divided into blocks of size 8 × 8. The same block-based algorithm with embedding in LSB is proposed. The proposed method provides a good trade-off between capacity and the imperceptibility of a watermarking system into square images. It is also able to restore the original cover image. There are also embedded medical diagnosis reports of patients in medical images. The PSNR value of embedded image is strong too, which is ~56 dB for 8 x 8 block division. Although every result is similar to HILBERT-LSB-C, but the scheme is still compatible to squared grayscale medical images only.

Schemes by [19] and [20] have similar approach which is to embed in RONI of the image. However, the average PSNR values of embedded image are different. Eswaraiah and Reddy (2014) [19] state that the results of PSNR value range from 51 dB to 56 dB. It is satisfactory. While [20] state that their results of PSNR value range from 32 dB to 35 dB. This is due to the watermark data that is also being inserted in the three sub-bands, HH, HL and LH.

To conclude the result, although all these schemes are compatible to all medical modalities, yet [18] still has the limitation of square image only as dataset, beside all of them can only embed in grayscale images.

The watermark data generation and embedding process are done in each plane. The data is still embedded in the LSB of each pixel in each data. This can make sure there is no change in our human visual system in order to prevent the clinical professionals from making wrong diagnosis. The generated recovery bits are believed to be sufficient when each pixel has the stored data in another pixel in each plane. We choose to embed in the original RGB plane and not transform it into $YC^bC_r$ space components, as detailed by [12], [8], and [17] or any other components [9] since we use the method of embedding in the LSB.

## IV. Conclusions

In a nutshell, comparing the average PSNR value with other methods [7, 8, 12], we believe the algorithm of Hilbert numbering for color method can cover all the criteria needed for medical image watermarking. The recovery bit of each original block will be embedded as far as possible to make sure although the image has been attacked with any vast attack, the recovery bit still can survive and the image is recoverable. The Hilbert numbering method is believed compatible for various types of images, color and grayscale. It is also equipped with detection, localization and recovery function. There is no issue of lacking space to embed and requiring much capacity of data as we optimize the three planes of RGB for storing watermark data.

TABLE I. Hilbert Pattern

| Mapping | Unit in iteration | Unit generated |
|---|---|---|
|  | +L | +R +L +L –R |
|  | -L | -R –L –L +R |
|  | +R | +L +R +R –L |
|  | -R | -L –R –R +L |

## References


[1] K. A. Navas, M. Sasikumar, S. Sreevidya, "A benchmark for medical image watermarking", 14th International workshop on systems signals & image processing and 6th EURASIP Conference of speech & image Processing, Multimedia Communication & services, pp. 249-252, June 2007.

[2] P. L. Lin, C. K. Hsieh , P. W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery", Pattern Recognition, vol.38 n.12, p.2519-2529, December, 2005

[3] Chang, Chin-Chen, Yi-Hsuan Fan, and Wei-Liang Tai., "Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery". Pattern Recognition. vol.**41**(2), pg..654-661, 2008.

[4] Pham Anh Hung; Sooraksa, P.; Klomkarn, K., "Extended Baker map using Scan patterns for image encryption". Information Technology and Electrical Engineering (ICITEE), 2013 International Conference, pp. 119-123, 2013.

[5] Zain, J. M., "Digital watermarking in medical images". PhD thesis, Brunel University, United Kingdom, 2005.

[6] J. Fridrich, M. Goljan, "Images with self-correcting capabilities". Proc. ICIP, Vol. 3, pp. 792-796, 1999.

[7] Zain. J. M., R. M. F. Abdul, A. A. Azian, "Clinical evaluation of watermarked medical images", Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 5459-5462, 2006.

[8] M. S. Wang, W. C. Chen, "A majority-voting based watermarking scheme for color image tamper detection and recovery", Computer Standards & Interfaces, v.29 n.5, p.561-570, July, 2007.

[9] N. Wang, C. H. Kim, "Color Image of Tamper Detection and Recovery Using Block-Based Watermarking", 4th International Conference on Embedded and Multimedia Computing, pp.1 - 6, 10-12 Dec. 2009.

[10] B. S. Sergio, A. K. Nandi, "Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities", Signal Processing, vol. 91(4), pp. 728-739, 2011

[11] H. Lin, S. Yang, L. Xu, "Watermark algorithm for color image authentication and restoration", 2011 International Conference on Electronic and Mechanical Engineering and Information Technology, vol. 6, pp. 2773-2776, Aug. 2011.

[12] K. C. Liu, "Color image watermarking for tamper proofing and pattern-based recovery", IET (IEE) Image Processing, vol. 6, no.5, pp. 445-454, 2012.

[13] I. H. Syifak, N. M. Afifah, J. M. Zain, G. Badshah, N. W. Arshad, "Digital Watermarking for Recovering Attack Areas of Medical Images using Spiral Numbering", The 10th International Conference on Electronics, Computer and Computation, 2013.

[14] X. W. Luo, Q. Cheng, J. Tan, A Lossless Data Embedding Scheme For Medical in Application of e-Diagnosis, Proceedings of the 25th Annual International Conference of the IEEE EMBS, (2003) Vol. 1, pp. 852 – 855.

[15] D. Hilbert, Uber die stetige Abbildung einer Linie auf ein Fl¨ achenst¨ uck. Mathematische Annalen, vol. 38, pp. 459-460, 1891

[16] M. Zhang, A. Bermak, Does the Scanning Pattern affect adaptive Quantization Processing?, Proceedings of the 12th International Symposium on Integrated Circuits, pp. 163-166, 14-16 Dec. 2009.

[17] Kostopoulos, I., Gilani, S.A.M., Skodras, A.N.: "Colour image authentication based on a self-embedding technique". Proc. Int. Conf. on Digital Signal Processing, vol. 2, pp. 733–736, 2002.

[18] Manish Madhava Tripathi and S.P Tripathi. "A Block based Reversible Medical Image Watermarking". International Journal of Computer Science and Information Technologies. **4**(2):381 – 384, 2013..

[19] Eswaraiah, R.; Reddy, E.S., "ROI-based fragile medical image watermarking technique for tamper detection and recovery using variance". Contemporary Computing (IC3), 2014 Seventh International Conference. pp. 553-558, 2014.

[20] Al-Haj A and Amer A. "Secured telemedicine using region-based watermarking with tamper localization". J Digit Imaging. Vol. **27**(6), pp. 737-750, 2014.

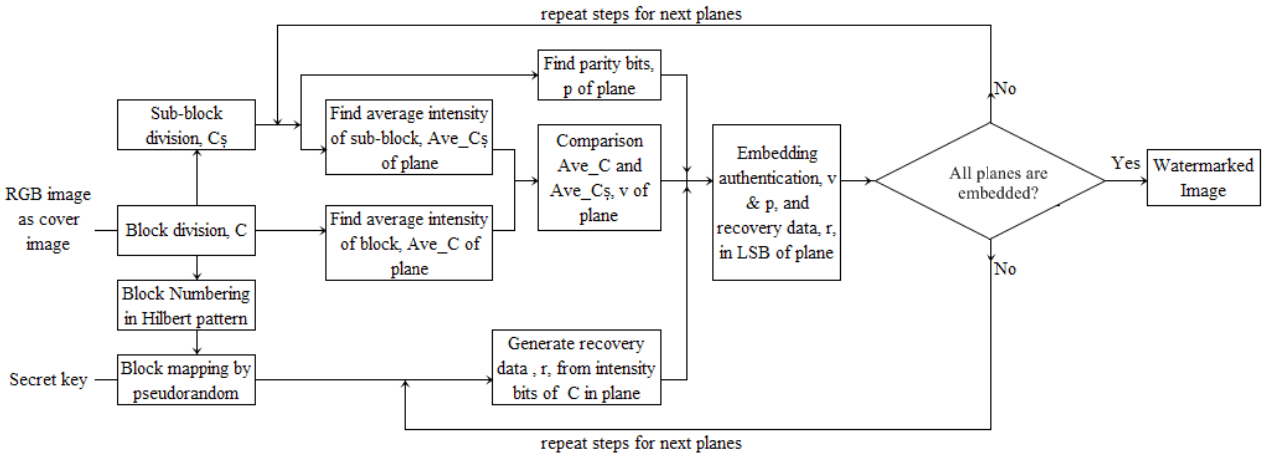


Fig. 1. The Flow Diagram of HILBERT-LSB-C to Embed in Color Medical Image.

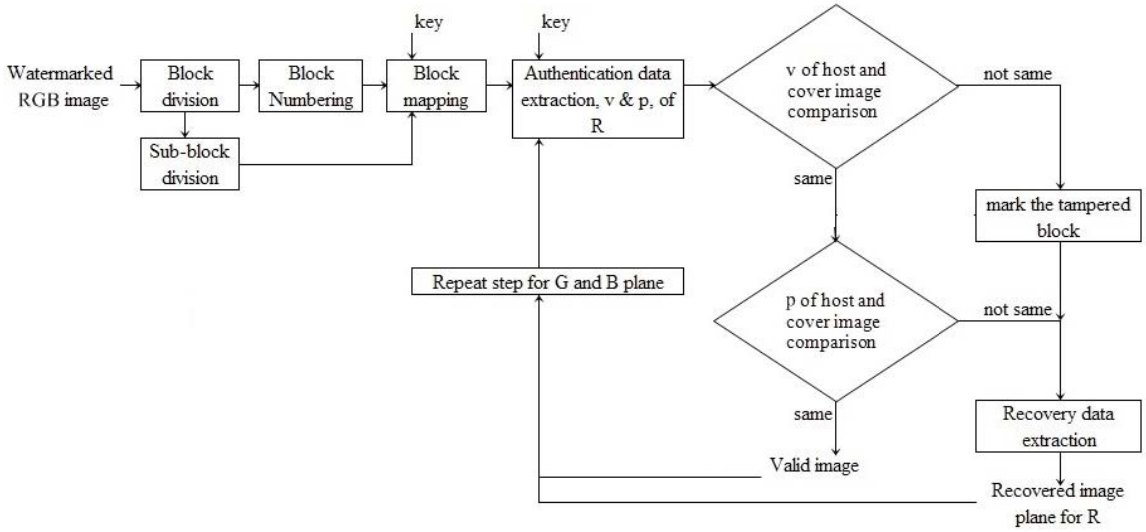


Fig. 2. The flow diagram for proposed tamper detection and recovery in proposed watermarking scheme

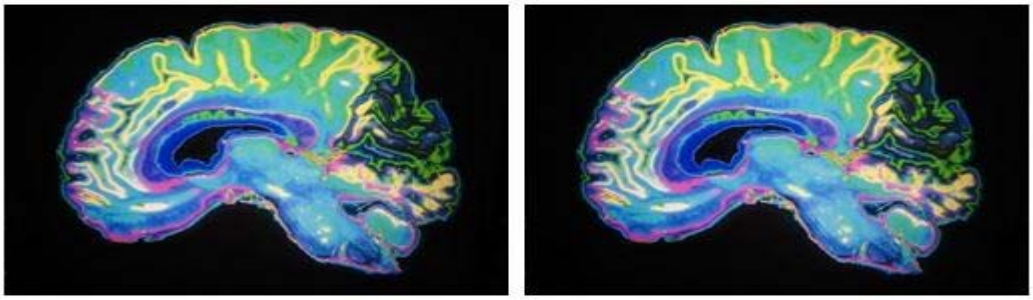

Fig. 3. (From left) The brain image used in the simulation and the watermarked color images (PSNR: 57.1472)

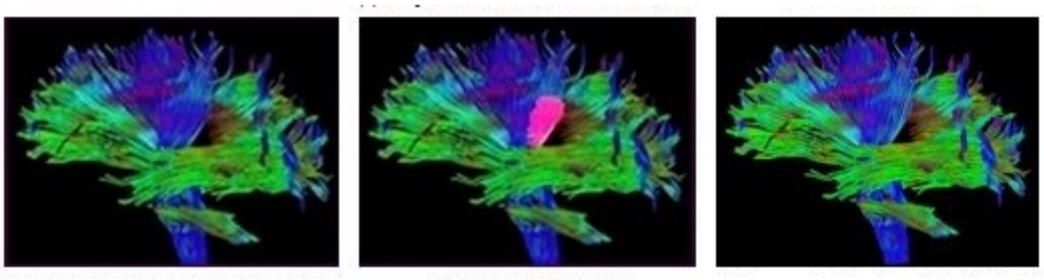

Fig. 4. Filter attack; (from left) tampered 'brain tissue' with mosaic filter ; detected 'brain tissue'; recovered 'brain tissue' (PSNR: 65 dB)

Fig. 5. Cut-and-paste attack; (from left) tampered 'fetus', tamper detected 'fetus' ; recovered 'fetus' (PSNR: 69 dB)

Fig. 6. Collage attack; (from left) tampered 'hand'; tamper detected 'hand'; recovered 'hand' (PSNR: 63.5 dB)