Original Identifier Code for Patient Information Security

Ahmed Nagm[1†] and Mohammed Safy[2††],

[1†]Electrical Engineering, Modern Academyy, Cairo, Egypt

2††Electrical Engineering, Egyptian Academy for Engineering & Advanced Technology, Cairo, Egypt

Summary
During the medical data transmissions, the protection of the patient information is vital. Hence this work proposes a spatial domain watermarking algorithm that enhances the data payload (capacity) while maintaining the authentication and data hiding. The code is distributed at every pixel of the digital image and not only in the regions of non-interest pixels. But the image details are still preserved. The performance of the proposed algorithm is evaluated using several performance measures such as the mean square error (MSE), the mean absolute error (MAE), and the peak signal to noise Ratio (PSNR), the universal image quality index (UIQI) and the structural similarity index (SSIM).

Keywords:
Patient information; data payload; spatial domain; Medical image watermarking; Data Integrity Protection.

1. Introduction

The presence of electronic data of patients within the current worldwide health care information systems has important benefits for patients and care practitioners, including greater patient discretion and improved clinical management. The flow of knowledge between hospitals, doctors and others has increased by 40% between 2008 and 2009.

A study published in late July 2009 e-Health Initiative [1] shows that many of them are using these systems to save costs.

The patient information security and patient's medical data privacy are of high importance nowadays. Medical information plays a significant role in the health system and its modification might result in misdiagnosis. Rarely a day passes by where we don't see a featured article or publication about some aspects of medical privacy, or a report about a breach of security.

Medical patient information could be distorted by mistake, such as during conversation, or intentionally. In the latter case, pictures can be intentionally tampered with results being added or deleted.

Some image processing could also result in unintentional changes. For example, the loss in the patient's information while using the compression technique. This loss is occurs in telemedicine applications to minimize the amount of information to be transmitted. Thus this process can induce inacceptable loss of knowledge depending on its degree which may result in a misdiagnosis.

Security requirements differ from application to application, and the protected aspects that they underline. It will guarantee three characteristics: confidentiality, honesty and availability [2]. The meanings of these terms are outlined in [3][4][5]. A spatial domain watermarking technique is proposed to improve the data payload and at the same times both authentication and data hiding are included.

2. Literature review

Different types of information security technique are available like cryptography (Schneier, 2007), steganography (Amirtharajan and Rayappan, 2012a, b, c, d, Amirtharajan et al., 2012; Padmaa et al., 2011; Rajagopalan et al., 2012; Thenmozhi et al., 2012; Janakiraman et al., 2012a, b) and Watermarking. To protect medical images during transmission, the watermarking is used. It is a process of embedding significant information over a patient's medical image to provide authentication, information hiding, tamper proof data, etc., (Coatrieux et al., 2009). Confidentiality, authenticity and reliability are considered as main factor for watermarking process. The process of watermarking is classified into invisible and visible watermarking. For watermarking attacks (Priya et al., 2012), the invisible watermarking is a robust technique.

The first usage of the digital watermarking was to protect the copyright of digital multimedia on the Internet. In [6], the quality requirements for patients' pathology medical data are extremely strict, and no changes are allowed. The research in the field of medical image digital watermarking [7] is essential because any change in the transmitted patient information is forbidden and will affect the doctor's decision.

Digital image watermarking can be mainly done in both transform and spatial domains. In spatial domain, the watermark is inserted within the original medical image (Wang, 2009). Many techniques are used to insert a watermark such as LSB (Least Significant Bit) substitution technique, Pixel alteration and bit shifting, etc. The

Manuscript received July 5, 2023
Manuscript revised July 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.7.16

technique of the spatial domain watermarking is very easy and simple with less complexity. The technique of the spatial domain watermarking makes use of human visual system, but sensitive to image scale so that same information must be embedded again and again in different locations of the host image.

Embedding watermarks into the spatial domain components of the cover images is a straightforward method. It is one of the fundamental schemes used since the digital watermarking began in 1993 [8]. Usually the spatial-based watermarking schemes select a number of pixels from the cover image, and modify the luminance values of these pixels selected according to the watermark bits to be embedded [8] [9] [10]. The image containing these modified pixels therefore now carries the information of the watermark. To extract (or detect) the watermark embedded, usually the same pixels used in the embedding procedure should be selected from the watermarked image firstly. Then, according to the strategy used, the bit carried within each pixel can be determined (or detected). By collecting all the bits extracted (or all the results detected), the hidden watermark (or whether the image contains the considered watermark) can be obtained. A well-known classic spatial-based watermarking method is the last-significant-bits (LSB) modification scheme [9]. It selects a number of pixels from the cover image, and modifies their luminance to carry watermark bits. The simplicity of implementation and the low complexity are the advantages of spatial-based watermarking schemes. On the other hand they are not robust against common methods of attack [11], [12], [13]. To improve the spatial domain weakness, many methods are proposed. In [4], the performance of spatial-based watermarking schemes can be improved using the BCH (Bose-Chaudhuri-Hochquenghem) block codes. In [15], the authors presented a scheme having stronger robustness. Like the general scheme mentioned, their scheme also selects the considered number of pixels from the cover image firstly. Then, for each pixel selected, the mean value of its neighbor pixels is calculated. This mean value is referred to modify the pixel selected. The robustness of their scheme is better, which indicates this scheme is more suitable for practical use. Moreover, the scheme also provides a parameter to control the balance between imperceptibility and robustness. Users of this system therefore can decide to have better imperceptibility or better robustness.

The main categories of using the digital watermarking in the medical field are data hiding, authentication and the combination between the data hiding and the authentication [16], [17].

In [18], the content authentication of the patient's images (CT) is the main purpose. The image is separated into two regions one of them is the region of noninterest (RONI) and the other is the region of interest (ROI). The watermark is inserted in the RONI, so the quality of ROI is persevered. This code is very simple but it can be easily attacked.

In [19], the security of the ultrasound (US) images is increased based on the authentication and the integrity. First a rectangular shape is used to separate the RONI and the ROI. Then SHA256 hash function is used to calculate the hash value of the whole image. To make the code more secure, a secret key is used to create a hash value as well as a secret key for the inserted watermark. Finally the hash value is inserted into the LSBs of RONI.

In [20], the data hiding is the main purpose. The digital watermark is inserted on the boundary of the ROI region. The code can preserve the image quality but at the same time it is not efficient against the attacks.

In [21], watermarking and cryptography is used in a one system in a way that inserts an encrypted version of the patient's original information. After watermarking, the corrupted details of the medical information were recovered using a reversible property.

In [22], a robust watermark is proposed based on the combination of the identification code of the physician, patient's information and the LSBs of the ROI, which after encryption were embedded into the RONI of the patient's original image.

3. Proposed Methodology

In this method, an image is decomposed into three components using Color Filter array (CFA). One of these components is elected for further processing. This elected component is encrypted using a dynamic keys approach. These dynamic keys combine the patient ID, the name and the arrival date. After the encryption is carried out, the new component is called a modified comment. Next a substitution processing is performed in the frequency domain between one of the other CFA outputs and the modified component to get the final encrypted component. In the last stage, the demos icing algorithm is performed on the final encrypted component and the other two CFA outputs. This has been done in order to get an image that includes our proposed Originality Identifier Code (OIC).

For illustration, the whole structure of the proposed algorithm is shown in Figure 1.

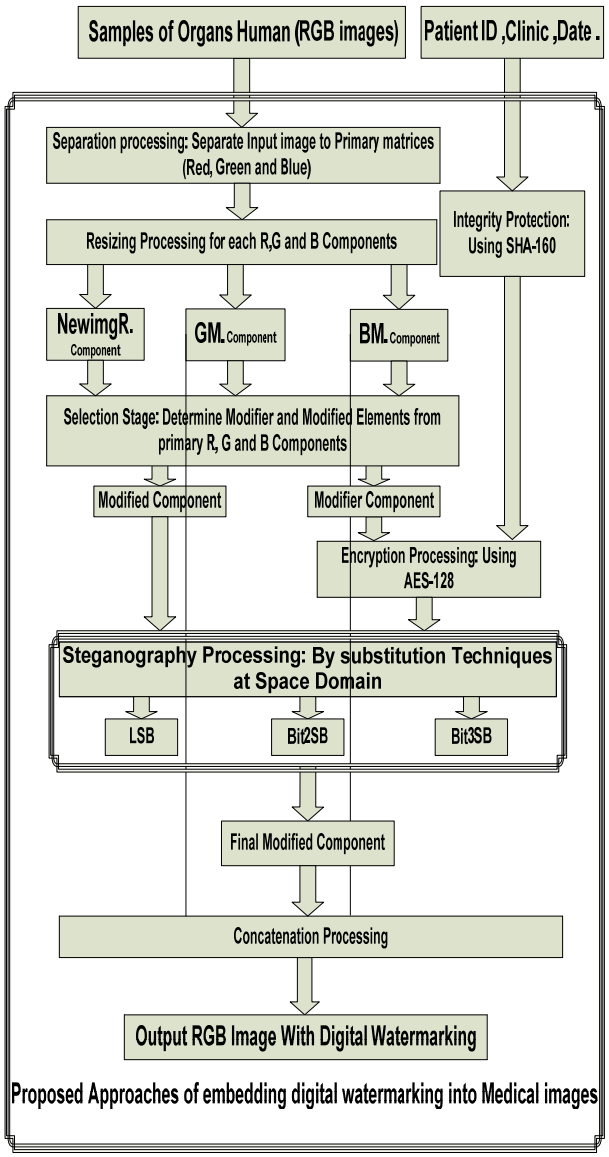


Fig. 1 Proposed Approach of embedding digital watermarking into Medical images

Starting with the input color image I has a $n * m$ dimension as a RGB image with JPEG format. Where, it represented as a:

$$I = (Irc) = \begin{bmatrix} I_{11} & \cdots & I_1 m \\ \vdots & \ddots & \vdots \\ In_1 & \cdots & Inm \end{bmatrix} \quad (1)$$

The represented matrix of input RGB image at equation 1 is composed from three matrixes have the same number of rows and columns of the input images. The first matrix is the Red component, the second matrix is the Green component and the third matrix is the Blue component as shown in equation 2.

$$G = (Grc) = \begin{bmatrix} G_{11} & \cdots & G_1 m \\ \vdots & \ddots & \vdots \\ Gn_1 & \cdots & Gnm \end{bmatrix}$$
$$R = (Rrc) = \begin{bmatrix} R_{11} & \cdots & R_1 m \\ \vdots & \ddots & \vdots \\ Rn_1 & \cdots & Rnm \end{bmatrix} \quad (2)$$
$$B = (Brc) = \begin{bmatrix} B_{11} & \cdots & B_1 m \\ \vdots & \ddots & \vdots \\ Bn_1 & \cdots & Bnm \end{bmatrix}$$

Then for every pixel, there is a three numeric values in terms of Red, Green and Blue component as shown in equation 3.

$$(Irc) = \{(Rrc), (Grc), (Brc)\} \quad (3)$$

Equation 4 shows the separation of the input image I to the three components.

$$R = I - (G + B) \quad (4)$$
$$G = I - (R + B)$$
$$B = I - (R + G)$$

Resize the separated Red, Green and Blue components to be suitable to the encryption algorithm.

$$RM(r) = R\left(r + \left(8 - (r \text{ MOD } 8)\right)\right) \quad (5)$$

if remender of numeric value for input rows $\neq 0$

else, $RM(r) = R(r)$

$$RM(c) = R\left(c + \left(8 - (c \text{ MOD } 8)\right)\right), \quad (6)$$

if remender of numeric value for input colum $\neq 0$

else, $RM(c) = R(c)$

The numerical intensity of the component depends on the used bits according to:

$$(Rrc) = 2^L - 1 \quad (7)$$

Where L: is the length of used bits, if L = 8 then the bits will be from 0 to 7. That mean the representation of pixels have intensities level from 0 (black) to 255 (white). And it is formatted as a depicted in equation (8).

$$(Rrc)_{10} = (Rrc)_2 = [b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0] \quad (8)$$

Where b: is the bit value (0 or 1).

The transformation function as a Discrete Cosine Transform is used, so equation (9) for each 8*8 block as following:

$$RM'(u,v) = \left(\frac{2}{m*n}\right) \sum_{r=0}^{m-1} \sum_{c=0}^{n-1} R(r,c) \left(\cos\left(\frac{(2r+1)\pi u}{2m}\right) * \cos\left(\frac{(2c+1)\pi v}{2n}\right)\right) \quad (9)$$

Where
u is raw number in the transformed data
v is column number in the transformed data
r is raw number in the original data
c is column number in the original data
m is number of rows in the original data
n is number of columns in the original data
RM^t is value of pixel in the transformed data
RM is value of pixel in the original data.

$$RM^t = (Ruv) = \begin{bmatrix} RM^{11} & \cdots & RM^1m \\ \vdots & \ddots & \vdots \\ RMn^1 & \cdots & RMnm \end{bmatrix} \quad (10)$$

To get the initial Key for the Symmetric Encryption Algorithm one of the crypto- graphic hash function on ID of capture device (Camera ID, as an example Serial number of capture device) as a SHA-1 is used to.

Performing the secure hash function on Capture ID by SHA-160, the output block size has 160 bit (Message Digest Length = 160). With initial input Key was "acef" and initial hash value were:

H [0] ='67452301',
H [1] ='EFCDAB89',
H [2] ='98BADCFE',
H [3] ='10325476',
H [4] ='C3D2E1F0',

Accordingly to equation (11), then the output will be:

$$K1 = SHA-1(\text{Camera ID}) = 86E152C142DB1256FC1EF004ADEB7B935741D94D \quad (11)$$

The first sixteen digits from the output is extracted to be the Initial key for encryption processing by AES-128 as shown in equation (12).

The Key K = '86E152C142DB1256' and CB are represent a ciphered blue component of original color image with forty four internal key and 80 round according to equation (12).

$$CBrc = AES-128([K],(BMrc)) = \begin{bmatrix} CB^{11} & \cdots & CB^1m \\ \vdots & \ddots & \vdots \\ CBn^1 & \cdots & CBnm \end{bmatrix} \quad (12)$$

The steganography processing is started to get final modified component NRM in equation (13).

$$NRM = (NRMrc \Leftarrow CBrc) = \begin{bmatrix} NRM_{11} & \cdots & NRM_1m \\ \vdots & \ddots & \vdots \\ NRMn_1 & \cdots & NRMnm \end{bmatrix} \Leftarrow \begin{bmatrix} CB_{11} & \cdots & CB_1m \\ \vdots & \ddots & \vdots \\ CBn_1 & \cdots & CBnm \end{bmatrix} \quad (13)$$

The Discrete Cosine Transform substitution processing is performed on frequency domain between the element matrix of the ciphered blue and the red component and then the inverse transformation method is used to get the final modified component in the space domain.

The element number (1, 1) at every 8*8 block from the transformed red component is replaced by the same element of transformed ciphered blue component to get the final modified component at frequency domain then perform the inverse transform to get it at space domain.

At the end the modified red component is appeared according to equation number (14).

$$NRM = (Ruv) = \begin{bmatrix} CB_{11} & \cdots & RM_{18} \\ \vdots & \ddots & \vdots \\ RM_{81} & \cdots & RM_{88} \end{bmatrix} \quad (14)$$

First AC coefficient, the element number (1, 2) at every 8*8 block from the transformed red component is replaced by the same element of transformed ciphered of the blue component to get the final modified component at frequency domain then perform the inverse transform to get it at the space domain, where the element $(1, 2)$ of CB^t and other 64 coefficients for RM^t.

Middle AC coefficient, the element number (3, 6) at every 8*8 block from the transformed red component is replaced by the same element of the transformed ciphered of the blue component to get the final modified component at frequency domain then perform the inverse transform to get it at the space domain, where the element $(3, 6)$ of CB^t and other 64 coefficients for RM^t.

Last AC coefficient, the element number (8, 8) at every 8*8 block from the transformed red component is replaced by the same element of the transformed ciphered of the blue component to get the final modified component at frequency domain then perform the inverse transform to get it at the space domain, where the element $(8, 8)$ of CB^t and other 64 coefficients for RM^t.

At the end the modified red component will be according to the equation number (15).

$$NRM = (RMuv) = \begin{bmatrix} RM_{11} & \cdots & RM_{18} \\ \vdots & \ddots & \vdots \\ RM_{81} & \cdots & CB_{88} \end{bmatrix} \quad (15)$$

The final modified component is concatenated with the two other original components "Modified Red, Green and Blue" accordingly to equation (16), where NI is protected originality image.

$$(\mathrm{NIrc}) = \{(\mathrm{NRMrc}), (\mathrm{GMrc}), (\mathrm{BMrc})\} \quad (16)$$

There are two main categories of attacks, the Conventional Attacks that include the Gaussian Noise Attacks, the JPEG Attacks and the Median Filter Attacks. The Geometrical Attacks that include the rotation, the scaling, the translation and the Cropping Attacks. The main target of the traditional algorithms is how to restore the original image. But the proposed algorithm checks whether the patient's information has been deliberately changed or not. Figure 2 demonstrates the proposed algorithm that detects the attacks:

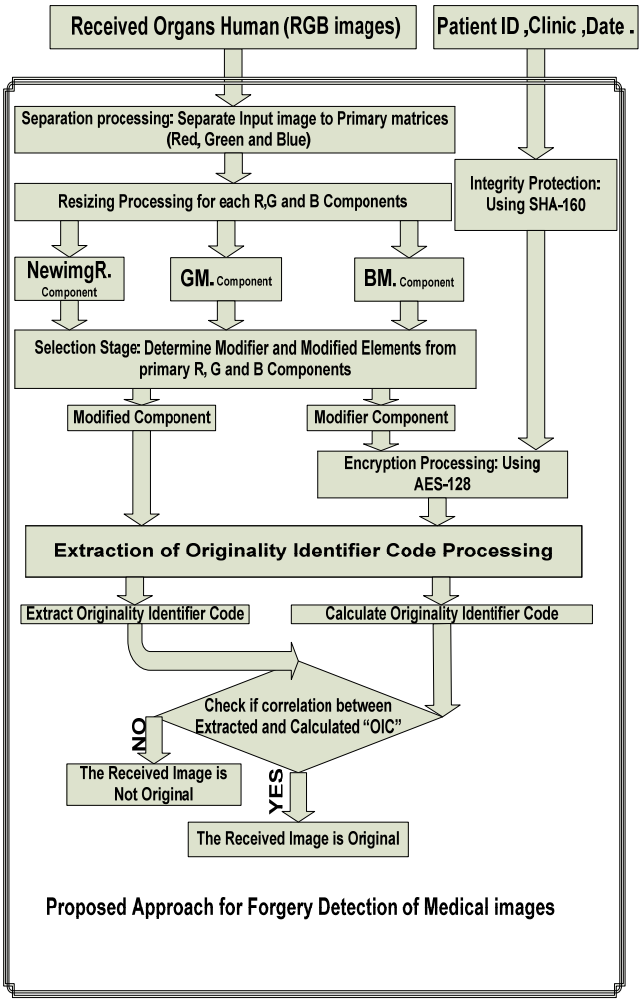


Fig. 2 Proposed Approach for Forgery Detection of medical images

4. Evaluation of the proposed algorithm

In the experiment, MATLAB 2015 Version 8.5.0.197613, core i3 processor 2.3 Ghz and 4GB RAM is used as the test platform. There are two main classes to assist the image distortion one of them the mathematically class which includes MSE. MAE and PSNR and the other class is the human visual system.

The Mean Absolute Error and the Mean Square Error (MSE) are used to calculate the difference between the original image and the sent one.

$$\mathrm{MSE} = \frac{1}{\mathrm{M*N}} * \sum_{j=1}^{n} [x(i,j) - v(i,j)]^2 \quad (17)$$

$$\mathrm{MAE} = \frac{1}{N}\sum_{i=1}^{N} |x_i - v_i| \quad (18)$$

The peak signal to noise ratio is used and it is used to measure the similarity between the input image and the image after watermarking.

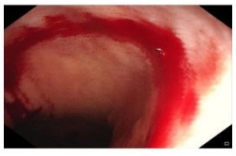
$$\mathrm{PSNR} = 10\log_{10}\left(\frac{S^2}{\mathrm{MSE}}\right) \quad (19)$$

Beside these metrics there are some important metrics like the Universal Image Quality Index (UIQI) which three factors loss of correlation, luminance distortion, and contrast distortion Also The most important metric is the Structural Similarity Index (SSIM) because it is not only measure the similarity between original image and the output image as a number but also it measures the similarity in the structure.

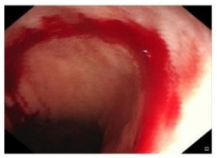
$$Q = \left(\frac{\sigma_{xv}}{\sigma_x \sigma_v}\right) * \left(\frac{2 * \bar{x} * \bar{v}}{\bar{x}^2 + \bar{v}^2}\right) * \left(\frac{2 * \sigma_x * \sigma_v}{\sigma_x^2 + \sigma_v^2}\right) \quad (20)$$

$$\mathrm{SSIM}(X,V) = (2 * \bar{x} * \bar{v} + c1) * \frac{(2 * \sigma_{xv} + c2)}{(\bar{x}^2 + \bar{v}^2 + c1) * (\sigma_x^2 + \sigma_v^2 + c2)} \quad (21)$$

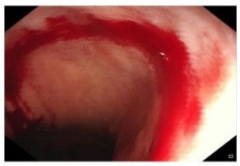
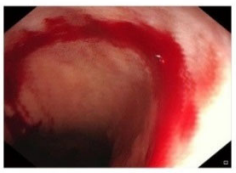
In figure [3, 4, and 5] randomly selected medical images are used as an original images



AB image without digital watermarks



AB digital watermarked by LSB

AB digital watermarked by Bit2SB AB digital watermarked by Bit3SB

Fig. 3 Digital watermarking using different strategy for the AB image


AC image without digital watermarks AC digital watermarked by LSB


AC digital watermarked by Bit2SB AC digital watermarked by Bit3SB

Fig. 4 Digital watermarking using different strategy for the AC image


FLU image without digital watermarks FLU digital watermarked by LSB


FLU digital watermarked by Bit2SB FLU digital watermarked by Bit3SB

Fig. 5 Digital watermarking using different strategy for the Flu image

PSNR, MAE, MSE, SSIM and UIQI are used to measure the performance of the proposed algorithm.

Table 1and 2 shows that the mean absolute error and mean square error of the single LSB has the lowest value compared with the other elements. Table 3 and 4 shows that the peak signal to noise ratio and the Structural Similarity Index of the single LSB and single-Bit2SB have the highest value compared with the single-Bit3SB. Table 5 shows that the Entropy of the all elements are high.

From analyzing these results it is clear that the choosing of the single LSB gave the best performance over the rest of elements.

Table 1: Mean Absolute Error of the Proposed Approach

Images/Size/ JPEG	***Mean Absolute Error of the Proposed Approach***		
	Single-LSB	***Single-Bit2SB***	***Single-Bit3SB***
AB/512*512, 22KB	0.0824	0.1611	0.3342
AC/512*512, 340KB	0.0832	0.1643	0.3369
Flu/348*288, 26KB	0.0827	0.1608	0.3205

Table 2: Mean Square Error of the Proposed Approach

Images/Size/ JPEG	***Mean Square Error of the Proposed Approach***		
	Single-LSB	***Single-Bit2SB***	***Single-Bit3SB***
AB/512*512, 22KB	0.167069753	0.664449056	2.700602214
AC/512*512, 340KB	0.166893005	0.663869222	2.703511556
Flu/348*288, 26KB	0.167730638	0.665400752	2.672935957

Table 3: The Peak signal to noise ratio of the Proposed Approach

Images/Size/ JPEG	***Peak signal to noise ratio of the Proposed Approach***		
	Single-LSB	***Single-Bit2SB***	***Single-Bit3SB***
AB/512*512, 22KB	55.9018253	49.90618672	43.81619742
AC/512*512, 340KB	55.90642225	49.90997826	43.81152131
Flu/348*288, 26KB	55.88467963	49.89997073	43.86091808

Table 4: SSIM for the Proposed Approach

Images/Size/ JPEG	***SSIM of the Proposed Approach***		
	Single-LSB	***Single-Bit2SB***	***Single-Bit3SB***
AB/512*512, 22KB	0.999295797	0.997930044	0.987737559
AC/512*512, 340KB	0.999673577	0.999171438	0.993768634
Flu/348*288, 26KB	0.999867319	0.999476348	0.997853068

Table 5: UIQI for the Proposed Approach

Images/Size/ JPEG	***UIQI of the Proposed Approach***		
	Single-LSB	***Single-Bit2SB***	***Single-Bit3SB***
AB/512*512, 22KB	0.999952895	0.999812608	0.999240437
AC/512*512, 340KB	0.999891903	0.99956814	0.998248895
Flu/348*288, 26KB	0.999951511	0.999807683	0.999228211

The vulnerability assessment approach is based on assuming an attack on one of the quadrants zones. In this approach, the technique should show full immunity against space attacks, whereas the image could be changed in any of the areas explained. Moreover, the assessment technique shall include as well the color component changes since the algorithm is based on manipulation based on color components. In this approach, and as explained in figure 6, the attack takes place either using a single color basic component (Red, Green or Blue) or a natural color change (i.e. a mix of basic color components). Figures [7,8 and 9] demonstrate a different attack regions and all of them are detected the proposed algorithm.

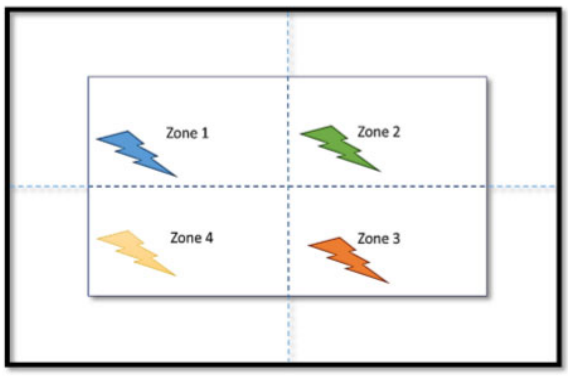


Fig. 6 Infected component and locations of active attack for received RGB images.

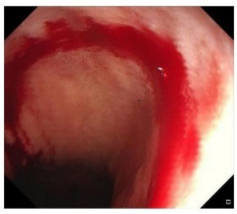


Fig. 7(a) AB modified at red the by same blue component from raw 238 - 241 and column 300 - 303 (2)

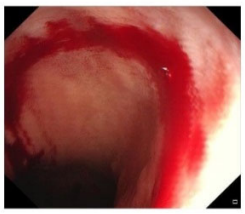


Fig. 7 (b) AB modified in Red by Blue component at row from 383 - 386 and column 313 - 316 LSB

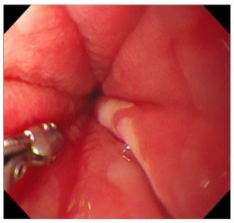


Fig. 8(a) AC modified at blue by the same of green component from raw 238 - 241 and column 300 - 303

Fig. 8(b) AC modified in Red component by 1 at row from 383 - 386 and column 313 - 316 LSB

5. Conclusion

In this paper a new watermarking algorithm for medical images called Originality Identifier Code (OIC) has been proposed. This new approach to maintain high data security combines between the integrity protection, the encryption algorithms and the steganographic techniques.

The new approach has the following advantages:

1. The Processed images have the same size of input images.
2. Although the digital watermark is distributed on every pixel on the image the code has no effect on the output image quality.
3. The Approach is applicable on every RGB Images.
4. The created Secret code has dynamic properties based on:-Imaging devices manufacturers. -basic components of color images (R, G and B).

References

[1] "Health information networks gain wider use." [Online]. Available: http://www.ama-assn.org/amednews/2009/08/17/bisb0817.htm.

[2] F. A. Allaert and L. Dusserre, "Security of health information system in France: what we do will no longer be different from what we tell," International

Journal of Bio-Medical Computing, vol. 35, pp. 201-204, Feb. 1994.
[3] A. Armoni, Healthcare information systems: challenges of the new millennium. Idea Group Inc (IGI), 2000.
[4] P. Jennett, M. Watanabe, E. Igras, K. Premkumar, and W. Hall, "Telemedicine and security. Confidentiality, integrity, and availability: a Canadian perspective," Studies in Health Technology and Informatics, vol. 29, pp. 286-298, 1996.
[5] S. K. Katsikas and D. Gritzalis, Information systems security: facing the information society of the 21st century. Chapman & Hall, 1996.
[6] Mousavi, S.M.; Naghsh, A.; Abu-Bakar, S.A.R. Watermarking techniques used in medical images: A survey. J. Digit. Imaging 2014, 27, 714–729. [CrossRef] [PubMed]
[7] Nyeem, H.; Boles,W.; Boyd, C. A review of medical image watermarking requirements for teleradiology. J. Digit. Imaging 2013, 26, 326–343. [CrossRef]
[8] Pan, J.S., Huang, H.-C., Jain, L.C. (eds.): Intelligent Watermarking Techniques. World Scientific, Singapore (2004)
[9] van Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.: A digital watermark. Proc. IEEE Int. Conf. Image Processing (ICIP 1994), November 1994, vol. 2, pp. 86–90 (1994)
[10] Tirkel, A.Z., Rankin, G.A., van Schyndel, R.M., Ho, W.J., Mee, N.R.A., Osborne, C.F.: Electronic water mark. In: Digital Image Computing Techniques and Applications 1993, pp. 666–672 (1993)
[11] Wolfgang, R.B., Delp, E.J.: Overview of image security techniques with applications in multimedia systems. In: Proc. SPIE Conf. Multimedia Networks: Security,Displays, Terminals, and Gateways, pp. 297–308 (1997)
[12] Voyatzis, G., Pitas, I.: Chaotic watermarks for embedding in the spatial digitalimage domain. In: Proc. IEEE Int'l Conf. Image Processing, pp. 432–436 (1998)
[13] Langelaar, G.C., Setyawan, I., Lagendijk, R.L.: Watermarking digital image andvideo data: A state-of-the-art overview. IEEE Signal Processing Magazine 17, 20–46 (2000)
[14] Hern´andez, J.R., P´erez-Gonz´alez, F., Rodriguez, J.M.: The impact of channel coding on the performance of spatial watermarking for copyright protection. In: Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, pp. 2973–2976
[15] Wang, F.H., Jain, L.C., Pan, J.S.: Genetic watermarking techniques based on spatial domain. In: Proc. 6th Int. Conf. on Knowledge-Based Intelligent Information and Engineering System (KES 2002), Crema, Italy, September 2002, pp.417–422. IOS Press, Amsterdam (2002)
[16] Navas KA, Sasikumar M: Survey of medical image watermarking algorithms, in International Conference: Sciences of Electronic Technologies of Information and Telecommunications. TUNISIA, 2007, pp 1–6.
[17] Al-Qershi OM, Khoo BE: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOMimages. J Digit Imaging 24(1):114–125, 2011
[18] Memon NA, Gilani SAM: Watermarking of chest CT scan medical images for content authentication. Int J Comput Math 88(2):265–280, 2010
[19] Zain JM, Clarke M: Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. Int J Comput Sci Netw Secur 7(9):19–28, 2007
[20] Wakatani A: Digital watermarking for ROI medical images by using compressed signature image, in System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on. pp 2043–2048,2002.
[21] Viswanathan P, Krishna PV: Fusion of cryptographic watermarking medical image system with reversible property, in Computer Networks and Intelligent Computing.In: Venugopal KR, Patnaik LM Eds. Springer Berlin: Heidelberg, 2011, pp 533–540.
[22] Memon NA, Chaudhry A, Ahmad M, Keerio ZA: Hybrid watermarking of medical images for ROI authentication and recovery. Int J Comput Math 88(10):2057–2071, 2011

Ahmad Nagm received B.Sc. degrees in Electrical Engineering from Al-Azhar University, Cairo, Egypt, 2003. Also, He received M.Sc. degree "A NEW ALGORITHM FOR IMAGE RECOGNITION (Face Detection)" from Al-Azhar University, 2010. and Ph.D. degree "Analysis and Design of Data Security Architecture for Next Generation Networks", University of Al-Azhar university, 2018. His research interests include Integrity protection, Steganography Techniques and Encryption Algorithms using by Image processing, based on Image Quality performance estimation, Optimization methods in Digital Watermarking Images.

Mohammed Safy received B.Sc. degrees in Electrical Engineering from Military Technical College (MTC), Cairo, Egypt, 2001. Also, He received M.Sc. degree "Micro-machined bolometer for thermal imaging" from MTC, 2008. and Ph.D. degree "High Resolution Digital Terrain - Elevation Data For Intelligence Gathering and Tactical Target", University of Xian, China, 2014. His research interests include Image processing, Air and Space-borne InSAR, InSAR performance estimation, Optimization methods in SAR image registration.