International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:3, 2018

Medical Image Watermark and Tamper Detection Using Constant Correlation Spread Spectrum Watermarking

Peter U. Eze, P. Udaya, Robin J. Evans

***Abstract*—**Data hiding can be achieved by Steganography or invisible digital watermarking. For digital watermarking, both accurate retrieval of the embedded watermark and the integrity of the cover image are important. Medical image security in Teleradiology is one of the applications where the embedded patient record needs to be extracted with accuracy as well as the medical image integrity verified. In this research paper, the Constant Correlation Spread Spectrum digital watermarking for medical image tamper detection and accurate embedded watermark retrieval is introduced. In the proposed method, a watermark bit from a patient record is spread in a medical image sub-block such that the correlation of all watermarked sub-blocks with a spreading code, W, would have a constant value, *p*. The constant correlation *p*, spreading code, W and the size of the sub-blocks constitute the secret key. Tamper detection is achieved by flagging any sub-block whose correlation value deviates by more than a small value, ε, from *p*. The major features of our new scheme include: (1) Improving watermark detection accuracy for high-pixel depth medical images by reducing the Bit Error Rate (BER) to Zero and (2) block-level tamper detection in a single computational process with simultaneous watermark detection, thereby increasing utility with the same computational cost.

***Keywords*—**Constant correlation, medical image, spread spectrum, tamper detection, watermarking.

I. Introduction

IN a modern day healthcare system, a hospital, insurance company and the patient may be allowed to have access to and keep a copy of the patient's digital medical image scans. These medical images such as X-ray, Ultrasound (US) scans, Computed Tomography (CT) scans, Magnetic Resonance Imaging (MRI) scans and Mammography scans are often stored in digital form in either Compact Discs (CDs) or in an online retrieval system. The custodians of these medical images could modify the medical images for various reasons which might be illegal and unauthorised [1]. In order to establish the integrity and authenticity of the medical image, there is a need to detect and determine the extent to which any part of the medical image that is relevant for diagnosis has been tampered with and to what extent. Also, the process could localise the region of tampering as well as recover the modified data if possible.

Generally, image authentication by tamper detection can be achieved by either embedding a watermark in the region to be monitored or through a passive image authentication method that does not need any watermark to be embedded [2]. Wherever possible and attainable, the passive method is recommended for medical images as it does not degrade the image in any form. However, the passive method has the shortcoming that it does not often permit additional information that protects and interprets the original cover information to be included.

In Teleradiology, other information relating to patient's Electronic Medical Record (EMR) and source authentication are often needed for accurate diagnosis and also the scan itself needs to be protected from unauthorized tampering. Hence, in most practical situations, passive image authentication is not feasible. Another issue that exists with passive tamper detection is that of computational complexity.

Guo and Zhuang in [3] proposed three design principles for medical image watermarking and Steganography: (i) defining acceptable distortion tolerance for medical images, (ii) separating a medical image into a region of interest (ROI) and region of non-interest (RONI) and (iii) reversible watermarking techniques, where the watermark can be guaranteed to be removed from the ROI during diagnosis. In this research, the first principle is being explored. The second principle limits capacity especially when ROI is very large while the third principle is known to have higher computational cost and requires more side information to be transmitted with the key to enable watermark reversibility.

This work is focused on designing an efficient watermarking method that simultaneously addresses tamper detection, accurate watermark detection, security (imperceptibility of embedded watermark) and low computational cost but without compromise on the diagnostic quality of medical images. We focus on Digital Imaging and Communication in Medicine (DICOM) – compliant medical images as it is an established format for medical image communication.

The rest of this paper is organised thus: The general concept of SS watermarking is introduced in Section II. Section III reviews literature on tamper detection in medical images especially in Spread spectrum watermarking domain. Section IV defines a problem, while Section V proposed theoretical and experimental methods for its solution. Section VI

P. U. Eze is a PhD Student in the Department of Computing and Information System at The University of Melbourne, Parkville, 3010 Australia (corresponding author; e-mail: peze@student.unimelb.edu.au).

P. Udaya is a Reader in the Department of Computing and Information System at The University of Melbourne, Parkville, 3010 Australia (e-mail: udaya@unimelb.edu.au).

R. J Evans is a Professor the Electrical/Electronic Engineering Department, the University of Melbourne, Parkville, 3010 Australia (e-mail: robinje@unimelb.edu.au).

performs experiments to evaluate the theoretical backgrounds and presents results in Section VII. Section VIII discusses the results. Section IX concludes the work and includes direction for future work.

II. Spread Spectrum Watermarking

The concept of Spread Spectrum (SS) watermarking originates from spread spectrum technology. Here, a message is transmitted with a bandwidth much larger than the one required to transmit such information. This spreading across a wider band is achieved with a Pseudorandom Noise (PN) sequence with known correlation properties [4]. This ensures that the actual data being transmitted do not have a distinguishable peak to ensure that it is not easily detected or jammed within the transmission channel. This helps to achieve higher information security and robustness. The extraction of the embedded watermark could be done without requiring the original message or cover image by a process called Blind extraction [4]. This process, involves the use of the original PN sequence used in the embedding process to perform a linear correlation with the watermarked image. Blind watermarking is important in Telemedicine because a common cover image (medical image from a new patient) would not be available before hand for non-blind extraction.

For a Teleradiology system, a typical blind spread spectrum watermarking system is shown in Fig. 1. The EMR and other source authentication data could be embedded in the ROI/RONI of the medical image using additive embedding function.

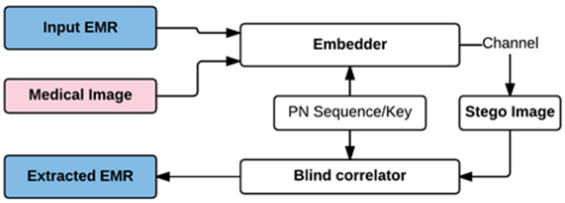

Fig. 1 SS watermarking for Telemedicine

The stego image is a combination of the medical image and the EMR and/or source authentication data. At the receiving hospital or health facility, the PN sequence used for embedding is made available and an appropriate correlation algorithm is applied to detect the watermark, authenticate image and perform watermark reversibility if necessary.

III. Related Works

Various algorithms have been designed to detect digital image forgery. These algorithms are either based on active or passive tamper detection methods. Active methods involve the addition (in spatial or transform domain) of a kind of signature which will help one to detect forgery. With the passive method, there is no access to original data and only operations on certain image features such as correlation and statistical analysis could help to detect forgery [5]. The method to be used is dependent on purpose and information available. However, in this section, our review will be limited to those closely related to active correlation coefficients of the potentially tampered regions.

Saini et al. in [5] proposed both the mean vector and correlation coefficient methods of detecting forged parts of BMP images. They experimented on about 50 original and 50 tampered images using the correlation coefficient between overlapping sub-blocks from the corresponding images, respectively. They gave a threshold of 0.025 to delineate between tampered sub-blocks and original sub-blocks. It was shown that the higher the sub-block size, the more the accuracy of the algorithm. However, their method requires the availability of both forged and original image in order to detect tampering. Hence, it is non-blind.

Singh and Goel in [7] carried out similar experiments as in [5]. However, they used up to 150 image pairs representing the original and forged ones. Correlation values between overlapping sub-blocks were used to determine image tampering. However, just like [5], the original image is required to detect tampering and also larger sub-block dimension leads to high detection accuracy. Also, both methods in [5] and [7] do not required prior embedded data, and thus, do not require watermark detection as well.

Feature vector detection method seems to be more robust against different types of tampering. Y. Gan and J. Zhong in [8] combined Tamura texture features and gray-value information to form the feature vectors for determining tampering. Tampering detection is done by computing some confidence distance between sub-blocks of the image. This algorithm achieved a false reject rate of 3%. Their algorithm is claimed to detect copy-move, rotation, Gaussian noise addition, high/low pass filtering among others. Whereas this method claims robustness to post-processing, it is only useful where no source authentication or copyright protection is necessary.

A good summary of attempts on digital image forgery detection approaches is given in [9]. They summarised most of the active and passive methods of image tampering detection based on papers published between 2003 and 2015.

For applications where watermarking is needed and more data needs to be transmitted with the medical image, it will be important to combine watermark embedding and image authentication. A usual approach for medical images is to separate the image into ROI and RONI. As proposed by Wakatani in [10], the watermark should be embedded only in the RONI. However, if the ROI is large and the required watermark cannot be accommodated in the RONI (as is often the case with spread spectrum depending of spreading factor), we need to embed some data in the ROI as well. If the data to be embedded in ROI is only for integrity and authentication, then a fragile watermarking method is good enough. However, if the watermark is part of EMR and will as well be used for tamper detection, then a combination of robust and imperceptible and/or reversible watermarking scheme is required.

Most of the literature reviewed has not solved the problem of robust but imperceptible watermarking for reliable

detection of watermark, tamper detection and preservation of diagnostic quality of medical image. In this research, we propose how these conflicting but desirable features could be achieved using the spread spectrum watermarking method.

The contribution of this paper is to introduce how a modified additive blind SS watermarking called constant correlation Watermarking method could be used for combined watermark detection and localised tamper detection for medical images. The advantages in practice include reduction in overall computational cost and increased watermark detection efficiency and accuracy. It also has the prospect of enabling increased Steganographic capacity for SS watermarking through a Constant Correlation Compression Coding Scheme (CCCCS – C_4S). This works better with medical images of high pixel depth.

IV. Notations and Problem Statement

Let $\boldsymbol{C_{MN}}$ be an original cover Medical Image of size **M** x **N**. Then $\mathbf{C_{mn}}$ is a sub-block from $\mathbf{C_{MN}}$, where **m** x **n** is the size of the sub-block. $\mathbf{m} \leq \mathbf{M}$ and $\mathbf{n} \leq \mathbf{N}$.

Let $\boldsymbol{W_{mn}}$ be pseudo-noise sequence with $\boldsymbol{N\ (0,\ 1)}$ normal distribution.

Let $\boldsymbol{S_k}$ be a vector of watermark bits of length **k** generated from the EMR Record or authentication signature.

Let $\boldsymbol{Y_{mn}}$ be a watermarked sub-block with a single bit, $S_a \in \{0, 1\}$. S_a is embedded following additive embedding method. For easy embedding into different sub-blocks of **k** watermark bits using an iterative process, the embedding equation is given in (1):

$$Y_{ij} = C_{ij} + \alpha W_{ij}\,(-1)^{S_a} \tag{1}$$

For $1 \leq i \leq m$, $1 \leq j \leq n$ and $1 \leq a \leq k$. α is the embedding or watermark strength and it controls both robustness and imperceptibility of the embedded watermark.

If a single bit is to be embedded, then k=1 and S_a is either a 0 or a 1. Then (1) transforms to (2):

$$Y_{ij} = \begin{cases} C_{ij} + \alpha W_{ij}\,, S_a = 0 \\ C_{ij} - \alpha W_{ij}\,, S_a = 1 \end{cases} \tag{2}$$

Generally, the method of blind retrieval of S_a from a single block is to perform a linear correlation between **Y** (or an attacked version, **Z**) and the PN sequence ***W***. The basic retrieval equation is given by (3):

$$S'^{(k)} = \begin{cases} 0, Corr(Y,W) > 0 \\ 1, Corr(Y,W) < 0 \end{cases} \tag{3}$$

Linear Correlation of **Y** and **W** is given as $\boldsymbol{p}$ in (4):

$$Corr(Y,W) = \boldsymbol{p} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n} Y_{ij}W_{ij} \tag{4}$$

One of the problems is that $\boldsymbol{p}$ is not often equal to zero for a block without watermark, as shown in Fig. 2. This may lead to false positives when (3) is applied for watermark detection. Hence, there is need to set a threshold, $\boldsymbol{p}_{th}$, for the accurate retrieval of a bit. Thus, $|\boldsymbol{p}|$ should be greater than $|\mathbf{p}_{th}|$ to reduce **false positives** or **false negatives** in the watermark retrieval process.

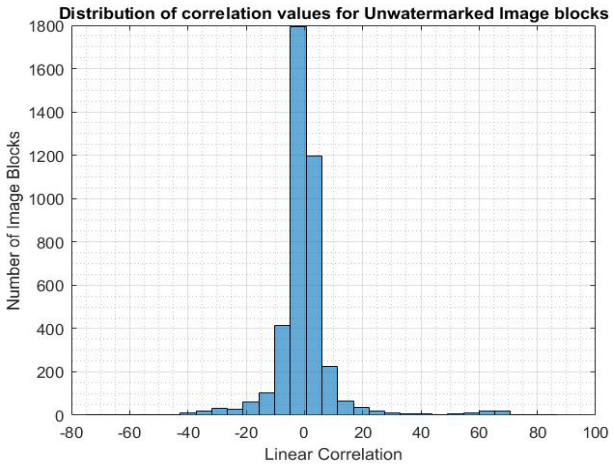

Fig. 2 Correlation values with no watermark

Though the no-watermark values are centred on 0, there are non-zero (either positive or negative) correlation values. Due to this inherent internal noise present in non-watermarked image, a threshold value, $\boldsymbol{T_h}$, is often set for retrieval of either a 0 or 1. Hence, (3) is often modified into (5) below for most practical applications.

$$S'^{(\alpha)} = \begin{cases} 0, Corr(Y,W) > T_h \\ 1, Corr(Y,W) < -T_h \end{cases} \tag{5}$$

How to determine $\boldsymbol{T_h}$ varies and still remains controversial. However, Nguen and Tuan in **[6]** argued that $\boldsymbol{T_h}$, should be approximately equal to α/2. Then another question is how to determine α to ensure a balance between robustness and imperceptibility. Further experimental evidence has shown that modification, as shown in (5), still has a lot of problems if the embedding strength α, is not properly chosen. This is illustrated in Fig. 3 for α=3.

From Fig. 3, it can be seen that there are some correlation values whose absolute value is below 1.5 (α/2) and some are even far above 1.5. This shows that an adversary can tamper with any block and correct watermark could still be retrieved provided the absolute correlation value, $\boldsymbol{p}$ lies between α/2 and ∞ (infinity). Hence, existing spread spectrum methods can ensure robust watermarking but can lead to more false positives or false negatives and are open to adversary manipulation of the cover image.

Hence, there is a need to accurately detect a watermark by eliminating host signal noise. There is also a need to robustly embed a watermark for accurate detection. For medical images, being able to detect tampering while solving these two problems remains a problem in itself.

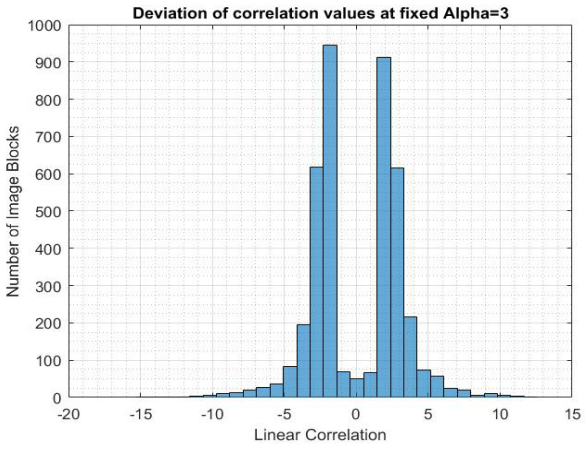

Fig. 3 Correlation values for α=3

V. Proposed Method

We first derive the constant correlation equations and then present it in the form of an algorithm used to evaluate the method for DICOM image samples.

From (2), both $\mathbf{C_{mn}}$ and $\mathbf{W_{mn}}$ are constant matrices within an image sub-block. Hence, only $\boldsymbol{\alpha}$ and $\mathbf{Y_{ij}}$ could vary.

Now coming to (4), if $\boldsymbol{p}$ is kept constant from one sub-block to another and W_{mn} is already a constant per sub-block, then only Y could vary to keep $\boldsymbol{p}$ constant as C_{mn} varies (from sub-block to sub-block). Hence, within a sub-block, only α in (2) could be varied in order to scale Y_{ij} into a value that would help it keep $\boldsymbol{p}$ constant in (4). Bearing this in mind, we derive equations to dynamically determine $\boldsymbol{\alpha}$ for each sub-block in order to keep $\boldsymbol{p}$ constant across all sub-blocks of the medical image.

A. Derivation of α to Maintain Constant p

From (2) a 0 or 1 is embedded as:

$$Y_{ij} = C_{ij} \pm \alpha W_{ij} \tag{6}$$

Substituting (6) for **Y** into (4):

$$p = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(C_{i,j} \pm \alpha W_{i,j})W_{i,j}$$

This implies that:

$$pmn = \sum_{i=1}^{m}\sum_{j=1}^{n}(C_{i,j}W_{i,j}) \pm \alpha \sum_{i=1}^{m}\sum_{j=1}^{n} W_{i,j} * W_{i,j}$$

By making **α** subject of the formula and adding the required subscripts:

$$\alpha_{0,1} = \frac{pmn \mp \sum_{i=1}^{m}\sum_{j=1}^{n}(C_{i,j}W_{i,j})}{\sum_{i=1}^{m}\sum_{j=1}^{n} W_{i,j}^2} \tag{7}$$

Depending on the message bit to be embedded, (7) is used to determine embedding strength, α.

B. Watermark and Tamper Detection

Detection of watermark follows from (4). A linear correlation is performed between **Y** and **W**. We expect to get a correlation of $\boldsymbol{p}$ for extracting a 0 or $\boldsymbol{-p}$ for extracting a 1. A deviation from these values suggest tampering in the particular sub-block or it is a non-watermarked sub-block. In a case where all sub-blocks have been watermarked, then there is definitely intentional or unintentional tampering in the sub-block. Equation (8) will be used for both watermark and image tamper detection.

$$S'^{(a)} = \begin{cases} 0, Corr(Y,W) = p \pm \mathcal{E} \\ 1, Corr(Y,W) = -p \pm \mathcal{E} \end{cases} \tag{8}$$

The value of Ɛ could be determined experimentally. However, it should typically start from 0.5. This follows from the theories of *Continuity Correction* and *Central Limit Theorem* [11] in Statistics for approximating discrete variable histogram by Normal distribution. Secondly, pixel values could be rounded up or down by the addition or removal of a maximum of 0.5 from the actual computed value. This value of **Ɛ** will also cater for unintentional attacks and simple image processing performed on the ROI if necessary.

C. Evaluation Parameters

The following parameters were used to evaluate the correctness and efficiency of the proposed method.

i. ***Peak Signal to Noise Ratio (PSNR)*** – the ratio of the original cover over the noise (standard error) introduced by watermarking.

$$PNSR = 10 * \log_{10}\frac{B}{\sqrt{MSE}} \tag{9}$$

B is the largest value of signal or the dynamic range for the pixel values (2^n, where n is pixel depth) and ***MSE*** is the Mean Square Error per pixel. PSNR is a statistical degradation measure.

ii. ***Structural Similarity Index Measure (SSIM)*** – The author in [12] made it clear that PNSR is not a good measure of a subjective, and thus, visual quality of an image. For this work, we have assumed that SSIM is a better measure of perceptual fidelity between two images, as proven in [12]-[14].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{10}$$

where $\boldsymbol{\mu_x, \mu_y}$ and $\boldsymbol{\sigma_x^2, \sigma_y^2}$ are the corresponding mean and variance of the images **x** and **y,** respectively. The parameter σ_{xy} is covariance of x and y.

iii. ***False Negatives (FN)*** - Number of actually watermarked blocks but had no watermark bit detected.

iv. ***Bit Error Rate (BER)***

$$\text{BER} = (\text{FN} + \text{Flipped bits})/\text{Total bits} \tag{11}$$

BER is the percentage of bits retrieved in error. Flipped bits are 0s retrieved as 1s, and vice versa.

VI. Experimental Set Up

135 samples of DICOM MRI images of size 256x256 and 512x512 (MxN) and pixel depth of 16 bits were used in this experiment. Twenty-one of them were 256x256, while 114 were 512x512 DICOM images. Some of these images are shown in Fig. 4. Each of the images were divided into either 1024 (for 256x256) or 4096 (for 512x512) sub-blocks of 8x8 (mxn) pixel size giving us a total of 21x1024 + 114x4096 = 488,448 image sub-block samples. Each sub-block is a sample and was embedded at the rate of 1 bit per sample each having a chip rate of 64.

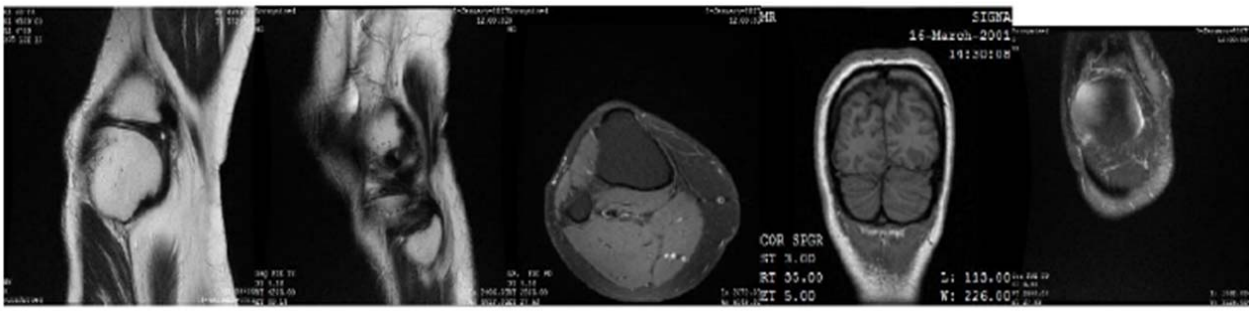

Fig. 4 Sample DICOM images

The spreading code, W_{mn}, is a gold code generated from x^6+x^5+1 and $x^6+x^5+x^4+x+1$ preferred pairs.

To run the experiments, 1024 or 4096 random bits were generated in MATLAB 2015 using the function:

Message = round (rand (M/8, N/8));

This generates random 0s and 1s to be used as watermark bits to be embedded into each sub-block. The algorithmic procedures employed in this research are as follows:

Step 1: Load the sample images.
Step 2: For each sample image divide it into **m x n** (m=n= 8 in our experiment) sub-blocks.
Step 3: Generate gold code, **W** and choose constant correlation value, p (= 1.2) between 0.5 and 8.0**.**
Step 4: Generate message bits to embed.
Step 5: For each sub-block and corresponding message bit compute the required embedding strength, α, using (7) and embed using (2).
Step 6: Compute SSIM and PSNR per sub-block.
Step 7: Use (4) to detect watermark and (8) to extract and/or detect tampered blocks.
Step 8: Compute False Negative (FN) and Bit Error Rate (BER), for the extracted bits per image sample.
Step 9: Repeat Steps 2-8 for each sample image.
Step 10: Plot the required graphs as presented in the results section.

The code for this algorithm is located at: https://github.com/KingPeter2014/MediHide/blob/master/ConstantCorrelationWatermarking.m.

Results are presented in the next section.

VII. Results

The results obtained from the above experiment are presented in plots mainly due to their large volume. The plots that follow will also allow one to observe trends and outcomes.

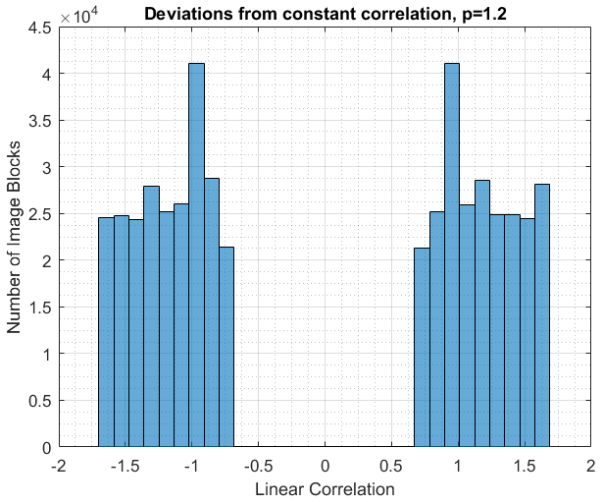

Fig. 5 Effectiveness of Constant Correlation Method

Fig. 5 shows that all correlations values centred on the chosen constant correlation value, p=1.2. Comparing Fig. 5 with Fig. 3 shows that constant correlation method gives less tolerance for variation in the extracted watermark value, yet it accurately detects the watermark barring quantization errors and tampering attacks.

In Fig. 6, all the images had zero BER. This means that all the embedded watermark bits were correctly extracted when there is no tampering.

Fig. 7 shows that negligible sub-blocks out of the 488,448 sub-image blocks had a PSNR value less than 50dB irrespective of the large embedding strength computed for some image sub-blocks.

Average global PSNR for 135 images was 72.92 dB with a range of 63.56 to 91.80 dB.

SSIM has shown to be a better visual perceptibility measure than PSNR [13], [17]. Fig. 8 shows the local distribution of SSIM measures for the 488,448 sub-blocks derived from the

135 images.

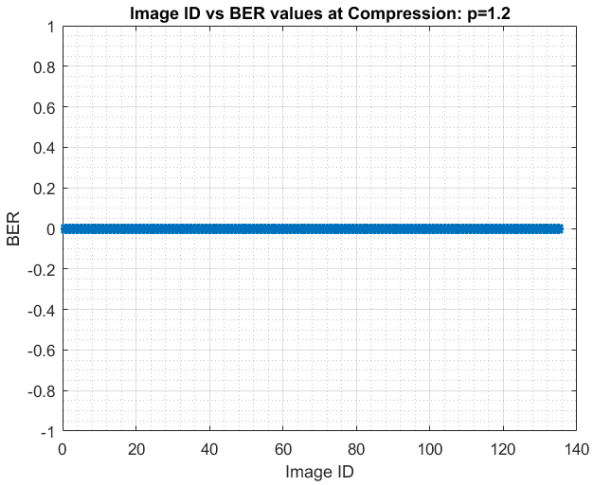

Fig. 6 Zero Bit Error Rate (BER)

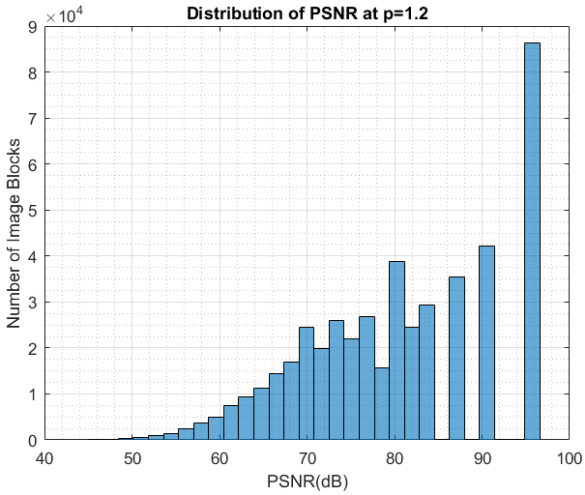

Fig. 7 Local PSNR Distribution

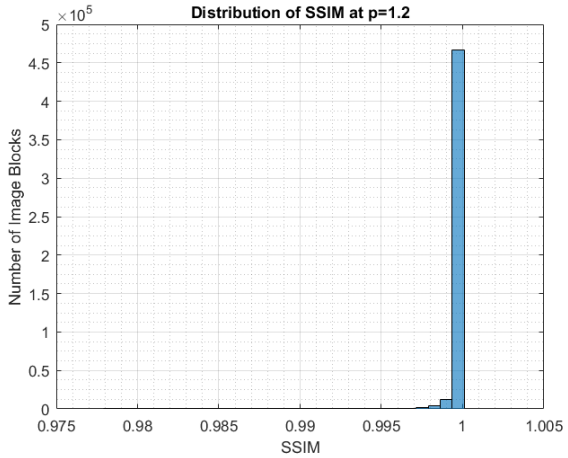

Fig. 8 Local SSIM Distribution

More than 460,000 out of 488,448 (94.18%) has SSIM of approximately 1.0, which is the maximum value.

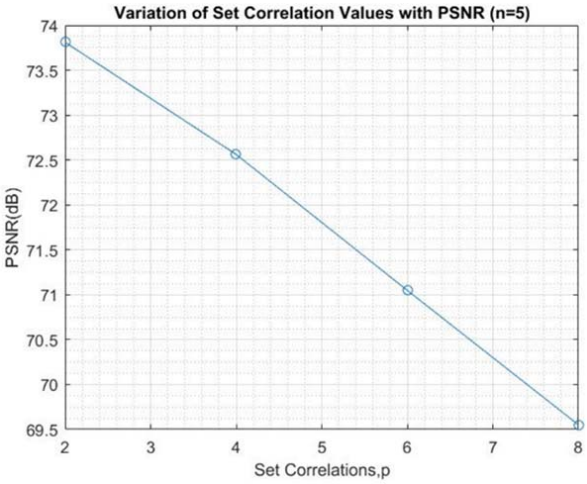

Fig. 9 Effect of value of p

Fig. 9 shows how the value of chosen constant correlation value, ***p***, affects global image quality.

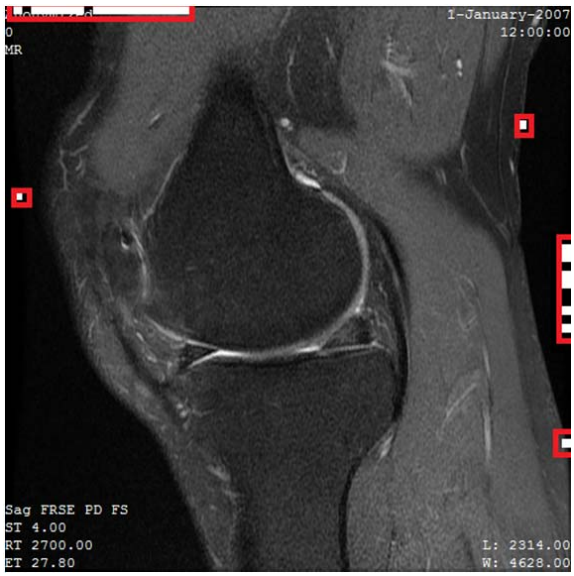

Fig. 10 Tamper Detection Example

Fig. 10 shows the flagged potentially tampered regions based on their undue deviation from the set constant correlation by the sender and receiver. The tampered regions are originally indicated in white by the algorithm. We only added the red marks using Paint in order to make it very conspicuous for readers.

VIII. Discussions

Our discussion will be focused on watermark detection/decoding accuracy, tamper detection and diagnostic quality preservation.

A. Watermark Detection Accuracy

The accuracy of watermark detection is measured by BER. Fig. 5 shows that all the extracted correlation values correspond to the set values of p = ±1.2. Fig. 6 also shows that all bits were correctly extracted. The detection accuracy of our algorithm is comparable and outperforms the results obtained by researchers in [15] using both traditional SS and Correlation-aware SS methods for DCT domain watermarking.

It should be noted that the value of ε affects the detection accuracy. It determines if the algorithm is to be used for fragile or robust watermarking. It should be noted that ε can take any value from $0 \leq \varepsilon < p$.

Hence, Constant Correlation method reduces host signal interference significantly and increases detection accuracy. The implication of this result is that barring quantisation errors (caused by rounding off to integer values in a pixel) and other malicious attacks, this method can be used to embed and retrieve text-based watermarks as opposed to image-based watermarks which has higher tolerance for bit errors. This is why it is being proposed for hiding Electronic Health Records (EMR) for use in Teleradiology applications. Histogram shifting in the RONI region was implemented in order to achieve the result.

Fig. 11 shows a typical medical image prone to underflow in the RONI of the medical image due to its saturated nature. Hence, the performance of this algorithm's detection accuracy by performing a histogram shift in the RONI before embedding in such images was desirable.

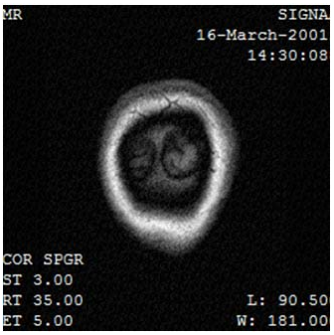

Fig. 11 Sample outlier DICOM image

The ROI of this image has good texture, and thus, the underflow problem would not affect it. This phenomenon is desirable for medical images. Pre-processing would not occur in the ROI used for medical diagnosis, while pre-processing can be applied in the RONI to enhance watermark detection. This pre-processing would not affect medical diagnosis as they would not contain medical information.

B. Possibility and Strategy for Tamper Detection

In Fig. 3, which is based on widely used SS methods, the attacker is given a wide range of opportunities to introduce malicious cover tamper data. This is because the correlation range for watermark retrieval is very wide compared to Fig. 5. Using (5) and recommendations from [6], all correlation values with absolute values between T_h and ∞ are actually valid. Hence, combining message and image tamper detection is nearly impossible using existing methods. Separate and/or non-blind algorithms as in [5] and [7] will be necessary for each function. However, by using the constant correlation method (the proposed method), it is evident in Fig. 5 that the correlation values strongly followed (8), which is more secure and cover tamper-sensitive. This is true because apart from quantisation error and unintentional mild processing attacks, the correlation value for each sub-block would not deviate from p by ε (0.5 in our experiment). It should be noted that the value of p must not be integer. Hence, if p and block size are made part of secret key (together with W), our proposed method is considerably secure and tamper-sensitive. Tamper sensitivity increases as the value of ε decreases and vice versa. By this algorithm, the SS watermarking method can easily be leveraged as both a fragile and robust watermarking algorithm by simply adjusting the value of ε.

Fig. 10 shows the areas marked by our algorithm as having been tampered with. The tampering determined here is in the class of unintentional processing. This is because higher quantisation errors were introduced in those areas. More strategic attacks and evaluation will be implemented in future works. Also, some correlation-invariant perturbations that may not be detected by this method would be studied as well.

C. Diagnostic Quality Preservation

Figs. 7-9 will help one to visualise the extent of preservation of diagnostic quality of the image at both the sub-block and global image levels. According to [16], a medical image watermarking algorithm is effective if its ***PSNR is greater than 40 dB***. Based on this and Fig. 7, the presence of the watermark would not significantly affect the original diagnostic information contained in the medical image. This is because no PSNR value was below 45 dB and only a few are below 50 dB. Fig. 8 also indicates that all sub-blocks maintained high visual and structural imperceptibility. This is because more than 460,000 out of 488,448 (94.18%) has SSIM of approximately 1.0 and none of the remaining 5.82% had SSIM below 0.98.

Fig. 9 shows what happens at the global image level as the value of p increases. As the value of p increases, PSNR value decreases and thus image quality decreases as well. However, at the high value of $p = 8$ used in this experiment, the PSNR value is still above 69.5 dB. This value is higher than the lower bound of 64 dB obtained by [17] in the ROI using Singular Value Decomposition and contourlet transform.

These results have made it become more pertinent that the recommendation in [3] should be given adequate consideration when designing watermarking algorithms for Medical systems. The degree of allowable degradation should be established, probably using expert opinion, machine learning classifiers, computer vision algorithms and from historical data. Is the recommendation by [16] still valid? In regard t the higher results obtained by our work and that of [17], would they make a difference for current resentment for use of watermarking in telemedicine? If these questions are

answered, the impact of this research would increase.

Table I compares the results of the proposed algorithm with other related research. The comparison is only for MRI-based samples used by the researchers as only MRI samples was used in this research as well. This research used larger sample data and obtained higher metrics for the same image modality. Though [17] divided image into ROI and RONI, their maximum PSNR value in the ROI is 67.27 dB, which is lower than our average of 72.92 dB.

TABLE I
COMPARISON OF SOME MEDICAL IMAGE WATERMARKING METHODS

Authors	Zero BER?	Average SSIM	Average Image PSNR (dB)	Tamper Detection?	DICOM-based?	SS-based?
Eswaraiah et al. [16]	-	0.9776	49.41	Yes	Yes	No
Rahimi et al. [17]	Yes	0.9406	46.22	Yes	Yes	No
Proposed Method	Yes	0.9999	72.92	Yes	Yes	Yes
Maity & Maity [18]	-	0.9750	44.85	No	No	Yes
Kumar et al. [19]	No	-	37.52	No	No	Yes
Proposed Method	Yes	0.9999	72.92	Yes	Yes	Yes

IX. CONCLUSION AND FUTURE WORK

A constant correlation method is preferable when the features of accurate watermark detection and tamper detection need to be achieved in a blind spread spectrum watermarking system. It does not only reduce the internal interference inherent in most images, but also ensures tampering in local regions are detected. Though it may introduce more degradation to the image (due to large value of α in some local blocks), it also has high global watermark qualities for high-pixel DICOM images according to our experiments and also in [17]. Furthermore, it is recommended that medical images that require watermarking should be created at higher pixel depths greater than eight. This ensures better watermarking qualities in terms of capacity, flexibility between robustness and fragility, and imperceptibility.

In future work, different tampering strategies such as cropping, copy-and-replace and rotation will be tested. The reversibility performance for heavily attacked ROI of medical images using this method will be investigated as well. Future research will also include transform domain of embedding. Finally, we shall fully describe the ***C₄S*** method of improving Steganographic capacity of SS watermarking methods in future work.

REFERENCES

[1] J. H. K Wu et al. "Tamper Detection and Recovery for Medical Images Using Near-lossless Information Hiding Technique" *Journal of Digital Imaging*, vol. 21, No. 1, March, 2008: pp 59-76.

[2] G. Ulutas et al. "Medical Image Tamper Detection Based on Passive Image Authentication" *Journal of Digital Imaging*, Springer, DOI: 10.1007/s10278-017-9961-x, May 08, 2017.

[3] Guo and T.G Zhuang. "A lossless watermarking scheme for enhancing security of Medical data in PACS" In *Proceedings of SPIE Medical Imaging*. SPIE 2003. Pp 350 – 359

[4] V. Dhore and P. M Arfat. "Secure Spread Spectrum Data Embedding and Extraction" *International Journal of Science and Research*, ISSN:2319-7064. vol 4, no.1, pp 743-747, 2015.

[5] C. Saini et al. "Digital Image Forgery Detection using Correlation Coefficients" *International Journal of Computer Applications* (0975-8887), vol.129, no. 14, pp 17-23, Nov, 2015.

[6] T. T Nguyen and H. D Tuan. "A Modified Spatial Spread Spectrum Method for Digital Image Watermarking" In *IEEE 2nd International Conference Communication and Electronics*, ICCE, Hoi an Vitenam, pp. 282-287, 4-6 June, 2008.

[7] P. Singh and S.S Goel. "Correlation-based Image Tampering Detection" In *International Journal of Computer Science and Information Technologies*, vol. 7, no. 2, pp 990-995, 2016.

[8] Y. Gan and J. Zhong. "Image copy-move Tamper blind detection algorithm based on integrated feature vectors" *Journal of Chemical and Pharmaceutical Research*, vol 6, no. 6, pp 1580-1589, 2014.

[9] A. Kashyap et al. "An Evaluation of Digital Image Forgery Detection Approaches" In Press: https://arxiv.org/abs/1703.09968, 30th March 2017.

[10] Wakatani, A., "Digital watermarking for ROI medical images by using compressed signature image" In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)* , pp. 2043–2048, 7-10 Jan.2002.

[11] R. V Hogg and A. T Craig. Introduction to Mathematical Statistics (4th ed.). Macmillian Publishing Company, Newyork, USA, 1978.

[12] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment" *Electronics letters,* vol. 44, no. 13, pp.800–801, 2008.

[13] Z. Wang, A.C. Bovik, H.R. Sheikh, and E. P. Simoncelli. **"**Image Quality Assessment: From Error Visibility to Structural Similarity**"** In *IEEE Transactions On Image Processing*, vol. 13, no. 4, pp 1-14, April, 2004.

[14] M. Fakhredanesh, R. Safabakhsh and M. Rahmati. "A Model-Based Image Steganography Method Using Watson's Visual Model*"* *ETRI Journal*, vol.36, no.3 pp. 479 – 489, June 2014.

[15] X. Zhang, Z.J Wang and X. Wang. "Correlation-and-bit-aware additive spread spectrum data hiding for Laplacian distributed host image signal*"* In *Signal Processing: Image Communication* vol. 29, pp. 1171 – 1180, 2014.

[16] R. Eswaraiah and E. S Reddy. "Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest" In *IET image Process*, vol. 9, no. 8, pp. 615 – 625, Doi:10.1049/iet-ipr.2014.0986, 2015.

[17] F. Rahimi and H. Rabbani. "A dual adaptive watermarking scheme in contourlet domain for DICOM images" In *Biomedical Engineering*, Doi: 10.1186/1475-925X-10-53, vol. 10, no.53, 2011.

[18] H. K Maity and S.P Maity. "Joint Robust and Reversible Watermarking for Medical Images" In 2nd *International Conference on Communication, Computing and Security, Procdia Technology* vol.6, pp 275 – 282, 2012.

[19] B. Kumar, H. V. Singh, S. P Singh and A. Mohan, "Secure Spread-Spectrum Watermarking for Telemedicine Applications" *Journal of Information Security* Vol 2, pp. 91-98, 2011.