Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 4, April 2019, pg.198 – 203

A Novel Digital Image Watermarking Scheme for Medical Image

MAIMAITIMING MAMUTI[1]; Dr. Serap KAZAN[2]

[1]Computer Engineering, Sakarya University, Turkey

[2]Computer Engineering, Sakarya University, Turkey

[1] maimatiming.mamuti@ogr.sakarya.edu.tr

Abstract— Different types of image watermarking schemes have been proposed over the years to come up with a more robust image watermarking algorithm. This paper presents a novel digital image watermarking scheme for medical image. The proposed improved watermarking scheme for medical image utilizes R, G, and B color channels of the color image. RGB cover image is fist decomposed into R, G, B channels, then Discrete Wavelet Transform* (DCT) *is applied on R channel, Discrete Cosine Transform* (DCT) *on G channel and List Significant Bit* (LSB) *on B channel, Medical image is processed with Arnold Scrambling before being embedded. With combination of conventional and widely used watermarking algorithms such as LSB, DWT and DCT and application of Arnold scrambling technique the new watermarking scheme proves to be more robust as it is evident from the experimental result. In order to measure performance of the proposed scheme Normalized Correlation and Peak Signal to Noise Ratio are chosen.

Keywords— LSB, DCT, DWT, Arnold, Watermarking, Medical Image

I. INTRODUCTION

As the world is becoming increasingly digitized, security and integrity of digital data have become the centre of attention. Digital image watermarking is a process of hiding valuable digital data of any kind so that it can be kept intact. Watermarking has been seen as promising to keep integrity of medical images. Digital image watermarking has two main domains: Spatial domain and Frequency domain. LSB is a widely used spatial domain method, as the name suggests, is chiefly used to hide watermark image in the least significant bit of the host image. The method is easy to understand and implement. However, lower complexity comes with a disadvantage, which is being less resistant to attacks.

Most known watermarking methods in frequency domain are DCT and DWT. In frequency based methods, pixel values of watermark image are transformed and the image is inserted in to change coefficients of host image. Despite being more complex, the methods are studied more than often due to robustness.

LSB, proposed by Deshpande Neeta, et al., is used to hide data using the least significant bits of the host image, which is unable to notice by the naked human eye [1]. The technique as the name suggests is used to hide intended information in a cover image, pixels of which are altered by bits of the message-to-be-hidden. Changing the last significant bit of a pixel yields slight change in colour intensity, making it hardly perceivable by naked eye. Having said that, simplicity comes with a price. There is a strong possibility that any attacker can easily extract hidden information.

DCT is a frequency domain watermarking that splits cover image into low, middle and high frequency bands, of which one is chosen to hide watermark image, pixels of cover image would stay unaltered. The DCT technique is more attack-resistant compared to spatial domain watermarking technique such as LSB. However, the technique is relatively complex and hard to implement. And DCT can be divided into Global DCT and Block based DCT [2], the latter is chosen for this study.

DWT is a wavelet transform for the wavelets are discretely sampled [3]. 2 dimensional DWT is considered for the study and it includes two operations: horizontal operation and vertical operation. In 2D-DWT, pixels are first scanned from left to right in horizontal direction. Addition and subtraction operations will be performed on neighbouring pixels. Then, the sum is stored on the left, the difference on the right. The whole process is finished when same operation is applied on all rows. Low frequency part is represented by L while the differences are represent by H as high frequency.

Pixels are scanned from top to bottom in vertical direction. Addition and subtraction operations are performed on neighbouring pixels. The sum is kept on the top and the difference on the bottom. Until all columns are finished the whole operation will be repeated. 4 sub-bands as LL, HL, LH, and HH will be acquired, where LL is low frequency.

Scrambling the information before the concealment makes the data disordered and unsystematic and hence the transmission will be more secure [4]. In order to provide extra security to the watermark, Arnold is used in pre-processing. Arnold, also known as Cat map, is a periodic process. And by changing pixel positions of image it acts as an encryption technique. More importantly, attacker cannot extract the watermark without having proper information about scrambling algorithm. So Arnold does improve security of the watermark and increase the robustness of the proposed scheme. Two-dimensional scrambling can be defined follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad \ldots 1$$

(x, y) is the pixel coordinates of the original image; (x', y') is the pixel coordinates after iterative computation scrambling and N is the watermark size.

II. PROPOSED WATERMARKING SCHEME

Watermarking scheme involves following steps: Embedding and Extracting

Embedding algorithm:

Two images are required, one is cover image and another one is medical image as a watermark to be hided.

Step1: Read two input images, one is RGB image as cover image and one medical image as watermark.
If medical is not in grayscale, then image is converted to grayscale image.
Step2: Decompose RGB image and Assign R, G, and B three matrices for each component of RGB image
Step3: Scramble watermark image using Arnold scrambling
Step4: Convert each pixel of cover image to an 8-bit binary
Step5: Generate three two-dimensional matrices to store the converted binary strings
Step6: Store the scrambled watermark image in three 64rows*64cols matrices
Step7: Apply DWT algorithm on R Matrix, DCT on G Matrix and LSB on B Matrix
Step8: Combine and rewrite three matrices in one Matrix
Step9: Save watermarked image
Embedding process is illustrated in Figure 1.

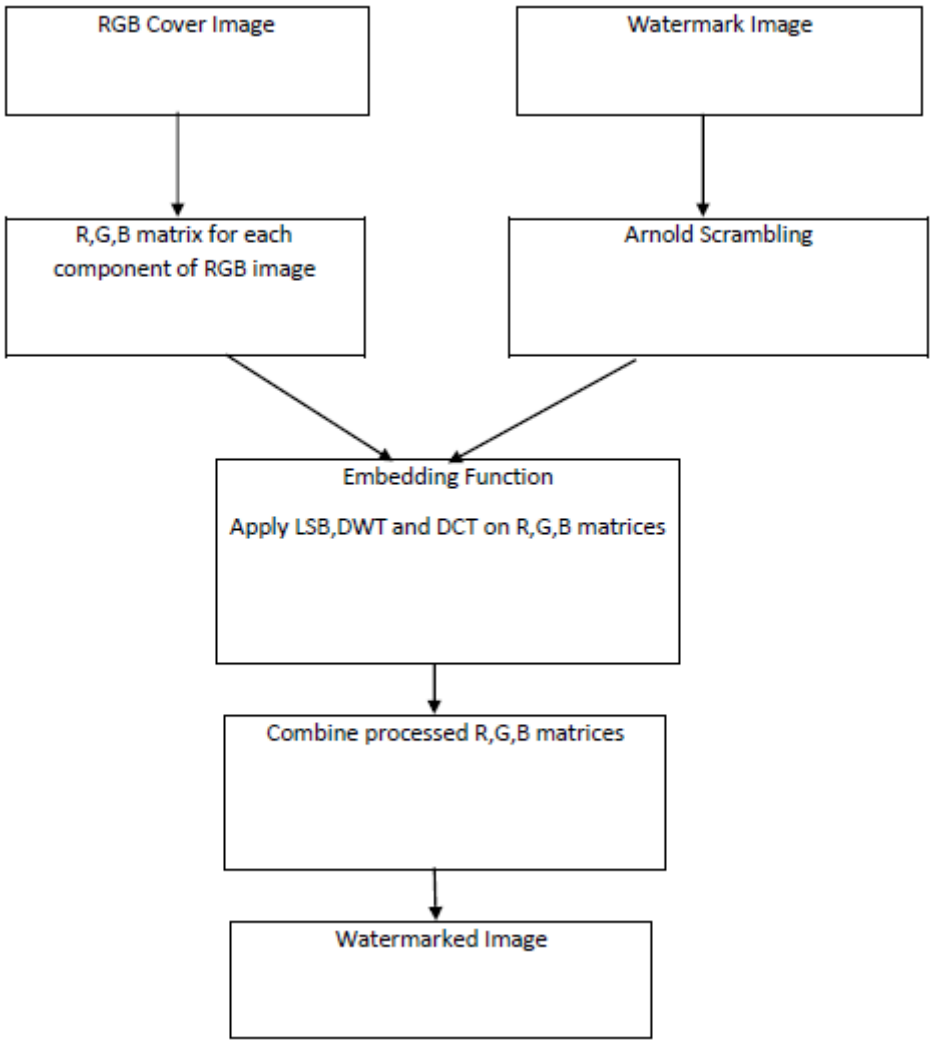

Fig. 1 Embedding Algorithm

Extraction algorithm:

Step1: Read watermarked image
Step2: Get the R, G, B matrix of Watermarked Image
Step3: Call one dimensional matrix storing R, G, B matrix for later recovery
Step4: Perform recovery function, apply extraction method on each matrix
Step5: Convert the obtained 8-bit binary string to decimal and store in recovery matrix
Step6: De-Arnold
Step7: Extracted watermark image
Watermark extraction can be described as in the figure below:

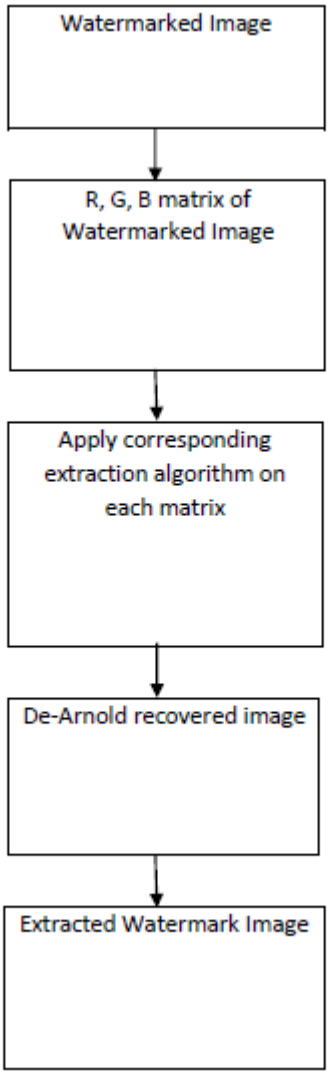

Fig. 2 Extraction Algorithm

III. EXPERIMENT AND ANALYTICAL RESULTS

Matlab is used for visualization of experimental data. RGB image is selected as cover image and a medical image as secret information to be hidden. As shown in Figure3 and 4.

Fig. 3 Cover Image

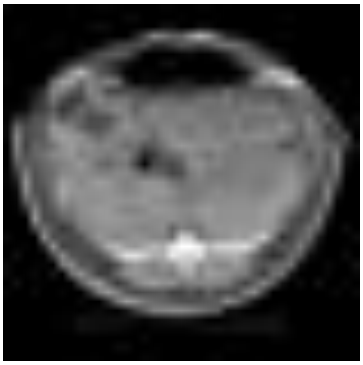

Fig. 4 Watermark Image

Arnold scrambling is applied before watermarking begin and the scrambled image as shown in Figure5.

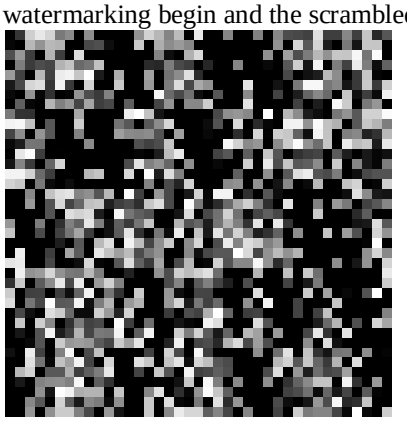

Fig. 5 Scrambled Image

The image after extraction process is as shown in Figure 6.

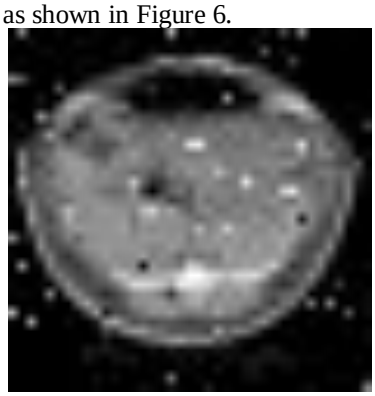

Fig. 6 Extracted Watermark Image

The following two metrics are used in the performance analysis.

A. Normalized Correlation

The Normalized Cross-Correlation (*NC*) is defined as

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j)\cdot W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W'(i,j)]^2}} \quad \ldots 2$$

The value of Normalized Cross-Correlation (*NC*) varies between o and 1. It is calculated using the following equation. If *NC* = 1 then the embedded watermark and the extracted watermark are same. Generally the value of *NC*>0.7500 is accepted as reasonable watermark extraction. Where *W* is Original Watermark and *W′* is detected watermark.

B. Peak Signal to Noise Ratio

Peak Signal-to-Noise Ratio (*PSNR*), applied to images as a quality metric by scaling the MSE according to the image range, the following equation is used to calculate PSNR [5].

$$PSNR = 10 \log_{10} \frac{256^2}{MSE} \quad \ldots 3$$

PSNR is measured in decibels (*dB*). PSNR is a good measure for comparing restoration results for the same image. The bigger the PSNR value is better the watermark conceals [6].

When PSNR is higher than 35 *dB* watermarked image has a very good quality and the eye could hardly tell the difference between the original and the watermarked image. While when *NC* is higher than 0.7500 the extracted watermark is considered as valid one.

Obtained results are as follows for the proposed study: *dNC* is 0.9799 and PSNR (*dB*) is 55.9463118. It has been found proposed scheme is more robust and relatively secure. Watermark image and extracted image are visually identical.

IV. CONCLUSIONS

A novel watermarking scheme for medical image is proposed in the paper, which hide important medical image in a RGB cover image. The scheme is developed to keep the integrity of medical image to the highest degree possible. As its nature demands preserving the visual fidelity of medical should not be compromised. Arnold scrambling is used to add extra level of security to medical image. The study combines all three major algorithms as base to generate a scheme to embed medical image in cover image to make it more secure. Implementation results show that the imperceptibility of the watermarked image is reasonably acceptable.

REFERENCES

[1] Frank Y.Shih, "Digital Watermarking and Steganography- Fundamentals and Techniques", CRC Press 2008.

[2] Y. Qianli, C. Yanhong, "A Digital picture watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform2012, pp. 1102-1105.

[3] W. Hong and M. Hang, "Robust Digital Watermarking Scheme for Copy Right Protection," IEEE Trans. Signal Process, 2006.

[4] Razieh Keshavarziana; Ali Aghagolzadehb "ROI based robust and secure image watermarking using DWT and Arnold map" published in Int. J. Electron. Commun. (AEÜ) 70 (2016) 278–288.

[5] F. A. P. Peticolas, et al., "Information hiding–a survey," Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.

[6] Chandra Mohan B., Veera Swamy K. and Srinivas Kumar S., (2011) "A Comparative performance evaluation of SVD and Schur Decompositions for Image Watermarking ", IJCA Proceedings on International Conference on VLSI, Communications and Instrumentation (ICVCI) (14), pp 25–29.

