A Quick Glance at Digital Watermarking in Medical Images

Technique Classification, Requirements, Attacks and Application of Tamper Localization

Syifak Izhar Hisham[*1], Siau-Chuin Liew[2], Jasni Mohd Zain[3]

Faculty of Computer Systems and Software Engineering,Universiti Malaysia Pahang
Lebuhraya Tun Razak, 26300 Gambang Kuantan, Pahang Darul Makmur, Malaysia
[*1]penawar85@gmail.com; [2]liewsc@ump.edu.my; [3]jasni@ump.edu.my

***Abstract*- Digital watermarking is seen as a necessary and important field to be developed since the attacks and manipulations of digital documents and media are actively done. This paper surveys and reviews some basic theory about digital watermarking, such as the technique classification, requirements and possible attacks nowadays. Since all data in medical images are significantly important, the demand for the authentication is high. Therefore, this paper also focuses on a specific application of digital image watermarking for medical images which are tamper localization.**

Keywords- Digital Watermarking; Tamper Localization; Medical Image; Tampering Detection; Review

I. INTRODUCTION

Nowadays it is a trend to create, store and distribute data in digital multimedia data format. In general, multimedia brought many benefits to society. For instance, the good quality of the image and voice as well, easily send or receive messages and important documents, which make our life easier and convenience. However, this revolution helps the pirates to exploit these features for their own intended purpose illegally [1].

Therefore, the demand for the authentication methods of digital media becomes significant issue in order to ensure that work has not been tampered with, especially for some cases like national security, medical safety, internet banking and transfer of military information and forensic investigations. In terms of medical use, a major concern among the clinical professionals is that the probability of being modified by attacker, thus, the demand for the authentication and originality is high [2, 3].

Image authentication can assure receivers that the received image is from the authorized source and that the image content is identical to the one sent [4]. Nowadays, even by using generic software for image elaboration, a medical image can be attacked by erasing or adding any sign of disease onto it. If this image were a critical piece of evidence in a legal case or police investigation, this form of tampering might pose a serious problem.

Researchers recognized that image authentication techniques are applied using two kinds of tools, digital signature and watermarking [4].A digital signature is non-repudiation, encrypted version of the message digest extracted from the data. It is usually stored as a separate file, which can be attached to the data to prove integrity and originality. Watermarking techniques consider the image as a communication channel. The embedded watermark, usually imperceptible, may contain either a specific producer ID or some content-related codes that are used for authentication [5, 6, 7, 8].

For comparison, digital signature is appended in the header of an image file, which may be easily stripped off, for instance, when the file is opened and saved in a different format. While in digital watermarking, the authentication information is directly embedded into the image data, which the authentication information survives even when the host image undergoes format conversions. Another advantage is the digital watermark's capability for isolating manipulated image regions. This functionality is known as the tamper localisation property [4].

A digital watermarking system considered as a solution for preserve the integrity, confidentiality and the authenticity of medical images. Among the recent authenticity concepts are tamper localization, reversible and recovery scheme [9]. This paper surveys the classification, requirements, attacks and the need of the watermarking, specifically on medical images.

II. TECHNIQUE CLASSIFICATION OF IMAGE WATERMARKING

Watermarking techniques can be classified according to how the watermark is embedded [1, 10]. Mainly, it is divided into two broad categories, spatial domain and transform domain [11].

A. Spatial Domain

One of the earliest and most simple techniques is to embed the watermark information into the least significant bits (LSBs) of the image [11, 12]. The watermarks are embedded in the last bit of selected pixels of an image. Since a change in LSB

DOI: 10.5963/BER0202004

corresponds a change in one unit of image gray value, its modification is not perceivable by human eyes [13]. This technique does not produce serious distortion to the original image. It is not as robust as transform domain techniques and rarely survives various attacks.

Therefore, usually the technique is in fragile watermarking which the aim is to be destroyed and become undetectable after the image has been modified in any way. If a fragile watermark is detected correctly in an image, we can say that the image has not been altered or tampered with since the watermark has been embedded [4].Such techniques are described in [14] and [15]. These techniques embed the mark in the least significant bit plane for perceptual transparency. Another early technique which has been a reference to many researches is the one proposed by [16]. The scheme embeds a binary logo of the same size as the host image by means of a key dependent look-up table (LUT) that maps every possible pixel luminance value to either 0 or 1. The watermark is inserted by adjusting the LSB value of each image pixel in the spatial domain to match its corresponding LUT value.

A modification of position-dependent LUT is proposed by [17] to dramatically increase the search space. In another study [18] improved the algorithm by using 64x64 block cipher instead of LUT, and the watermark is embedded in a 32x32 block. The improved scheme can be used against the block analysis attack.

B. Transform Domain

Most of the transform domain techniques embed the watermark information into the transform coefficients of the cover image. The transform domain techniques produces spectral domains where watermarking can be applied. The most popular techniques in this category are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). The advantage of these techniques is they can overcome possible compression and more robust against geometric transformation such as rotation, scaling, translation and cropping; but, the disadvantage is they need a certain amount of computation which take longer time to produce [10].

A study [19] had described a technique based on a modified JPEG encoder. The watermark is inserted by changing the quantized DCT coefficients before entropy coding. A special lookup table of binary values (whose design is constrained to ensure mark invisibility) is used to partition the space of all possible DCT coefficient values into two sets. The two sets are then used to modify the image coefficients to encode a bi-level image (such as a logo).

Authentication techniques based on the wavelet transform had been proposed by [20] and [21]. The scheme in [20] embeds a mark by modifying the quantization process of Haar wavelet transform coefficients while [21] selectively inserts watermark bits by processing the image after it is in a compressed form.

In Table 1, we illustrate the strength of transform domain compared to spatial domain.

TABLE I SPATIAL DOMAIN VS. TRANSFORM DOMAIN

Spatial Domain	Transform Domain
Embedding capacity is limited and not robust to common signal processing [27]	More effective and better imperceptibility [27]
Inefficient computational [27]	Robust to common signal processing [27] and many forms of attacks [22, 23]
Original image is needed [27]	No need for original image [27]
Direct embedding and Easy to implement and reacquire few computational resources [27]	Includes many schemes as DFT, FFT, FHT and DWT [27]
The watermarking scheme based on spatial domain is faster than that based on frequency domain since the step of transferring to frequency domain is not needed [28]	Among the transform domain watermarking techniques discrete wavelet transform (DWT) based watermarking techniques are gaining more popularity [29]
Spatial domain distorts the natural statistical properties of an image more than that in the frequency domain They can easily be fooled by any linear or non-linear distortion of the image, hence they cannot tolerate compression or noise [30]	Less distortion for natural of image's properties [22, 24]

III. REQUIREMENT FOR IMAGE WATERMARKING METHODS

Most image watermarking schemes try to meet the following requirements [22, 23, 24]:

A. Perceptibility

The perceptibility of a watermarked image can be judged according to its fidelity and quality. Fidelity measures the similarity between images before or after watermarking [1]. A reconstructed image that is very similar to the original has a high fidelity. A low fidelity reconstruction is dissimilar or distinguishable from the original.

DOI: 10.5963/BER0202004

The marked image must be perceptually identical to the original under normal observation. It is a challenge to researchers of making sure that the visual impact of watermarking is as weak as possible so that the watermarked image remains identical to the original [25, 26].

There are several ways to quantify the distortion to measure whether the scheme is perceptible or not. They are discussed in Section V.

B. Robustness

It should be robust against typical attacks, transmission and storage imperfections, such as compression, noise addition, format conversion, bit errors, filtering and noise reduction. For content authentication, a robust watermark may not be able to differentiate both compression and tampering.

Fragile watermarking can be an advantage for authentication purposes. If a fragile watermark is detected correctly in an image, it can be assumed that the image has not been altered or tampered with since the watermark has been embedded [13].

C. Capacity

Capacity is referred to size of the information or number of the bits encoded within unit of time or within a work. Sufficiently useful amount of information must be allowed by a watermarking scheme to be embedded into an image. The amount of information embedded is subjected to the application. A reversible watermarking scheme may need to embed more information to allow image restoration, than a watermark scheme that embeds hash value of an image for authentication purposes [13].

High capacity also let the system have the ability to restore, even partially, altered or destroyed regions in order to allow the user to know the original content of the manipulated areas [25, 26].If the watermark is applied with higher embedding strength (α),then the correlation values at binary detector will be higher, but at same time the modulate sites being more visible in the host image (losing the imperceptible) [13].

D. Computational Complexity

The watermarking scheme should not be computationally complex especially for applications where real-time embedding is desired. In a hospital environment for instance, where thousands of medical image are produced daily, watermarking process needs to be less time consuming so that the operation of the hospital is not affected. Reducing the number of computations also means lower cost for computer hardware [11].

Generally, watermarking schemes which embed in spatial domain, specifically LSB, take shorter time than schemes which embed in transform domain [11].

IV. ATTACKS TO DIGITAL WATERMARKING

Watermarked images may be vulnerable to various attacks as there is no watermarking scheme that can provide the perfect security protection needed. Reference [31] had classified watermark attacks into four categories as below.

A. Removal Attack

The aim of removal attacks is to remove the watermark signal from the watermarked image without breaking the security of the watermarking algorithm. It does not attempt to find out the encryption techniques applied or how the watermark is being embedded. This category includes compression, noising, collusion, sharpening and histogram equalization. If these methods do not remove the watermark completely, they may damage the watermark information significantly. Collusion attacks are applicable when an attacker can obtain many copies of a given data set each signed with a key or different watermark. Then the attack can be such that all the copies are being averaged and an attacker can take small parts of each different copy [32]. An example of attack by collusion is to take two separately watermarked images and average them to form another.

B. Geometry Attack

In geometry attack, the watermark signal is distorted rather than being removed from the image. It is possible to recover the original watermark if proper countermeasure is applied. Included in this category are skewing, image rotation and translation.

C. Cryptographic Attack

The aim of this kind of attack is to break the security measures applied in the watermarking schemes. Once the security measure is broken, the embedded watermark is removed or a misleading watermark is embedded. Brute-force search is one of the techniques in this category. This technique attempts to break the security of the watermark by using a large number of known possible measures to find meaningful secret information.

DOI: 10.5963/BER0202004

D. Protocol Attack

The last category is the protocol attack. It aims at attacking the entire concept of watermarking application such as in copyright protection. The attacker adds its own watermark into an image and causes the true ownership of the image in question.

1) Copy Attacks:

The intention of this attack is not to destroy or distort the watermark, but to estimate the watermark from the watermarked data and copy this estimated watermark to some other data which are called target data. The copy attack is applicable when a valid watermark in the target data can be produced with neither the knowledge of the watermarking algorithm nor knowledge of the watermark key [33].

2) Ambiguity Attacks:

Ambiguity attacks create the appearance that a watermark has been embedded in a data when in fact no such embedding has taken place [34]. An attacker can use this attack to claim ownership of a distributed data. He/she may even be able to make an ownership claim on the original data. As such, ambiguity attacks can be considered a form of unauthorized embedding. However, they are usually considered as system attacks.

In ambiguity attacks with informed detection, the attacker defines his/her fake watermark to be a randomly generated reference pattern. He/she then subtracts this pattern from the watermarked data that had been distributed to create his/her fake original. Such, a situation is created in which both the owner and attacker can make equal claim of ownership. In ambiguity attacks with blind detection, it can be performed by constructing a fake watermark that appears to be a noise signal but has high correlation with the distributed data. However, Ambiguity attacks are unique in that they often do not require the watermarked data to be altered at all [35].

3) Scrambling attacks:

It is a system-level attack in which the samples of the data are scrambled before reaching to the watermark detector and then subsequently descrambled. The type of scrambling can be a simple sample permutation or a more sophisticated scrambling of sample values. The degree of scrambling usually depends on the detection strategy.

A well-known scrambling attack is the mosaic attack, in which an image is broken into many small rectangular patches, each too small for reliable watermark detection. These image segments are then displayed in a table such that the segment edges are adjacent. The resulting table of small images is perceptually identical to the image prior to subdivision [35]. More general scrambling attacks require the receiver of the pirated data to obtain a descrambling device or a program.

V. METHODS TO QUANTIFY DISTORTION AFTER ATTACKS

Watermarked images may bear visible or invisible distortion due to the embedding process. There are several methods to quantify distortion.

A. Mean-square error (MSE)

This is defined as:

$$MSE = \frac{1}{n}\sum_{i}^{n}(I'_i - I_i)^2$$

which is the average term by term difference between the original image, I, and the watermarked image, I'. If I and I' are identical, then MSE (I', I) = 0.Nowadays, MSE is not widely used to quantify distortion because of the poor estimation of the true fidelity [4]. A better method has been introduced as peak signal-to-noise ratio (PSNR).

B. Peak signal-to-noise ratio (PSNR)

A related measure of MSE is defined as PSNR as stated:

$$PSNR\ (db) = 10\ \log_{10}\frac{\max I^2}{MSE}$$

Where max I is the peak value of the original image We will get the PSNR as infinity if MSE is 0, which means both signals are identical. PSNR is often used as a measurement for image fidelity in researches. A high PSNR means the image has a high fidelity.

C. Structural similarity index measure (SSIM)

The SSIM is also a well-known quality metric used to measure the similarity between two images, I and I'. According to

DOI: 10.5963/BER0202004

[37], SSIM is designed by modeling any image distortion as a combination of three factors that are loss of correlation, luminance distortion and contrast distortion.

The SSIM is defined as:

$$\text{SSIM}(I,I') = l(I,I')c(I,I')s(I,I'),$$

where

$$l(.I,I') = \frac{2\mu_I\mu_{I'} + C_1}{\mu_I^2 + \mu_{I'}^2 + C_1},\ c(I,I') = \frac{2\sigma_I\sigma_{I'} + C_2}{\sigma_I^2 + \sigma_{I'}^2 + C_2},\ s(\text{I,I}') = \frac{\sigma_{II'} + C_3}{\sigma_I\sigma_{I'} + C_3}.$$

It is considered to be correlated with the quality perception of the human visual [38]. The first term, $l(I,I')$ is the luminance comparison function which measures the closeness of the two images' mean luminance ($\mu_I$and$\mu_{I'}$). This factor is maximal and equal to 1 only if $\mu_I=\mu_{I'}$. The second term, $c(I,I')$ is the contrast comparison function which measures the closeness of the contrast of the two images. Here the contrast is measured by the standard deviation σ_Iσfand $\sigma_{I'}$.This term is maximal and equal to 1 only if $\sigma_I=\sigma_{I'}$.The third term, $s(I,I')$is the structure comparison function which measures the correlation coefficient between the two images I and I'. Note that $\sigma_{II'}$is the covariance between I and I'. The positive values of the SSIM index are in [0, 1]. A value of 0 means no correlation between images, and 1 means that I=I'. The positive constants C_1, $C_2$and $C_3$are used to avoid a null denominator [38].

There is no specific rule in choosing PSNR or SSIM when evaluation of image quality is required [38]. Unlike MSE value which will not be affected by some attacks [37], and might lead to false assumption, PSNR value can be predicted from the SSIM value and vice-versa [38]. Their main difference is on the sensitivity degree to attacks. In this paper, most of the papers that are reviewed used PSNR to evaluate the quality. Only one study evaluates with both methods.

VI. APPLICATION OF DIGITAL IMAGE WATERMARKING: TAMPER LOCALIZATION FOR MEDICAL IMAGES

From the Section IV, we can see that removal attack is a crucial problem to medical images. One of the requirements of an effective watermarking based authentication system as defined by [39] is the ability to identify manipulated area or also known as localization where the authentication watermark should be able to detect the location of manipulated areas, and verify other areas as authentic.

Reference [40] proposed a reversible scheme with tamper localization based on difference expansion. This scheme partitions an image into certain non-overlapping regions and appending the associated local authentication information directly into the watermark payload. The scheme also introduces the concept of region of authentication (ROA). ROA is a region used for integrity authentication or in other words, the area that needs to be protected. A ROA, which can be flexibly defined by the user, is partitioned into small regions as an image block or polygonal region in a multilevel hierarchical manner. The novelty of this scheme is that the information about the ROA is embedded as part of the watermark. The ROA will be used to reconstruct the ROA in the verification process. A hashing function is used to produce digital signatures for each image block which are then added to the watermark payload. In order to verify the authenticity of the image, the process starts by comparing the signature for the whole image. If the initial verification process fails, the ROA will be reconstructed. The signatures for the ROA will be compared to detect any tampering.

An interesting technique is used in the tamper localization process where an output image consists of shadings of the ROA is produced. The shading is used to reflect the level of confidence in the integrity of the ROA where light shadings correspond to high confidence value and dark shadings correspond to low confidence value. The tamper localization has the accuracy of up to 32 x 40 pixels. Ultrasound image was used in the experiment of this watermarking scheme and quality of the watermarked image is crucial especially for medical diagnoses. The perceptibility of the watermarked ultrasound image is not known as the measurement of the distortion level of watermarked image was not done in the experiment.

Reference [41] also proposed a tamper localization watermarking scheme that uses pixel value modification in order to allow the watermark to be reversible. The image is divided into 16 x 16 pixel blocks and Cyclic Redundancy Check (CRC) is computed for each block. Each CRC is embedded into its own block and in the event that the CRC cannot be embedded into its own block, the remaining bits will be carried over to the next block. The watermarked image can be verified by extracting the watermark and comparing the CRC of each block. Any mismatch of CRC values during comparison indicates tampering and the tampering localization accuracy is within 16 x 16 pixels. Medical images were watermarked and the PSNR of the watermarked images was between 34.0 and35.0 dB. The disadvantage of this scheme is that in order to allow reversibility, all pixel value needs to be increased by four pixel values during the embedding process to prevent bit overflow and thus the maximum pixel value allowable in an image to be watermarked had been constrained.

Both schemes proposed by [40] and [42] operate in the spatial domain and have tamper localization and reversible capability. The schemes might be able to identify the area of tampering but tampered region cannot be recovered. Recovery of the tampered region is useful in order to know exactly what had been tampered and the motive of the tampering.

Reference [42] proposed a reversible tamper localization scheme with tampered region recovery capability. This scheme is

DOI: 10.5963/BER0202004

based on a difference expansion scheme proposed by [43]. It was modified to allow the watermark to be embedded into the transform domain by using the integer Haar wavelet transform. The image is first divided into blocks. The recovery information is generated by taking the average pixel value of each block and embedded as watermark. The watermark is encrypted before the embedding process as a security feature. The whole image can be verified by comparing the retrieved average pixel value from the watermark with the current average pixel value of the image. Any mismatch indicates tampering and tampered region can be localized to an accuracy of 4 x 4 pixels. The tampered block is recovered using the average pixel value retrieved from the watermark. The advantage of this scheme is that it can be modified to allow applying the watermarking process to a defined ROI rather than to the whole image. The recovery information of the ROI is stored as the exact pixel value rather than average pixel values. Mammograms were watermarked and have the PSNR between 36.4 and40.5 dB.

Reference [44] proposed a scheme that consists of two types of watermark. The first watermark is embedded into spatial domain and the second watermark is embedded into transform domain. The image is first divided into 16x16 pixel blocks. The first watermark consists of patient's data and the hash value of the ROI and is embedded into the ROI itself by using a modified difference expansion technique. An embedding map of the ROI is produced to form a second watermark together with compressed recovery information of ROI and average value of each block in the ROI. The second watermark is compressed and embedded into the region of non- interest (RONI) using a DWT technique. Tamper localization is done by comparing the average value of each block in the ROI with the retrieved average value from the watermark. Tampered blocks can be recovered using the compressed ROI. It was claimed that this scheme is robust against salt and pepper attack and cropping. A watermarked ultrasound image has the PSNR of 36.7 dB.

Earlier research by [45] had also produced a tamper localization and recovery watermarking scheme. It also uses block based technique where each block consists of 8 x 8 pixels. Each block is then divided into sub-blocks of 4 x 4 pixels.

A three-tuple watermark embedded consists of a two-bit authentication watermark and a seven -bit recovery watermark for other sub-block. Average intensity of a corresponding block and its sub-blocks is calculated to generate the authentication watermark. Average intensity of a sub-block is embedded as the seven-bit recovery watermark in another block which was predetermined in a mapping sequence. A parity bit is generated based on the seven-bit recovery watermark. Tamper localization is done by comparing the average intensity and parity bit. Blocks that were marked invalid are recovered using the embedded average intensity of the sub-block. The watermarked ultrasound image has a PSNR of 54.8 dB. This scheme was evaluated to know whether watermarked medical images affect clinical diagnoses. The study was done by [5] by adding an additional hash function to the existing watermarking scheme. Various types of medical images were watermarked and an ultrasound image has a PSNR of 54.2 dB with the total watermark bits of 480K. The watermarked images were assessed by radiologists and it was concluded that watermarked images did not alter clinical diagnoses. The disadvantage of this scheme is that it is not reversible. The original image is generally preferred by radiologist for diagnostic purposes [41]. Although it has been clinically evaluated, an option should be given to allow the watermark to be removed and the original image to be restored by request.

Reference [46] applied hash function to image blocks and embed the hash values into the LSBs of the corresponding blocks. They also used vector quantization to compress an image by producing an index table which can be used for image recovery. The index table is embedded into the second and third LSB of each pixel. Each block of the image is authenticated using the embedded hash value. Index table is used to reconstruct an image when tampering is detected. Tampered block is recovered using blocks from the reconstructed image. Non-medical image was watermarked with the PSNR of only 29.3 dB.

Reference [47] proposed an improved scheme which enables the detection of a tampered region and then recovers it by using the embedded information selected as the recovery feature. To extract the recovery feature, they analysed the image homogeneity using quad-tree decomposition. It divides a square image into several variable-sized blocks adaptively, and chooses the average value of each block as the feature. This method produces a more efficient length of the feature while ensuring that the visual quality of the restored image is better than the method proposed by [48]. The method had been experimented in CT image and MRI image. The PSNR for 12-bit CT image is 65.76 dB and is 89.3 dB for 16-bit MRI image. The values were improved from the result by [48].

Reference [49] proposed a scheme called Tamper Localization and Lossless Recovery Watermarking Scheme with ROI Segmentation and Multilevel Authentication (TALLOR-RSMA), which is the enhancement of the tamper localization and lossless recovery (TALLOR) [50] scheme. The quality of the watermarked images using this scheme is high, with the average PSNR of 48.7 dB for the proposed scheme. Significantly, the recovered images were identical with the original images. This was proven after comparing the hash values from the original and recovered images. The method used in the TALLOR-RSMA scheme proved effective in reducing the tamper localization and recovery average processing time by approximately 50% compared with the TALLOR scheme.

A comparison between this scheme and the tamper localization and recovery scheme proposed by [44] which is described previously has been done. The data were based on an experiment performed on an ultrasound image. The comparison result shows that TALLOR-RSMA scheme is better in terms of embedding capacity and PSNR. The tamper localization accuracy of

DOI: 10.5963/BER0202004

the proposed scheme is at one pixel compared with 16×16 pixels in the [44] scheme. The recovered ROI produced by TALLOR-RSMA is also of better quality due to exact recovery achieved.

Table II shows the summary of the schemes discussed above.

TABLE II SUMMARY OF TAMPER LOCALIZATION WATERMARKING FOR MEDICAL IMAGES

Researcher	Characteristic	PSNR
Guo and Zhuang (2009)	Tamper localization and reversible capability	N/A
Tan et al. (2011)	Tamper localization and reversible capability	34.0 – 35.0 dB
Chiang, K. Chang, R. Chang and Yen (2008)	Tamper localization, reversible and recovery capability	36.4 – 40.5 dB
Osamah and Khoo (2011)	Tamper localization and recovery capability	36.7 dB
Jasni and Abdul (2006)	Tamper localization and recovery capability	54.8 dB
Yang and Shen (2010)	Tamper localization and recovery capability	29.3 dB
Kim, M. J. Lee, J. W. Lee, Oh and H. Y. Lee (2011)	Tamper localization and recovery capability	For 12-bit CT image – 65.76 dB, For 16-bit MRI image – 89.3 dB
Liew (2012)	Tamper localization and lossless recovery	48.7 dB

VII. DISCUSSION

There are many watermarking schemes that aim for authentication verification. They have reversible, tamper localization and/or recovery applications. All schemes reviewed under tamper localization section in this paper were designed specifically for usage in medical images. All schemes have tamper localization capability and a majority has recovery capability. The watermarked images have the PSNR of between 29.3 to 89.3 dB. The schemes that have recovery capability operate in the transform domain are more robust against attack but require more complex computation. Eventually it needs more watermarking processing time.

From eight localization and tamper recovery schemes reviewed in this paper, seven of them work on the spatial domain. They are fragile watermarking. Many schemes find spatial domain is more suitable for authentication watermarking. In the case of authenticity, a fragile watermark has to prove that the image has been modified and is no longer authentic. If a fragile watermark is detected correctly in an image, we can say that the image has not been altered or tampered with since the watermark has been embedded.

Reference [47] proposed a unique scheme, where it works on both spatial and transform domain. It is a semi-fragile watermarking. It is claimed as robust against salt and pepper attack and cropping, however, the PSNR showed that the fidelity is average.

Scheme that operates in the spatial domain developed by [49] produces watermarked image that has high PSNR and has the reversible capability. The recovered image can get exact recovery. The schemes by [47] produce the highest PSNR among those studies in this paper, which is 65.76 dB for 12-bit image and is 89.3 dB for 16-bit image. The scheme had been tested to not only medical images like CT scan and MRI, but also general images. The PSNR and SSIM showed excellent result in recovery and high quality [49].

VIII. CONCLUSIONS

This paper surveys from some basic knowledge of digital watermarking, includes the techniques classification, requirements, and attacks of digital watermarking. This paper also reviews studies about an application of watermarking for medical images which are tamper localization. We focus on tamper localization since medical image should have a special security system from data manipulation and be very sensitive to any distortion and attacks. There are, still, many limitations and areas that should be developed for tamper localization, such as other modalities of medical images should be studied and implementation in the real data system at hospital should be done and evaluated.

REFERENCES

[1] I. J. Cox, M. L. Miller, andJ. A. Bloom, “Digital watermarking”, Morgan Kaufmann, San Francisco, 2002.

[2] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland and R. Collorec, “Relevance of watermarking in medical imaging”,Proc IEEE EMBS Information Technology Applications in Biomedicine, Arlington, VA 2000, pp. 250–255, 2000.

[3] C. K. Tan, C. Ng, X. Xu, C. L. Poh, L. G. Yong andK. Sheah, “Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability”, J Digit Imaging, 24(3):528–540.

[4] M. Z. Jasni, “Digital watermarking in medical images”, PhD thesis, Brunel University, 2005.

[5] M. Z. Jasni, R. M. F. Abdul, and 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, 2006, pp.5459-5462.

DOI: 10.5963/BER0202004

[6] Lin, Ching-Yung, "Watermarking and digital signature techniques for multimedia authentication and copyright protection", PhD diss., Columbia University, 2000.

[7] Penumarthi, Kiranmayi, and Subhash Kak. "Augmented watermarking."Cryptologia 30, no. 2 (2006): 173-180.

[8] Shaw, Sandy. "JISC Technology Applications Programme (JTAP)—Overview of Watermarks, Fingerprints, and Digital Signatures." (1999).

[9] Syifak I. H., S. C. Liew and Jasni M. Z., "A quick glance at digital watermarking in PACS", International Conference on Computational Science and Information Management (ICoCSIM), 3-5 December 2012, Parapat, Indonesia.

[10] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones, "Analysis of Digital Image Watermark Attacks", Proceedings of the 7th IEEE Consumers Communications and Networking Conference, 2010, pp. 1-5.

[11] S. C. Liew, and M. Z. Jasni, "A Review of Medical Image Watermarking and Its Implementations", Proceedings of Malaysian Technical Universities Conference on Engineering and Technology (MUCEET2009), 20-22 June 2009, Kuantan, Pahang, Malaysia.

[12] G. N. Mehta, Y. Kshirsagar, and A. Tankariya, "Digital Image Watermarking", International Journal of Scientific Engineering and Technology, 2012, Volume No. 1, Issue No. 2, pg: 169 – 174.

[13] S. C. Liew, "Tamper Localization and Recovery Watermarking Schemes for Medical Images in PACS", Doctor of Philosophy (Computer Science) Thesis, Universiti Malaysia Pahang, Malaysia, 2011.

[14] S. Walton, "Information authentication for a slippery new age", Dr. Dobbs, 1995.

[15] Journal, 20(4), pp. 18-26.R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark", Proceedings of 1st International Conference on Image Processing, Austin, TX, USA, IEEE Computer Society Press, pp. 86-90, 13-16Nov 1994.

[16] M. M. Yeungand F. C. Mintzer, "Invisible watermarking for image verification", Journal of Electronic Imaging, 7(3), pp. 578-591, 1998.

[17] N. Memon, S. Shendeand P. Wong, "On the security of the Yueng-Mintzer Authentication Watermark", Final Program and Proceedings of the IS&T PICS 99, Savannah, GA, USA, The Society for Imaging Science and Technology, pp. 301-306, April 1999.

[18] J. Fridrich, M. Goljan and A. C. Baldoza, "New fragile authentication watermark for images", International Conference on Image Processing (ICIP 2000), September 10-13 2000 Vancouver, BC, IEEE Computer Society pp. 446-449.

[19] M. Wu, and B. Liu, "Watermarking for image authentication", Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 2 (of 3), Oct 4-7 1998, Los Alamitos, CA, USA, IEEE Computer Society, pp. 437-441.

[20] D. Kundur and D. Hatzinakos, "Towards a telltale watermarking technique for tamper-proofing", Proceedings of IPCIP'98 International Conference on Image Processing, 4-7 Oct. 1998 Chicago, IL, USA, IEEE Computer Society, pp. 409-13.

[21] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking", Proceedings of the 1998 International Conference on Image Processing, ICIP. Part 2 (of 3), Oct 4-7 1998, Los Alamitos, CA, USA, IEEE Computer Society, pp. 427-431.

[22] I. J. Cox, M. L. Miller, and J. M. G. Linnartz, "A review of watermarking principles and practices". IEEE Digital Signal Processing for Multimedia System, 1999, 1:461-482.

[23] M. Kutter, and F. Hartung, "Introduction to watermarking techniques", Information Techniques for Steganography and Digital Watermarking, 1999, 1:97-119.

[24] P. Meerwald, andA. Uhl, "Watermark security via wavelet filter parameterization", Proceedings of the International Conference on Image Processing, 2001, pp.1027-1030.

[25] L. Tong and Q. Zheng-Ding, "The survey of digital watermarking-based image authentication techniques", Proceedings of International Conference on Signal Processing (ICSP), 26-30 Aug. 2002 Beijing, China, IEEE, pp. 1556-1559.

[26] C. Lin and S. Chang,"Semi-fragile watermarking for authenticating JPEG visual content", Security and Watermarking of Multimedia Contents II, Jan 24-Jan 26 2000, Bellingham, WA, USA, Society of Photo-Optical Instrumentation Engineers, pp. 140-151.

[27] A. A. Aburas, and F. O. Rashidah, "Intensive Review on Digital Watermarking", Processing of International Conference on science and technology application in industry and education(ICST). Penang Malaysia, 2008, PP2531-2536.

[28] Wei-Hung Lin, Yuh-Rau Wang, Shi-Jinn Horng, Tzong-Wann Kao, and Yi Pan, "A blind watermarking method using maximum wavelet coefficient quantization", Expert Systems with Applications,2009 Vol.36. pp. 11509–11516.

[29] R. Gantasala and M. V.N.K. Prasad, "New Quantization Technique in Semi-fragile Digital Watermarking for Image Authentication", Springer-Verlag Berlin Heidelberg, 2009.

[30] A. Cheddad, J. Condell, K. Curran, and P.McKevitt, "A secure and improved self-embedding algorithm to combat digital document forgery", Signal Processing 89 (2009) 2324–2332.

[31] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks", IEEE Communications Magazine, 2001, 39(8):118-126.

[32] K. Su, D. Kundur, and D. Hatzinakos,"Statistical invisibility for collusion-resistant digital video watermarking", IEEE Trans. on Multimedia 7(1), 43–51 (2005).

[33] M. Kutter,S. Voloshynovskiy, and A. Herrigel, "Watermark Copy Attack" IS&T 72th Annual Symposium of Electronic Imaging Security and Watermarking of Multimedia Content. 2000, Vol. 3971: 371-80. San Jose, CA.

[34] G. C. W. Ting, B. M. Goi, and S. H. Heng, "Attacks on a robust watermarking scheme based on self-reference image", Computer Standards and Interfaces 30 (2008) 32–35.

[35] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking (1st Edition)", Morgan Kaufmann Publishers. San Francisco, 2002.

[36] B. Smitha and K. A. Navas, "Spatial domain-High capacity data hiding in ROI images" Proceedings of the International Conference on Signal Processing, Communications and Networking, pp.528-533, 2007.

[37] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, 2004.

DOI: 10.5963/BER0202004

[38] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM", Proceeding ICPR '10 Proceedings of the 2010, 20th International Conference on Pattern Recognition, Pages 2366-2369, 2010.

[39] T. Liu, and Z. D. Qiu, "The survey of digital watermarking-based image authentication techniques", in Proceedings of the 6th International Conference on Signal Processing, 2002.

[40] X. Guo, and T. Zhuang, "Lossless watermarking for verifying the integrity of medical images with tamper localization", J Digit Imaging, 2009, 22 (6):620 – 628.

[41] C. K. Tan, C. Ng, X. Xu, C. L. Poh, L. G. Yong, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability", J Digit Imaging, 2011, 24(3):528–540.

[42] K. Chiang, K. Chang, R. Chang, and H. Yen, "Tamper detection and restoring system for medical images using wavelet-based reversible data embedding", J Digit Imaging, 2008, 21:77– 90.

[43] J. Tian, "Reversible data embedding using a difference expansion", IEEE Trans Circuits Syst Video Technol, 2003, 13(8):890 –896.

[44] M. Osamah, and B. E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images", J Digit Imaging, 2011, 24:114– 125.

[45] M. Z. Jasni, and R. M. F. Abdul, "Medical image watermarking with tamper detection and recovery", Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2006, pp.3270-3273.

[46] C. W. Yang, and J. J. Shen, "Recover the tampered image based on VQ indexing", Signal Processing, 2010, 90(1):331-343.

[47] K. S. Kim, M. J. Lee, J. W. Lee, T. W. Oh, and H. Y. Lee, "Region-based tampering detection and recovery using homogeneity analysis in quality-sensitive imaging", Computer Vision and Image Understanding, 115 (2011) 1308–1323.

[48] K. H. Chiang, K. C. C. Chien, R. F. Chang, and H. Y. Yen, "Tamper detection and restoring system for medical images using wavelet-based reversible data embedding", Journal of Digital Imaging. 21 (1) (2008) 77–90.

[49] S. C. Liew, S. W. Liew, and M. Z. Jasni, "Tamper Localization and Lossless Recovery Watermarking Scheme with ROI Segmentation and Multilevel Authentication", J Digit Imaging, 2012, DOI 10.1007/s10278-012-9484-4.

[50] S. C. Liew, and J. M. Zain, "Tamper localization and lossless recovery watermarking scheme", CommunComputInfSci, 2011, 179(1):555 – 566

DOI: 10.5963/BER0202004