

Three Layer Authentications with a Spiral Block Mapping to Prove Authenticity in Medical Images

Ferda Ernawan¹, Afrig Aminuddin², Danakorn Nincarean³, Mohd Faizal Ab Razak⁴, Ahmad Firdaus⁵

Faculty of Computing, Universiti Malaysia Pahang, Pekan 26600, Malaysia^{1,3,4,5}
Faculty of Computer Science, Universitas Amikom Yogyakarta, Sleman, 55283, Indonesia²

Abstract—Digital medical image has a potential to be manipulated by unauthorized persons due to advanced communication technology. Verifying integrity and authenticity have become important issues on the medical image. This paper proposed a self-embedding watermark using a spiral block mapping for tamper detection and restoration. The block-based coding with the size of 3×3 was applied to perform self-embedding watermark with two authentication bits and seven recovery bits. The authentication bits are obtained from a set of condition between sub-block and block image, and the parity bits of each sub-block. The authentication bits and the recovery bits are embedded in the least significant bits using the proposed spiral block mapping. The recovery bits are embedded into different sub-blocks based on a spiral block mapping. The watermarked images were tested under various tampered images such as blurred image, unsharp-masking, copy-move, mosaic, noise, removal, and sharpening. The experimental results show that the scheme achieved a PSNR value of about 51.29 dB and a SSIM value of about 0.994 on the watermarked image. The scheme showed tamper localization with accuracy of 93.8%. In addition, the proposed scheme does not require external information to perform recovery bits. The proposed scheme was able to recover the tampered image with a PSNR value of 40.45 dB and a SSIM value of 0.994.

Keywords—Fragile watermarking; self-embedding; image authentication; self-recovery; medical image; spiral block mapping

I. INTRODUCTION

The development of internet technology has grown exponentially in the last decade. Internet technology made digital multimedia data easy to be distributed to the world. With the rapid development of information technology, multimedia data was produced and sent seamlessly without boundaries and limitations. The digital image can be produced by various electronic devices such as digital cameras and X-ray machines for medical images [1], [2]. In addition, there are many available images editing software to modify these digital images, such as Photoshop, Lightroom, and GIMP. However, the advancement of this software also enables unauthorized modification to a digital image that makes it hard to identify the authenticity and integrity of the images. The medical images require the images to be authentic to prevent false decisions under some circumstances. Thus, any alteration or slight modifications cannot be accepted. Digital images could be modified by unauthorized persons for illegal use. The modification can be invisible or visible to the human eye. Furthermore, the illegal modification may lead to illegal action against the law. Image watermarking techniques can be

an alternative solution to authenticate digital image content [3].

Digital image watermarking is the process of embedding a watermark into digital images [4]. The watermark itself can contain a logo, serial number, or a security key. The watermark is then embedded into the cover image to be visible or imperceptible. An example of a visible watermark is a transparent logo as seen embedded in the corner of an image to prevent copyright violation. However, this type of watermark was prone to watermark removal by simply cropping or overlaying the new watermark over the original watermark. Hence, the researcher primarily focused on the imperceptible watermark with a security feature to not be easily removed by any attack. Digital watermarking techniques can be used to protect copyright and authenticate digital image content. There are three types of image watermarking: robust, semi-fragile, and fragile watermarking. Robust image watermarking is mainly used for copyright protection so that any modification on the image content, the embedded watermark should be resistant against several attacks. In contrast, semi-fragile and fragile watermarking are primarily utilized for image authentication. Fragile image watermarking is not resistant to any modifications on the watermarked image. Fragile watermarking has been widely used to detect tamper localization and authenticate the image content. Fragile watermarking does not allow modification to the image content, while semi-fragile image watermarking will tolerate minor changes to the image, such as image compression [5], [6].

A fragile image watermarking for authentication provides four important aspects which are watermark generation, insertion technique, tamper localization, and tamper recovery. The watermark generation presented a way to generate a watermark image to be embedded into the cover image. The existing schemes use the part of the cover image as the watermark image, which is called self-embedding fragile image watermarking [7], [8]. The watermark generation also can be obtained from a set of embedding bits that contains the authentication bit and recovery bits [9], [10]. The embedding watermark in fragile watermarking can be performed by modifying the bits of the host image. The embedding of watermark bits into the first Least Significant Bit (LSB) made it invisible to the human eye [11]. The embedding of the watermark into the second LSB significantly contributes to the reconstruction error. Lastly, the tamper recovery algorithm plays a key role in recovering the tampered area of the image.

The recovered image quality depends on the size of the tampered area.

Image authentication techniques can be used for verifying or authenticating the integrity of digital media content. Image authentication can be classified into passive and active authentication. Active authentication requires preliminary data from the original image. This data could be stored on a secured database so that the authentication can be done by comparing the data from the database and the extracted data from the receiving ends [12]. Another scheme directly embedded the data into the cover images, so it does not need any intermediate database to store the authentication data, while it slightly reduces the quality of the image [13], [14]. In addition, some active authentication schemes also support tamper recovery along with authentication and tamper detection [15], [16]. In contrast, passive authentication was performed without requiring any preliminary image information for authentication. Passive authentication was categorized as forgery dependent and independent. On one hand, forgery dependent will only detect some types of forgery, such as copy-move and splicing forgery. This type of forgery may not leave any visual trace, but the inconsistencies of the underlying statistics can detect it. On the other hand, forgery independent will detect the tampered image based on the visible artifacts left during the resampling process and lighting inconsistencies [17]. Thus, passive authentication has limited tamper detection capability depending on its forgery types and the visual artifacts left behind. Furthermore, passive authentication did not support tamper recovery compared to active authentication [18], [19].

The existing authentication schemes still do not achieve high accuracy in tamper detection. The high accuracy of tamper detection is significantly important for achieving the high quality of the self-recovered image. Therefore, this study presents three-layer authentications with a spiral block mapping that can support tamper recovery. The parity bit of each block is extracted to obtain the authentication bit for the first level. If the bit value is the same, then the second authentication bit will be computed and compared with the average pixel of its block image. If the average pixel of the sub-block is greater than the average pixel of its block, then the third authentication is performed to check the output of the second layer authentication in three RGB channels. The proposed scheme embeds the image content itself into the host image based on a spiral block mapping. The embedding process will be performed for each block of 3×3 pixels, the nine least significant bit is modified for authentication and recovery. The proposed embedding scheme utilized a set of conditions bits. The recovery bits are embedded into the different locations of sub-block images. The proposed spiral block mapping can detect any tamper occurred on the watermarked image. The proposed scheme will produce a higher accuracy of the tamper detection and higher quality of the recovered image than other existing schemes after tampering the image.

II. RELATED WORK

Belferdi et al. [15] presented a self-embedding fragile watermarking scheme for color image tamper detection and

recovery. The scheme implemented the Bayer pattern to reduce the size of embedding watermarks into the original image. The watermark was generated from the original image by decomposing the image into red, green, and blue channels. The scheme converted the color watermark into a grayscale image by using the Bayer filter to reduce the watermark size. This filter selects one color sample from each color channel. This grayscale watermark was decomposed into four sub-blocks to improve security and enhance robustness. Each sub-image was then permuted three times based on automorphic permutation using three keys to ensure maximum security. Finally, each permuted sub-images is converted into a binary sequence and embedded three times into the least significant bits (LSB) of the three RGB components of the host images. The scheme can improve detection accuracy if one channel was destroyed.

Gul and Ozturk [20] showed a fragile image of watermarking and tamper-detection based on the SHA-256 hash function. The scheme divided the cover image into non-overlapping blocks with the size of 32×32 pixels. Each block was then sub-divided into four sub-blocks of 16×16 pixels. The watermark was generated using the entire SHA-256 hash value of the first three sub-blocks. The resulting 256-bit binary watermark was embedded into the least significant bit (LSB) of the fourth sub-block. The tamper detection works by comparing the hash value of the first three blocks to the extracted watermark obtained from the fourth block.

Hisham et al [2] presented a watermarking scheme for tamper detection and self-recovery. The scheme presented a spiral pattern during embedding the watermark image. While the pattern of embedding a watermark in the LSB does not give effect to the quality of the watermarked image and security. The spiral pattern did not work for the non-square image; some parts of the image can't be embedded using a spiral pattern. The embedding watermark using a spiral pattern doesn't give any contributions to the watermarked image especially for modifying LSB. The embedding scheme was performed on each block of 8×8 pixels. Each block was divided into sub-block with the size of 4×4 pixels. Each sub-block with the size of 4×4 was embedded by nine bits, including two (v and p) authentication bits and seven recovery bits. The scheme considers only 9 bits over 16 bits of LSB on each sub-block. The scheme did not fully utilize the rest of the seven bits for embedding watermark images. The scheme has the potential to consume a large computational time and it did not optimize the embedding space of the host image. The recovery bits in the scheme are generated from the average pixel value on its image sub-block. The scheme is designed to recover the tampered area by using an average value of its sub-block image with the size of 4×4 pixels. If any small tamper occurred in the sub-block of 4×4 pixels, the average pixel value will replace it. The scheme has the potential to produce less quality of the recovery bits due to average pixels, even if the tamper that occurred was a small area.

III. PROPOSED SCHEME

A. Proposed self-embedding Watermark

The experiments utilize seven medical images with different sizes namely "Abdomen", "Brain", "Breast",

“Chest”, “Eye”, “Teeth”, and “Womb” images. The block diagram of the proposed scheme is depicted in Fig. 1.

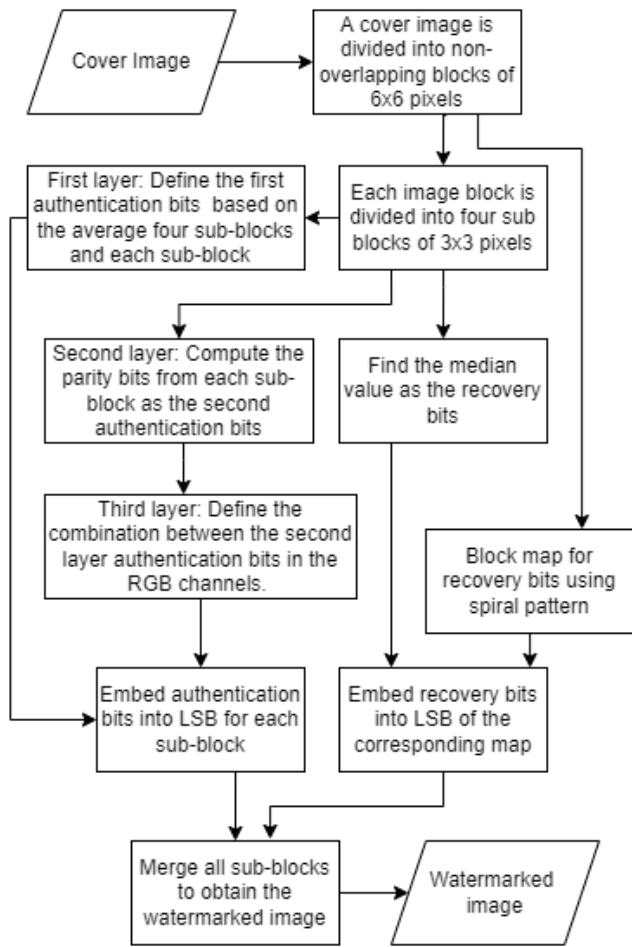


Fig. 1. Block Diagram of the Proposed Embedding Scheme.

A watermark image is obtained from the two bits, v and p for authentication and seven bits of the sub-block recovery. Each pixel of the cover image was embedded with watermark bits on the LSB of the cover image. The selected sub-block of 3×3 pixels in the embedding watermark is to achieve an optimal embedding of two authentication bits and seven recovery bits into the LSB of the cover image. The modifying LSB of the cover image does not give a significant effect on the quality of the medical image. The following steps discuss the proposed self-embedding watermark:

1) A cover image is divided into non-overlapping blocks of 6×6 pixels. Then, each block is divided into four sub-blocks with the size of 3×3 pixels. The visualization of the block and four sub-block images is shown in Fig. 2.

2) The average pixel value of image block $AvgB$ is calculated, and each of its sub-block $AvgSB$.

3) The first authentication bits were computed by comparing the average image block of 6×6 pixels $AvgB$ and each of its sub-block with the size of 3×3 pixels $AvgSB$. If the average $AvgB$ is larger than $AvgSB$, the authentication bit denoted as v is 1, and vice-versa.

4) The second authentication bits were generated from the parity bits of each sub-block. The authentication bit denoted as p is 1 if the parity number is equal to an odd number, and 0 if the parity bit is an even number.

5) The first and second authentication bits are embedded in each LSB of each sub-block. The illustration of each embedding authentication bits, v and p into the sub-block is shown in Fig. 3.

According to Fig. 3, the white region represents the original bit of pixels on each sub-block, P represents the pixel value, v is the first layer authentication bit and p is the second layer authentication bit.

6) The recovery bits of each sub-block are generated by finding the median value of its sub-block. The seven most significant bits of median pixel value are used as recovery bits. The recovery bits are embedded based on a spiral pattern as visualized in Fig. 4. In the proposed scheme, the authentication bits and recovery bits are embedded in different locations. The recovery bits on the first block are embedded into the nineteenth block and so on. The recovery bits for each block are embedded based on the spiral block mapping as shown in Fig. 4. The proposed spiral block mapping can avoid tampered coincidence.

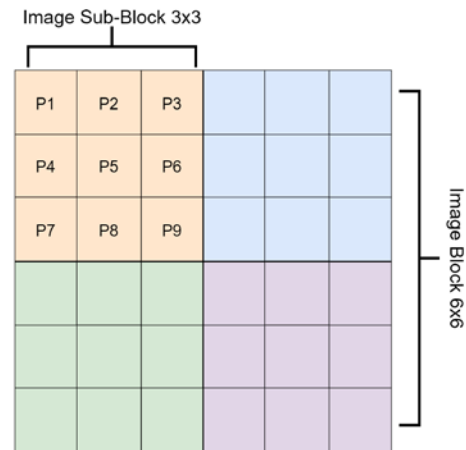


Fig. 2. Illustration of Image Block and each of its Sub-block.

MSB Bit								LSB	Authentication bits
	7	6	5	4	3	2	1	0	
P1								v	Authentication bits
P2								p	
P3								r	Recovery bits
P4								r	
P5								r	
P6								r	
P7								r	
P8								r	
P9								r	

Fig. 3. The Location of the Watermark Bits in the Cover Image.

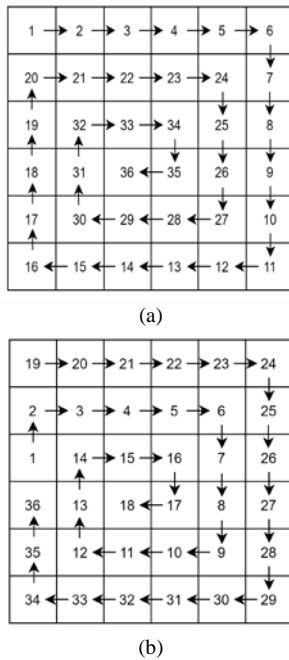


Fig. 4. The Illustration of (a) A Spiral Pattern of its Block and (b) A Spiral Block Mapping for Embedding the Recovery Bits.

7) The self-embedding watermark is repeated for all sub-blocks to obtain the watermarked image.

B. Proposed Tamper Detection and Recovery Scheme

The watermarked images are tested under several attacks such as blur, unsharp, cloning, mosaic, noise, removal, and sharpen images. The proposed scheme provides two-level authentications. The procedures of tamper detection are defined by:

1) *First-level authentication:* A tampered image is divided into non-overlapping blocks with the size of 6×6 pixels. Then, each block is divided into four sub-blocks with the size of 3×3 pixels. The extract bit v from LSB on the first pixel of its sub-block in the watermarked image. The parity bit of each block is computed, if the parity number is an odd number, the parity bit v' is set to 1, otherwise, set it to 0. The parity bit v' is compared with the extracted v from each LSB of its sub-block. If the bit value of v' and v are not equal, then mark it as a tampered image, otherwise, no tamper is detected. In addition, if the bit value between v' and v is the same, then the second authentication bit p will be checked in the second level authentication.

2) *Second-level authentication:* In the second authentication bit, the extracted bit p from LSB on the second pixel is compared with the p' represents algebraic relation between sub-block with the size of 3×3 pixels and block image with the size of 6×6 pixels. The average pixel of each sub-block is computed and compared with the average pixel of its block image. if the average pixel of the sub-block is greater than the average pixel of its block, the p' is 1, otherwise, the p' is 0. If the bit value of p' and p are not equal, then mark it as a

tampered image, otherwise, no tamper is detected. The proposed authentication is defined in Algorithm 1 as follows:

Algorithm 1. The proposed multilayer authentication levels

Input: v, v', p, p'

```

1   $\alpha = 0;$ 
2  for  $i=1$  to 4
3    if ( $v \sim v'$ )
4      # mark as tampered sub-block
5       $\alpha = 1;$ 
6    else
7      if ( $p \sim p'$ )
8        # mark as tampered sub-block
9         $\alpha = 1;$ 
10     elseif ( $\alpha == 1$ )
11       # mark as tampered sub-block
12        $\alpha = 0;$ 
13     else
14       # mark as untampered sub-block
15        $\alpha = 0;$ 
16     end
17   end

```

Output: tampered, untampered sub-block

where v denotes the extracted bit from LSB on the first pixel of its sub-block in the watermarked image, v' represents the parity bit of each sub-block, p is the extracted bit from LSB on the second pixel of its sub-block, and p' represents algebraic relation between sub-block and block image. The α value is 1 if the sub-block is marked as a tampered sub-block. The α value is used as a reference of its block that has tamper detection. If the previous sub-block has tampered with the attack, the next sub-block has a possibility of tampered image.

3) *Third-level authentication:* The third layer authentication checks the result obtained from the second layer authentication in three RGB channels. If an image block of the RGB channel is detected as a tamper, then set all blocks of RGB channels on its block locations to be tampered. This third layer authentication further reduces the false-negative detection. The diagram of the proposed tamper detection and the recovery bits is shown in Fig. 5.

C. Evaluation of the Proposed Scheme

The proposed tamper detection algorithm is evaluated by using a confusion matrix such as True Positive Rate (TPR), False Negative Rate (FNR), and False Positive Rate (FPR). TPR represents the ratio between the detected area against the real tampered. The highest TPR means that the tamper detections are correctly detected in the tampered regions. In contrast, FNR means the ratio between the undetected area compared to the real tampered area. The high FNR means inaccurate tamper detection in the tampered area of the images. Next, the FPR represents the ratio between the false detected area against the untampered area. The range of FPR values is between 0 to 1, the higher FPR value represents the higher detection of the untampered area as tampered area or false detection. The proposed scheme is also measured in terms of precision and accuracy for evaluating tamper detection. The TPR and FNR are defined by [11]:

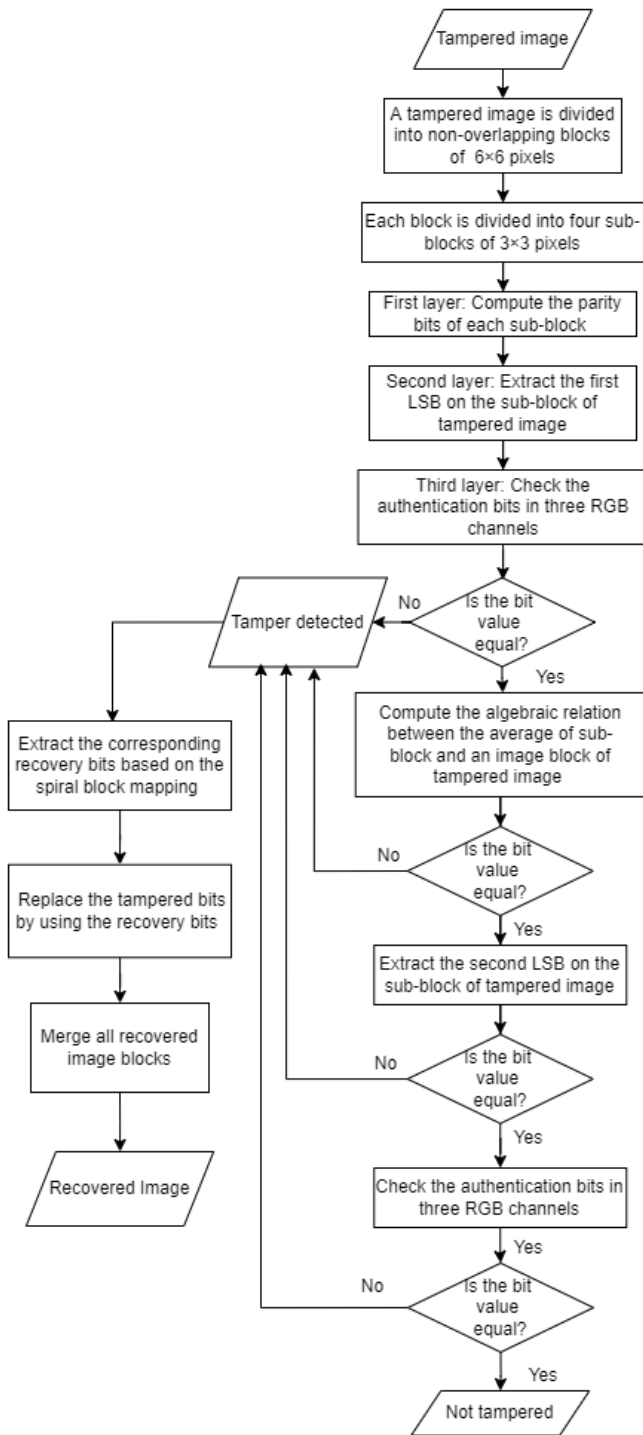


Fig. 5. Block Diagram of the Tamper Detection and Recovery Schemes.

$$TPR = \frac{TP}{TP + FN} = \frac{TP}{P} = 1 - FNR \quad (1)$$

$$FNR = \frac{FN}{TP + FN} = \frac{FN}{P} = 1 - TPR \quad (2)$$

where TP represents the number of true-positive tampered pixels, FN denotes the number of false-negative tampered pixels, P represents the number of real tampered pixels. The FPR is defined by:

$$FPR = \frac{FP}{FP + TN} = \frac{FP}{N} \quad (3)$$

where FP represents the number of false-positive tampered pixels, TN denotes the number of true-negative tampered pixels, N represents the number of untampered pixels. The precision and accuracy of the tampered detection are defined by [11]:

$$Precision = \frac{TP}{TP + FP} = \frac{TPR}{TPR + FPR} \quad (4)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{TP + TN}{P + N} \quad (5)$$

The precision represents the precise tamper detection on the image. The higher precision value means that the proposed scheme was able to produce high true positive values and low false-positive values. The accuracy of tampering detection is evaluated in order to measure the effectiveness of the proposed scheme. High accuracy on tamper detection can improve the recovery bits of the tampered image.

The quality of the watermarked image and recovered image is evaluated in terms of the imperceptibility by using PSNR, MSE and SSIM. The PSNR is defined as follows [21]-[24]:

$$PSNR = 10 \log \frac{(S)^2}{MSE} \quad (6)$$

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f(i, j) - g(i, j))^2 \quad (7)$$

where $f(i, j)$ is the original medical image, $g(i, j)$ is the watermarked image, M, N denotes as the row and column sizes of the medical image. MSE represents the difference value between original and watermarked image, S denotes a maximum pixel value of the medical image. The SSIM is defined as follows [25]-[32]:

$$SSIM(x, y) = [l(x, y)]^f \cdot [c(x, y)]^g \cdot [s(x, y)]^h \quad (8)$$

where $\alpha > 0, \beta > 0, \gamma > 0$, are parameters to define the relative importance of the three components l, c and s . The SSIM index is defined as three similarity terms of luminance, contrast, and structural between two local windows. The SSIM considers image degradation as the perceived change in structural information, separating the measure of similarity into luminance, contrast, and structure [33]. The range SSIM value in between 0 to 1, the higher SSIM value indicated that the watermarked image is structurally similar to the original cover image.

IV. EXPERIMENTAL RESULTS

The proposed scheme embeds self-image content as a piece of watermark information on the least significant bit (LSB) of the cover image. Each pixel of the cover image has 8-bits of information which corresponds to the range of pixel values 0 to 255. Embedding watermark information into LSB has some advantages include less distortion on the watermarked image and fast embedding watermark image. Thus the embedding LSB algorithm can preserve the quality of the cover image. The embedding watermark by using LSB can provide high sensitivity against an altered image. A small

altered image into the pixel value can be identified. Therefore, the LSB method has been widely used on fragile watermarking for image authentication. This study proposed a self-embedding scheme for tamper detection and restoration in the medical image by using multilayer authentications. The visual original covers a medical image, a watermark image obtained from its image content and the watermarked image is shown in Fig. 6.

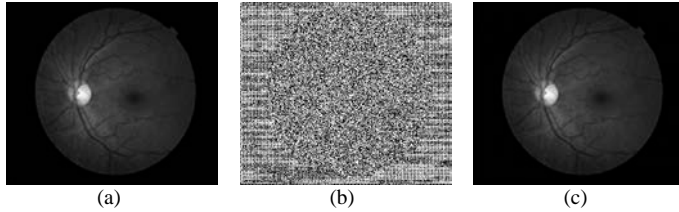


Fig. 6. (a) Original Eye Image, (b) Watermark Image, (c) Watermarked Image.

According to Fig. 6, the experimental results showed that the proposed scheme achieves high quality of the watermarked image with the PSNR value of 51 dB. The experimental results of the proposed scheme have been compared with the scheme by Hisham et al. [2]. The imperceptibility of the watermarked image in terms of MSE, PSNR, and SSIM is shown in Table I. Referring to Table I, it can be noticed that a scheme by Hisham et al. [2] achieved a lower MSE value compared with the proposed method. In addition, the scheme also produced higher PSNR and SSIM values than the proposed scheme.

A scheme by Hisham et al. [2] embedded nine bits out of sixteen bits as watermark information on each sub-block of 4x4 pixels. A scheme by Hisham et al. [2] used a sub-block size of 4x4 pixels which contains 16 pixels on each sub-block. All pixels are not embedded by the watermark bits, only nine bits 56.25% of pixels are modified on the LSB of the sub-block pixels. The remaining seven bits 43.75% are maintained as original bits or unmodified. The proposed scheme embedded the watermark bits on the sub-block of 3x3 pixels which contains 9 pixels. All the pixels are modified with watermark bits on the LSB of each sub-block. The proposed scheme embeds two bits as authentication bits and seven bits as recovery blocks as the watermark bits. Modifying all pixel values of the sub-block image can contribute to the reconstruction error. Therefore, the scheme by Hisham et al. [2] produced higher PSNR and SSIM values than the proposed scheme. The comparison of the existing methods using the block-based scheme for image authentication is shown in Table II.

Referring to Table II, it can be noticed that modifying 1 LSB of the cover image produced a higher quality of the watermarked image with a PSNR value of 50 dB above. Schemes by Huang et al. [7], Sing et al. [10], and Tohidi et al. [19] did not inform the detection accuracy. In addition, the existing watermarking schemes based on block coding required an original cover image or external information in

order to recover the image. The schemes by Belferdi et al. [15] and Tohidi et al. [19] embedded watermark information into the first and second LSB of the cover image. The schemes produce PSNR values of about 44 dB. At the same time, the schemes produced high distortion on the recovery image. The schemes by Belferdi et al. [15] and Tohidi et al. [19] produced the quality of the recovered image with PSNR values of 40dB and 32 dB respectively. The schemes by Huang et al. [7] and Sing et al. [10] embedded watermark data into the first, second, and third LSB of the image. The scheme produced a PSNR value of about 39 dB due to modifying 3 LSB on the cover image. The recovered image still produced a PSNR value of 41 dB and 39 dB, respectively. Even though the scheme presented a self-embedding watermark, it still required reference bits for authentication. A scheme by Hisham et al. [2] was able to produce high imperceptibility of the watermarked image with a PSNR value of 53 dB. The scheme embedded nine bits out of sixteen bits for authentication and recovery bits. The remaining seven bits are maintained as the original bits. Therefore, the scheme can achieve a high PSNR value of the watermarked image. While the scheme produced low accuracy on the tamper detection due to limited embedding watermark for each sub-block. A scheme by Hisham et al. [2] also required reference bits for recovering the medical images. The scheme produced a quality of the recovered image with a PSNR value of 40 dB. The proposed scheme achieved a slightly low quality of the watermarked image compared with a scheme by Hisham et al. [2] with a PSNR value of 51 dB. In addition, the proposed scheme provides higher accuracy of tamper detection than a scheme by Hisham et al. [2]. The proposed scheme produced a superior quality of the recovered image than the existing benchmark of the watermarking schemes. The proposed scheme is tested under various tampering rates, and then the results are evaluated by using True Positive Rate (TPR), False Negative Rate (FNR), and False Positive Rate (FPR). The comparison of the TPR, FNR and FPR under various tampering conditions is listed in Table III.

TABLE I. THE COMPARISON OF THE IMPERCEPTIBILITY PERFORMANCE BETWEEN THE PROPOSED SCHEME AND A SCHEME BY HISHAM ET AL. [2]

Medical Image	PSNR (dB)		SSIM	
	Hisham et al. [2]	Proposed scheme	Hisham et al. [2]	Proposed scheme
Abdomen	53.6267	51.1424	0.9995	0.9992
Brain	53.8694	51.3455	0.9978	0.9938
Breast	54.1428	51.7481	0.9951	0.9876
Chest	53.6200	51.1389	0.9996	0.9993
Eye	53.1564	50.9746	0.9953	0.9923
Teeth	53.6523	51.1339	0.9978	0.9961
Womb	54.1882	51.6033	0.9970	0.9910
Average	53.7508	51.2981	0.9974	0.9942

TABLE II. COMPARISON OF THE QUALITY, TAMPER LOCALIZATION, RECOVERY OF THE EXISTING WATERMARKING SCHEME

Method	PSNR Embedding	Embedding Location	Detection	PSNR Recovery	Recovery	Authentication type
Hisham et al. [2]	53.7508 dB	1 LSB	0.7668	40.7861 dB	Require original cover image	Active
Belferdi et al. [15]	44.2495 dB	2 LSB	1.0000	40.7300 dB	Using Bayer Pattern	Active
Huang et al. [7]	39.0900 dB	3 LSB	-	41.3200 dB	Using ROI & RONI	Active
Sing et al. [10]	39.8600 dB	3 LSB	-	39.1400 dB	Using Block Truncation Coding	Active
Tohidi et al. [19]	44.0000 dB	2 LSB	-	32.0000 dB	Using Compression Strategy	Active
Proposed scheme	51.2981 dB	1 LSB	0.8774	44.7922 dB	Not require the original cover image	Active

The watermarked medical images obtained from the scheme by Hisham et al. [2] and the proposed scheme are tested under various attacks and each tamper attack was subjected to the same size of the attack. According to Table III, the seven medical images have been tested under various tampering rates. The experimental results show that the proposed scheme achieves a higher average TPR than a scheme by Hisham et al. [2]. The scheme by Hisham et al. [2] presented multilayer authentication based on a set of conditions on the average value of sub-block and parity bits of sub-block with the size of 4x4 pixels. The scheme has the potential for detecting 75% certainty of the tampered sub-block. First, the parity bit on each sub-block was compared with the first extracted bit of its sub-block. The first layer authentication has a probability of being 50% undetected. The second layer authentication performed a comparison of the average sub-block and block image. This stage also provided a 50% probability of the previous undetected tampered area. The proposed scheme presented multilayer authentication bits by considering the previous tampered block. The first layer authentication compared the average value of the sub-block with the size of 3x3 pixels and block with the size of 6x6 pixels. If the bits are not equal, the sub-block was marked as tampered sub-block and the α was set to 1. Otherwise, the bits are the same, then the second layer authentication is computed to check the authenticity of bits. The second layer of authentication compared the parity of bits on each sub-block with the extracted bits obtained from LSB on its sub-block. If the bit values are not the same, then the sub-block was assigned as a tampered sub-block. In addition, if the α value is

1, the sub-block image was marked as a tampered block. If the previous sub-block has a tampered with, its block image has a high probability tamper. The proposed tamper detection algorithm successfully increased the detection rate compared with the scheme by Hisham et al. [2]. A scheme by Hisham et al. [2] produced an average TPR rate of 76.68%. The proposed scheme successfully detects the tampered image with a high TPR rate of 87.74%. The accuracy of the tamper detection scheme under various tamper attacks is shown in Fig. 7.

According to Fig. 7, the proposed scheme also provided a slightly higher FPR rate than the scheme by Hisham et al. [2], it does not significantly affect the reliability of the proposed scheme. It has been proven by achieving a higher accuracy rate compared to the scheme by Hisham et al. [2] as shown in Table III. According to Table III, our scheme produced slightly lower precision than the scheme by Hisham et al. [2]. The proposed scheme achieved higher accuracy than other schemes with an average accuracy of about 0.997. Both schemes provide multilayer authentication for detecting tamper images. Our scheme proposed tamper localization by using multilayer authentication with considering the previous sub-block α . Referring to Fig. 7, it has been proven that the proposed authentication algorithm can improve the accuracy of tamper detection. The proposed authentication algorithm can detect higher accuracy of the tamper localization compared with the scheme by Hisham et al. [2]. The proposed scheme is also able to recover bits against various tampered attacks. The experimental results of the recovered image are listed in Table IV.

TABLE III. COMPARISON OF THE TPR, FNR AND FPR UNDER VARIOUS TAMPERING RATES

Medical Image	Tamper Attacks	Tampering Rate (%)	TPR		FNR		FPR		Accuracy	
			Hisham et al. [2]	Proposed	Hisham et al. [2]	Proposed	Hisham et al. [2]	Proposed	Hisham et al. [2]	Proposed
Abdomen	Blurring	0.95	0.7261	0.8566	0.2739	0.1434	0.0010	0.0012	0.8626	0.9277
Brain	Unsharp Mask	0.70	0.7532	0.8642	0.2468	0.1358	0.0007	0.0010	0.8763	0.9316
Breast	Copy-Move	0.60	0.7493	0.9523	0.2507	0.0477	0.0004	0.0006	0.8745	0.9759
Chest	Mosaic	0.80	0.8343	0.8523	0.1657	0.1477	0.0011	0.0014	0.9166	0.9255
Eye	Noise	2.0	0.7639	0.8790	0.2361	0.1210	0.0017	0.0023	0.8811	0.9384
Teeth	Removal	1.35	0.7691	0.8409	0.2309	0.1591	0.0015	0.0013	0.8838	0.9198
Womb	Sharpening	0.91	0.7716	0.8962	0.2284	0.1038	0.0008	0.0011	0.8854	0.9476
Average			0.7668	0.8774	0.2332	0.1226	0.0010	0.0013	0.8829	0.9380

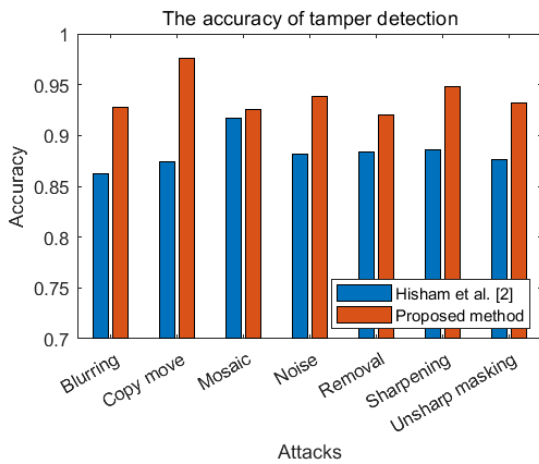


Fig. 7. The Comparison on the Accuracy of Tamper Detection between the Proposed Scheme and a Scheme by Hisham et al. [2].

TABLE IV. COMPARISON OF THE QUALITY OF THE RECOVERED BITS UNDER VARIOUS TAMPERING RATES

Medical Image	PSNR (dB)		SSIM	
	Hisham et al. [2]	Proposed scheme	Hisham et al. [2]	Proposed scheme
Abdomen	39.4512	49.4710	0.9960	0.9988
Brain	43.5453	45.4482	0.9948	0.9955
Breast	44.3019	46.8068	0.9968	0.9985
Chest	42.6248	48.8064	0.9972	0.9984
Eye	36.9968	39.6542	0.9773	0.9812
Teeth	40.8027	42.9007	0.9920	0.9935
Womb	37.7798	40.4584	0.9966	0.9975
Average	40.7861	44.7922	0.9930	0.9948

The watermarked images obtained from the proposed scheme were tested under various tamper attacks. Each watermarked image was tampered with using the common attack in the medical images such as blurring, unsharp masking, copy-move, mosaic, noise, removal, and sharpening. Each attack is carried out in a round shape with a diameter of 60 pixels to simulate a real-world attack. The visualization of the comparison between the proposed scheme and other existing schemes for the recovered image is depicted in Fig. 8.

The scheme by Hisham et al. [2] used the spiral block mapping for embedding watermark and retrieved the recovery embedded bits from another block by using pseudorandom equations. The secret key used the total number of blocks in the image. This block mapping introduced a tamper coincidence problem during the recovery process. The recovery bits may be altered due to randomized blocks. Therefore, the scheme was not able to retrieve the embedded recovery bits. In addition, the scheme only can be performed with the square image size. The block numbering starts from the center of the image and spirals outward to the edge of the image. If the image input is not a rectangle, then the block mapping algorithm will not be able to handle outside the

square area in the center of the image and the outside area will be unprotected. This study proposed a spiral inward block mapping started from the top-left of the image and ended in the center of the image. To solve this tamper coincidence problem, the proposed method maps the first half of spiral inward mapping to the second half of the spiral block mapping. This technique greatly decreases the tamper coincidence problem during the recovery bits. This approach also can overcome the square-image problem presented by Hisham et al. [2]. The proposed method successfully protects all the image pixels as well as the rectangle images. The proposed method successfully recovers the image from the tampered image. The proposed scheme achieved higher quality recovered images than the scheme by Hisham et al. [2] with an average PSNR value of 44.7922 dB and an average SSIM value of 0.9948. The proposed scheme presented a smaller sub-block code with the size of 3x3 pixels for embedding watermark. Our scheme proposed a spiral block map to prevent the tamper coincidence problem. The proposed scheme is also tested under different tampering rates. The quality of the recovered images is shown in Fig. 9.

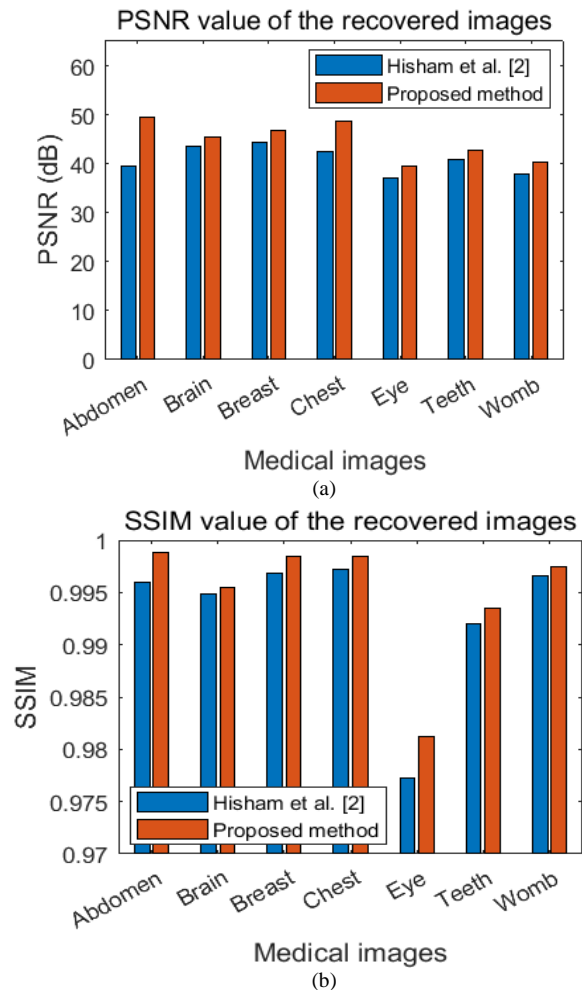


Fig. 8. The Quality of the Recovered Image from the Proposed Scheme and a Scheme by Hisham et al. [2] (a) PSNR (b) SSIM.

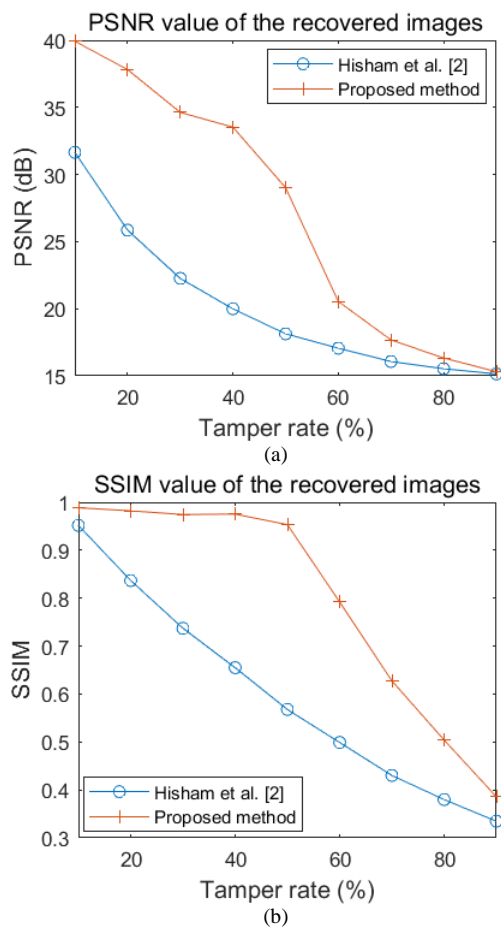


Fig. 9. The Quality of the Recovered Image: (a) PSNR Value, (b) SSIM Value under different Types of Tampering Rate.

In order to evaluate the effectiveness of the proposed scheme, the different amounts of tampering rates are applied to the watermarked image. The experimental results have shown that the proposed scheme achieved superior quality of the recovered image under different tampering conditions. According to Fig. 9, it can be seen that the proposed scheme can achieve high image quality of the recovered image under tampering rates of 10%, 20%, 30%, 40%, and 50%. The quality of the recovered image decreased when the watermarked image tampered with the tampering rates of 60%, 70%, 80%, and 90%. The proposed scheme can achieve PSNR values of 40db under 10% tampering rate, 35dB under 30% tampering rate, and significantly decrease to 20dB under 60% tampering rate. The proposed scheme produced a high-quality image in terms of SSIM value of 0.99 under tampering rates of 10%, 20%, 30%, 40%, and 50%, while it suddenly decreased when the watermarked image was tampered with at a 60% tampering rate. The visual tamper detection and recovered image from the tamper attack are shown in Fig. 10.

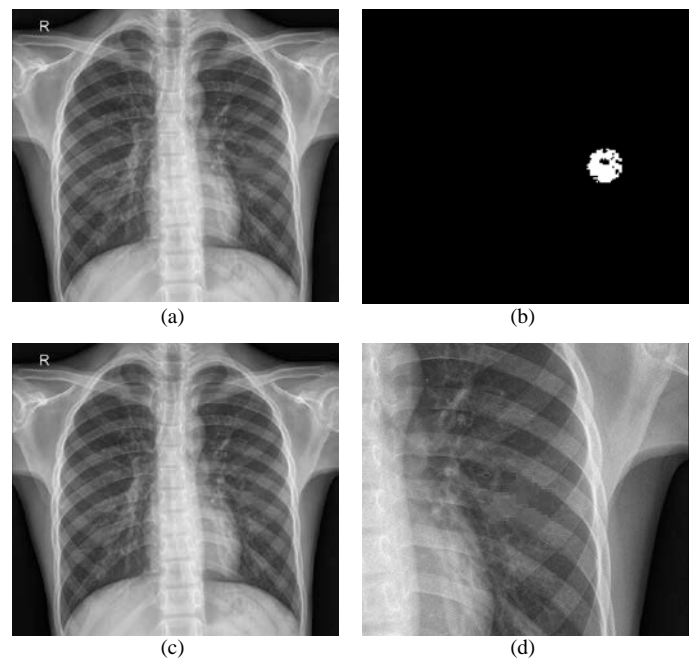


Fig. 10. (a) Tampered Image, (b) Tamper Detection, (c) Image Recovery, (d) Image Recovery with Zoom in 200%.

According to Fig. 10, the proposed scheme was able to recover the tampered image using the mosaic attacks. Fig. 10(a) shows the tampered “Chest” image by a mosaic attack where the tampered area is shown on the right side. Fig. 10(b) presented that the proposed scheme can show the tamper localization as shown in the white color. The proposed scheme can achieve a detection rate value of 85.23% for the tampered “Chest” image. Next, Fig. 10(c) shows the recovered “Chest” image, and the recovered image with zoom in 200% is shown in Fig 10(d). According to Fig. 10(d), our scheme can achieve high quality of the recovered image, it is closer to the original medical image. In addition, the proposed scheme can achieve high accuracy of tamper detection. The visual comparison of the recovered image between Hisham et al. [2] and the proposed scheme is shown in Table V. The detail visual tamper detection and recovered image under various attacks is shown in Tables VI and VII.

V. CONCLUSION

This research has presented self-embedding a watermark for medical image authentication and recovery. The watermark bits have been generated from its image content; it consists of two authentication bits and seven recovery bits. The first authentication bit is obtained from the comparison between an average pixel of sub-block and block image. The second authentication bit has been generated from the parity bits of each sub-block. The recovery bits are determined by finding the median value of each sub-block. The recovery bits are embedded in the different locations based on spiral block mapping. The proposed scheme maps the first half of spiral inward mapping to the second half of the spiral block mapping.

TABLE V. VISUAL COMPARISON OF THE QUALITY OF THE RECOVERED BITS UNDER VARIOUS TAMPERING RATES

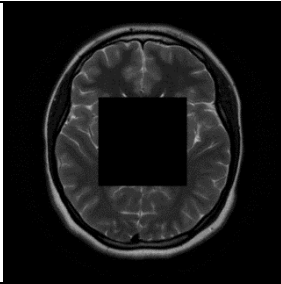
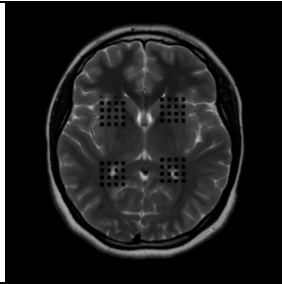
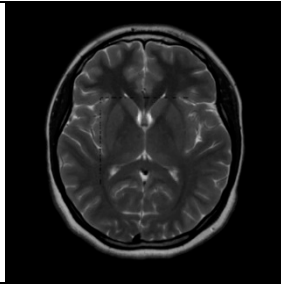
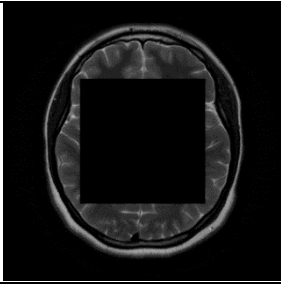
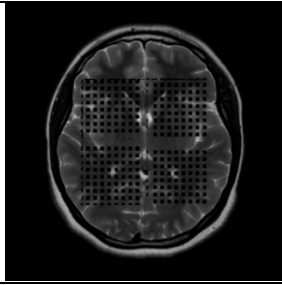
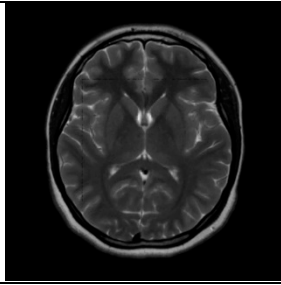
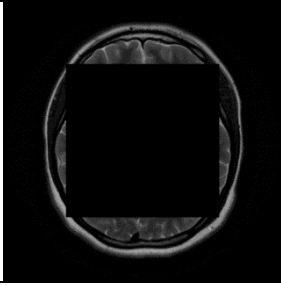
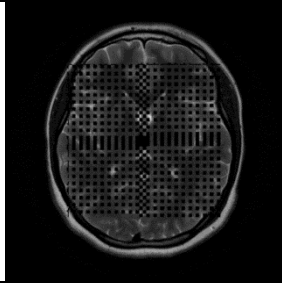
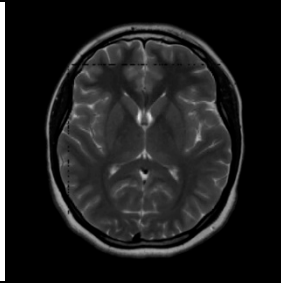
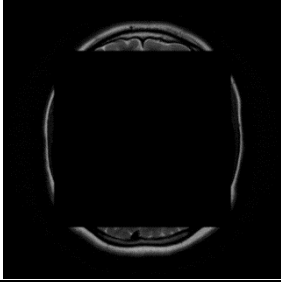
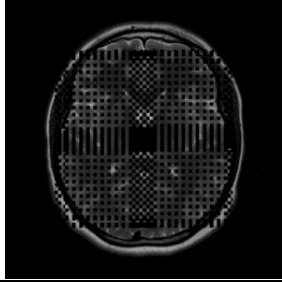
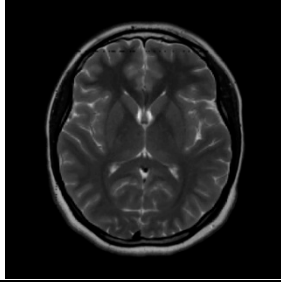
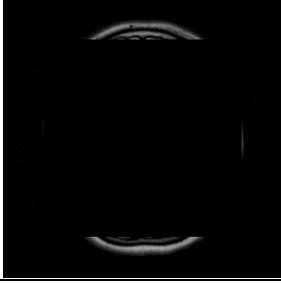
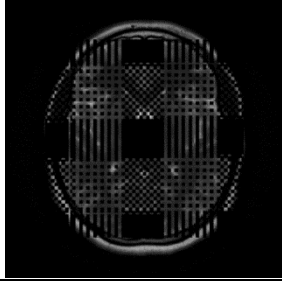
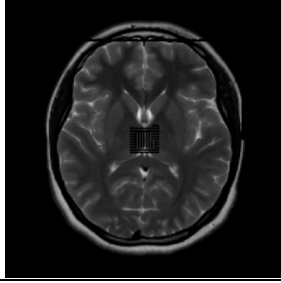
Tampered Image (Tampering rate)	Recovered Image	
	Hisham et al. [2] (PSNR / SSIM)	Proposed Method (PSNR / SSIM)
		
Tamper rate: 10 %	31.6484 dB / 0.9516	39.9283 dB / 0.9885
		
Tamper rate: 20%	25.8563 dB / 0.8368	37.8172 dB / 0.9822
		
Tamper rate: 30%	22.2600 dB / 0.7372	34.6273 dB / 0.9744
		
Tamper rate: 40%	19.9915 dB / 0.6550	33.5292 dB / 0.9754
		
Tamper rate: 50%	18.1313 dB / 0.5677	29.0157 dB / 0.9533

TABLE VI. VISUAL TAMPER DETECTION AND RECOVERED IMAGE FROM THE PROPOSED SCHEME UNDER VARIOUS TAMPER ATTACKS


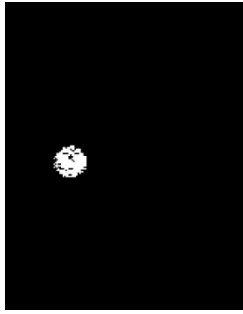

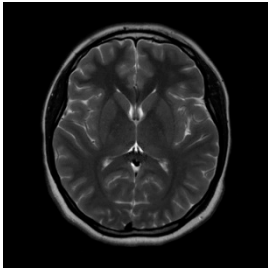
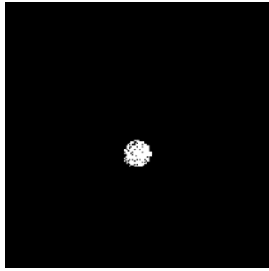
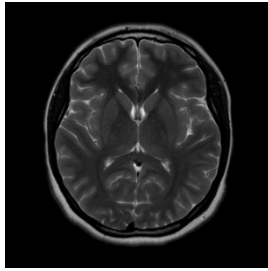
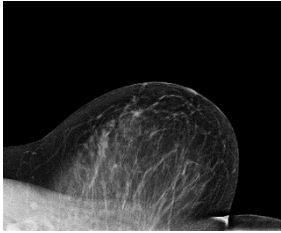
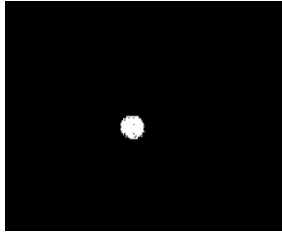
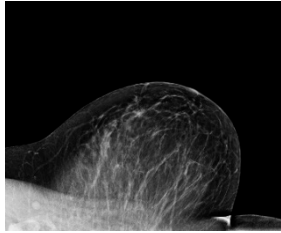
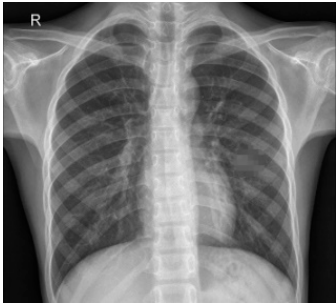
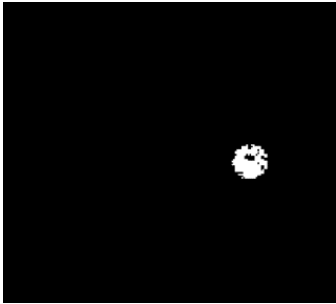
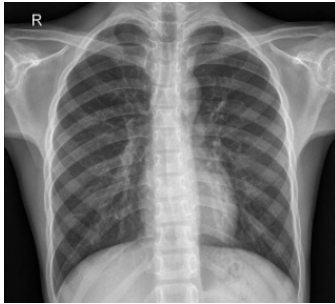
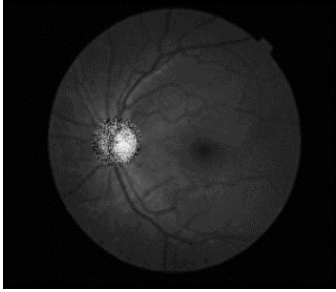

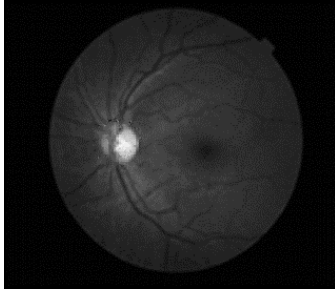
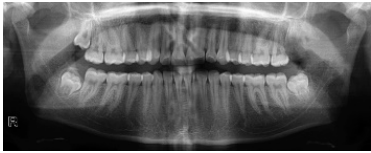

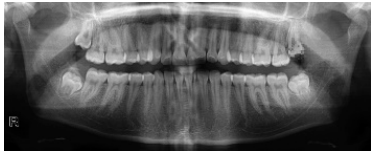

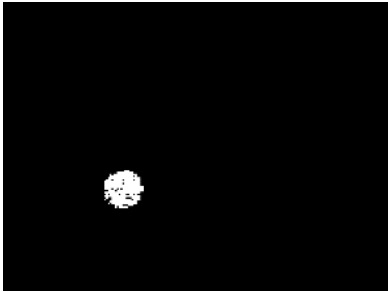

Tampered Image (Tampering rate)	Tamper Detection (TPR / FNR / FPR)	Recovered Image (PSNR / SSIM)
		
Blurring 0.94 %	0.8566 / 0.1434 / 0.0012	49.4710 dB / 0.9988
		
Unsharp masking 0.70 %	0.8642 / 0.1358 / 0.0010	45.4482 dB / 0.9955
		
Cloning 0.64 %	0.9523 / 0.0477 / 0.0006	46.8068 / 0.9985

TABLE VII. VISUAL TAMPER DETECTION AND RECOVERED IMAGE FROM THE PROPOSED SCHEME UNDER VARIOUS TAMPER ATTACKS

Tampered Image (Tampering rate)	Tamper Detection (TPR / FNR / FPR)	Recovered Image (PSNR / SSIM)
		
Mosaic 0.8 %	0.8523 / 0.1477 / 0.0014	48.8064 dB / 0.9984

		
Noise 2.01 %	0.8790 / 0.1210 / 0.0023	39.6542 dB / 0.9812
		
Removal 1.35 %	0.8409 / 0.1591 / 0.0013	42.9007 dB / 0.9935
		
Sharpening 0.91 %	0.8962 / 0.1038 / 0.0011	40.4584 / 0.9975

The watermarked images have been tampered with using different types of attacks. The proposed scheme was also evaluated by using tampering ratios of 10%, 20%, 30%, 40%, and 50% tampering rates. The experimental results show that it can improve the accuracy of tamper detection. The scheme achieved an average TPR value of 0.87 and an accuracy of 93%. In addition, the proposed scheme performed superior quality of the recovered image than the existing benchmark. The proposed scheme achieved high accuracy of the recovered image under various tamper attacks with a PSNR value of 44.79 dB and an SSIM value of 0.994.

ACKNOWLEDGMENT

This work was supported by Universiti Malaysia Pahang through the Research Grant Scheme (RDU190370).

CONFLICT OF INTEREST

On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES

- [1] T. Tuncer and M. Kaya, "A novel image watermarking method based on center symmetric local binary pattern with minimum distortion," *Optik (Stuttg.)*, vol. 185, pp. 972–984, May 2019, doi: 10.1016/j.ijleo.2019.04.038.
- [2] S. I. Hisham, A. N. Muhammad, G. Badshah, N. H. Johari, and J. Mohamad Zain, "Numbering with spiral pattern to prove authenticity and integrity in medical images," *Pattern Anal. Appl.* 2016 204, vol. 20, no. 4, pp. 1129–1144, May 2016, doi: 10.1007/S10044-016-0552-0.
- [3] B. Bolourian Haghghi, A. H. Taherinia, and R. Monsefi, "An Effective Semi-fragile Watermarking Method for Image Authentication Based on Lifting Wavelet Transform and Feed-Forward Neural Network," *Cognit. Comput.*, vol. 12, no. 4, pp. 863–890, Jul. 2020, doi: 10.1007/s12559-019-09700-9.
- [4] F. Ernawan, "Robust Image Watermarking Based on Psychovisual Threshold," *Journal of ICT Research and Applications*, vol. 10, no. 3, pp. 228–242, 2016, doi: 10.5614/itbj.ict.res.appl.2016.10.3.3.
- [5] B. Feng, X. Li, Y. Jie, C. Guo, and H. Fu, "A Novel Semi-fragile Digital Watermarking Scheme for Scrambled Image Authentication and Restoration," *Mob. Networks Appl.* 2019 251, vol. 25, no. 1, pp. 82–94, Jan. 2019, doi: 10.1007/S11036-018-1186-9.
- [6] H. Rhayma, A. Makhloufi, H. Hamam, and A. Ben Hamida, "Semi-fragile self-recovery watermarking scheme based on data representation through combination," *Multimed. Tools Appl.*, vol. 78, no. 10, pp. 14067–14089, May 2019, doi: 10.1007/s11042-019-7244-x.
- [7] R. Huang, H. Liu, X. Liao, and S. Sun, "A divide-and-conquer fragile self-embedding watermarking with adaptive payload," *Multimed. Tools Appl.* 2019 7818, vol. 78, no. 18, pp. 26701–26727, Sep. 2019, doi: 10.1007/s11042-019-07802-y.
- [8] A. Aminuddin and F. Ernawan, "AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking," *J. King Saud Univ. - Comput. Inf. Sci.*, Feb. 2022, doi: 10.1016/J.JKSUCI.2022.02.009.
- [9] X. Yuan, X. Li, and T. Liu, "Gauss–Jordan elimination-based image tampering detection and self-recovery," *Signal Process. Image Commun.*, vol. 90, p. 116038, Jan. 2021, doi: 10.1016/j.image.2020.116038.
- [10] D. Singh and S. K. Singh, "Block Truncation Coding based effective watermarking scheme for image authentication with recovery capability," *Multimed. Tools Appl.* 2017 784, vol. 78, no. 4, pp. 4197–4215, Feb. 2019, doi: 10.1007/S11042-017-5454-7.
- [11] J. Molina-Garcia, B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy, and C. Cruz-Ramos, "An effective fragile

- watermarking scheme for color image tampering detection and self-recovery,” *Signal Process. Image Commun.*, vol. 81, p. 115725, Feb. 2020, doi: 10.1016/j.image.2019.115725.
- [12] A. Singh and M. K. Dutta, “A robust zero-watermarking scheme for tele-ophthalmological applications,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 8, pp. 895–908, Oct. 2020, doi: 10.1016/j.jksuci.2017.12.008.
- [13] J. Molina, V. Ponomaryov, R. Reyes, S. Sadovnychiy, and C. Cruz, “Watermarking Framework for Authentication and Self-recovery of Tampered Colour Images,” *IEEE Lat. Am. Trans.*, vol. 18, no. 3, pp. 631–638, Mar. 2020, doi: 10.1109/TLA.2020.9082736.
- [14] S. Prasad and A. K. Pal, “A Secure Fragile Watermarking Scheme for Protecting Integrity of Digital Images,” *Iran. J. Sci. Technol. - Trans. Electr. Eng.*, vol. 44, no. 2, pp. 703–727, Jun. 2020, doi: 10.1007/s40998-019-00275-7.
- [15] W. Belferdi, A. Behloul, and L. Noui, “A Bayer pattern-based fragile watermarking scheme for color image tamper detection and restoration,” *Multidimens. Syst. Signal Process.*, vol. 30, no. 3, pp. 1093–1112, Jul. 2019, doi: 10.1007/s11045-018-0597-x.
- [16] O. Hemida, Y. Huo, H. He, and F. Chen, “A restorable fragile watermarking scheme with superior localization for both natural and text images,” *Multimed. Tools Appl.* 2018 789, vol. 78, no. 9, pp. 12373–12403, May 2019, doi: 10.1007/s11042-018-6664-3.
- [17] S. Mushtaq and A. H. Mir, “Digital Image Forgeries and Passive Image Authentication Techniques: A Survey,” *Int. J. Adv. Sci. Technol.*, vol. 73, pp. 15–32, 2014, doi: 10.14257/ijast.2014.73.02.
- [18] O. Hemida and H. He, “A self-recovery watermarking scheme based on block truncation coding and quantum chaos map,” *Multimed. Tools Appl.* 2020 7925, vol. 79, no. 25–26, pp. 18695–18725, Jul. 2020, doi: 10.1007/s11042-020-08727-7.
- [19] F. Tohidi, M. Paul, and M. R. Hooshmandasl, “Detection and recovery of higher tampered images using novel feature and compression strategy,” *IEEE Access*, vol. 9, pp. 1–1, Apr. 2021, doi: 10.1109/access.2021.3072314.
- [20] E. Gul and S. Ozturk, “A novel pixel-wise authentication-based self-embedding fragile watermarking method,” *Multimed. Syst.*, vol. 1, p. 3, Feb. 2021, doi: 10.1007/s00530-021-00751-3.
- [21] M. Ferroukhi, A. Ouahabi, M. Attari, Y. Habchi, and A. Taleb-Ahmed, “Medical Video Coding Based on 2nd-Generation Wavelets: Performance Evaluation,” *Electron.*, vol. 8, no. 1, p. 88, Jan. 2019, doi: 10.3390/ELECTRONICS8010088.
- [22] F. Ernawan, D. Ariatmanto, “Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels,” *International Journal of Electrical and Computer Engineering*, vol. 9, no.3, pp. 2185-2195, 2019, doi: 10.11591/ijece.v9i3.pp2185-2195.
- [23] F. Ernawan, “Tchebichef image watermarking along the edge using YCoCg-R color space for copyright protection,” *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1850-1860, 2019, doi: 10.11591/ijece.v9i3.pp1850-1860.
- [24] F. Ernawan, D. Ariatmanto, A. Firdaus, “An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients,” *IEEE Access* vol. 9, pp. 45474-45485, 2021, doi: 10.1109/ACCESS.2021.3067245.
- [25] A. Ray and S. Roy, “Recent trends in image watermarking techniques for copyright protection: a survey,” *Int. J. Multimed. Inf. Retr.* vol. 9, no. 4, pp. 249–270, Oct. 2020, doi: 10.1007/S13735-020-00197-9.
- [26] O. Hemida, Y. Huo, H. He, and F. Chen, “A restorable fragile watermarking scheme with superior localization for both natural and text images,” *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 12373–12403, May 2019, doi: 10.1007/s11042-018-0597-x.
- [27] W. Belferdi, A. Behloul, and L. Noui, “A bayer pattern-based fragile watermarking scheme for color image tamper detection and restoration,” *Multidimens. Syst. Signal Process.*, vol. 30, no. 3, pp. 1093–1112, Jul. 2019, doi: 10.1007/s11045-018-0597-x.
- [28] W. Hong, J. Chen, P. S. Chang, J. Wu, T. S. Chen, and J. Lin, “A color image authentication scheme with grayscale invariance,” *IEEE Access*, vol. 9, pp. 6522–6535, 2021, doi: 10.1109/ACCESS.2020.3047270.
- [29] E. Gul and S. Ozturk, “A novel triple recovery information embedding approach for self-embedded digital image watermarking,” *Multimed. Tools Appl.*, vol. 79, no. 41–42, pp. 31239–31264, Nov. 2020, doi: 10.1007/s11042-020-09548-4.
- [30] F. Ernawan, N.A. Abu and N. Suryana, “Adaptive tchebichef moment transform image compression using psychovisual model,” *Journal of Computer Science*, vol. 9, no. 6, pp. 716-725, 2013, doi: 10.3844/jcssp.2013.716.725.
- [31] F. Ernawan, N.A. Abu and N. Suryana, “An adaptive jpeg image compression using psychovisual model,” *Advanced Science Letters*, vol. 20, no. 1, pp. 26-31, Jan. 2014, doi: 10.1166/asl.2014.5255.
- [32] D. Ariatmanto, F. Ernawan, “An improved robust image watermarking by using different embedding strengths,” *Multimedia Tools and Applications*, vol. 79, no. 17-18, pp. 12041 - 12067, May 2020, doi: 10.1007/s11042-019-08338-x.
- [33] S. Prasad and A. K. Pal, “A secure fragile watermarking scheme for protecting integrity of digital images,” *Iran. J. Sci. Technol. - Trans. Electr. Eng.*, vol. 44, no. 2, pp. 703–727, Jun. 2020, doi: 10.1007/s40998-019-00275-7.