ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse238952020.pdf

https://doi.org/10.30534/ijatcse/2020/238952020

FRAGILE WATERMARKING SCHEME BASED ON SHA-256 HASH FUNCTION AND MERSENNE TWISTER FOR MEDICAL IMAGE AUTHENTICATION

Noor Aqilah Abdul Halim, Ferda Ernawan, Danakorn Nincarean Eh Phon, Kohbalan Moorthy

Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, 26600 Pekan,
Pahang Darul Makmur, Malaysia

e-mail: aqilahhalim@gmail.com, ferda@ump.edu.my, danakorn@ump.edu.my, kohbalan@ump.edu.my

ABSTRACT

Medical images can be easily manipulated by irresponsible persons and the altered medical image can be hard to identify. Fragile watermarking scheme is an alternative solution to authenticate and protect the medical images. Fragile watermarking scheme becomes vulnerable against modification by attackers. This research proposed a fragile watermarking scheme for medical images based onSHA-256 and Mersenne twister. A medical image was split into a region of interest (ROI) and region of non-interest (RONI). The ROI as watermarked image is encrypted by SHA-256 and the result is scrambled by Arnold transform with a secret key before embedding the watermark. The scrambled hash values are randomly embedded into RONI by using Mersenne Twister with a secret key. The experimental results showed that our scheme produces high imperceptibility with PSNR value of about 83 dB. The proposed scheme was able to detect tampers accurately on the medical images. The proposed scheme improved the invisibility of the watermarked image and it provided additional security. The proposed scheme authenticated and validated the originality of the medical images.

Key words : Arnold Transform , Image Authentication, Image Watermarking, Medical Image, Mersenne Twister

1. INTRODUCTION

The growth of internet technology has increased digital image distribution and transmission [1][2]. The contents of digital images can be easily manipulated by irresponsible persons [3]-[6]. The image contents can be modified to obtain fake image, causing unauthorised alteration of information [7]. Medical images contained patient's confidential information, the medical image transmission has the possibility to be intercepted and tampered by unauthorised users [8]. The modified medical image is prone to misdiagnosis. Therefore, medical images need to be protected from unauthorised alteration. Digital watermarking is one solution to authenticate the right property of digital images [9]. Digital watermarking can authenticate the medical image content or verify the altered digital content. The watermark embedded in the original image remained unaffected to the human visual system [10]. The embedded watermark can be used to detect the alteration of information. Fragile watermarking scheme has been widely used in verification, authentication of digital medical images [11]. Fragile watermarking technique can be used to authenticate the digital image and prove the presence of tamper in the medical image [12].

Watermarking technique can be used for authentication by detecting and recovering the tampered region [13]. Although the recovery on the tampered region is very helpful in reversing the modification, the most crucial part is to determine the authenticity of the medical image [11]. A scheme by Peng [14] presented a watermarking authentication scheme whereby the scheme provides a reversible hiding data against the altered image. The scheme improved the accuracy of tamper detection and maintained the quality of watermarked image.

Sinha et al. [15] showed an authentication and tamper detection in tele-medicine by using zero watermarking. The scheme used discrete wavelet transform (DWT) and SVD to provide unique identification of the host image. The image was divided into four bands of DWT and the LL sub-band id computed by SVD. The scrambling algorithm was computed to provide additional security. The experimental results show that the scheme was able to authenticate the medical image. Since DWT and SVD can provide good quality of the watermarked image, these methods consumed large amounts of computational time due to the mother wavelet transform.

Singh and Pradhan [16] proposed blind watermarking based on region of interest (ROI) and region of non-interest (RONI). The scheme produced good quality of the watermarked image and it was fragile against various tampering. The scheme segmented medical images into ROI and RONI. Each block was then divided into 3×3 sub-block. The average intensity of each sub-block was compared with the average intensity of the respective block to obtain (v) value. The summation of bit value was used to obtain the parity value (p) and the average pixels (r) of each block was used to recover the image block. The scheme embedded v, p and r values using LSB for authentication and image recovery in the ROI region. The least significant bit of each pixel in ROI was collected and embedded into RONI. The embedded bits in ROI and RONI were used to authenticate the medical image. The scheme was able to generate watermarked images with PSNR value of 43.2 dB. The embedding watermark into the ROI region may have given off the effect to the quality of ROI region. The scheme will cause the ROI to become slightly degraded and change the image information.

Liew et al., [17] presented tamper localisation and lossless recovery (Tallor) in watermarking schemes to authenticate medical images. The Tallor scheme achieved PSNR value of 47.7 dB for the watermarked image. The scheme aims to identify the tampered location and recover the tampered region. Tallor scheme divides the host image into a ROI and eight RONI areas. First, the ROI image is compressed by using lossless compression. The compressed ROI image is embedded in the RONI area for watermark recovery. Second, the ROI is computed by hash function, the encrypted hash value is inserted in another RONI for authentication. Tallor scheme embedded hash value in a vector of RONI regions. The scheme allows the irresponsible person to predict the hash function location. It marks the tampered image that is detected as non-tampered image. The scheme allows irresponsible users to change the image information.

This paper proposed a fragile watermarking scheme to maintain the quality of watermarked image, detect tampered image and prove the authenticity of medical images. The region of interest is found in the host medical image as watermark was computed by SHA256, then encrypted hash values were scrambled by using Arnold Transform with a secret key. The embedding location in the RONI area wasrandomly chosen by using Mersenne twister. The scrambled hash values wererandomly embedded in RONI by using LSB. The proposed watermarking authentication is expected to improve the security of the embedded watermark and it can authenticate the altered image information. The proposed scheme can maintain the quality of watermarked image with high PSNR value.

2. PROPOSED SCHEME

This research proposed embedding watermark using hash function value for tamper localization and authentication. The proposed scheme randomly embedded the bits of ROI into the RONI region using Mersenne Twister with a secret key. The ROI is computed by Hash function and it is scrambled by Arnold transform before embedding the watermark bits. The block diagram of the proposed fragile watermarking scheme is shown in Figure 1.

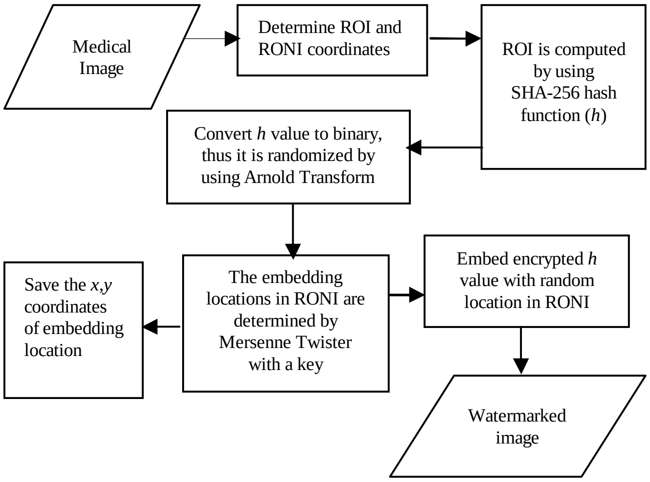

Medical Image
Determine ROI and RONI coordinates
ROI is computed by using SHA-256 hash function (*h*)
Convert *h* value to binary, thus it is randomized by using Arnold Transform
Save the *x*,*y* coordinates of embedding location
The embedding locations in RONI are determined by Mersenne Twister with a key
Embed encrypted *h* value with random location in RONI
Watermarked image

Figure 1: Embedding Process

Figure 1 shows step-by-step of embedding process. The medical image is divided into ROI and RONI regions. The ROI is computed by Hash function and thus, it is scrambled by Arnold transform. The embedding locations of RONI is randomly selected by using Mersenne Twister with a key. The hash value of ROI image is randomly embedded in RONI location. The compressed ROI is also embedded into another RONI image. The flowchart of the authenticating the medical image is shown in Figure 2.

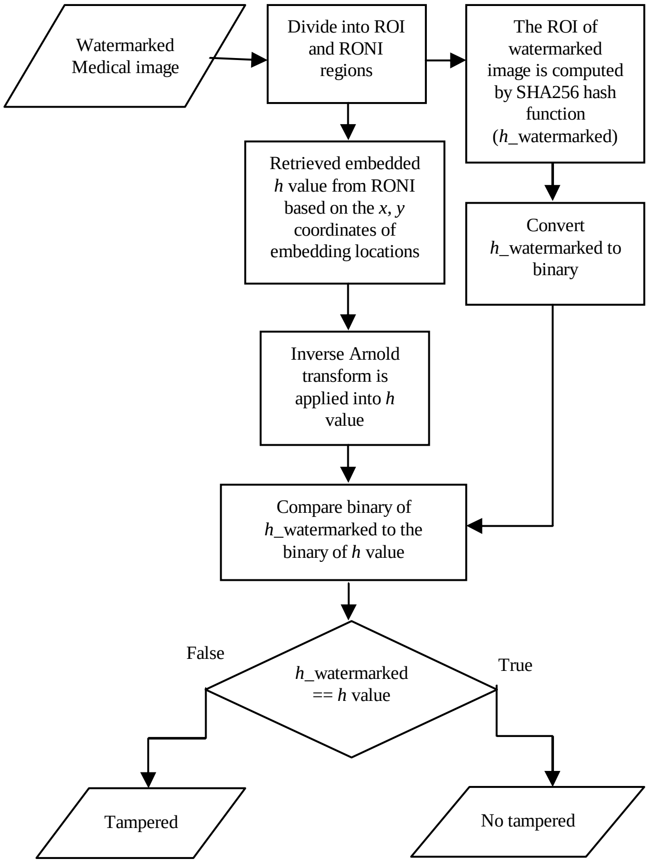

Watermarked Medical image
Divide into ROI and RONI regions
The ROI of watermarked image is computed by SHA256 hash function (*h*_watermarked)
Retrieved embedded *h* value from RONI based on the *x*, *y* coordinates of embedding locations
Convert *h*_watermarked to binary
Inverse Arnold transform is applied into *h* value
Compare binary of *h*_watermarked to the binary of *h* value
False
*h*_watermarked == *h* value
True
Tampered
No tampered

Figure 2: Authenticating Process

Figure 2 shows the authentication process of the proposed scheme. The watermarked image was divided into ROI and RONI. The ROI of the watermarked image was computed by hash function to authenticate the hash value. The coordinates of embedded hash values were retrieved according to the Mersenne twister. The inverse Arnold transform was applied to decrypt the hash value for authentication. The hash values of ROI and RONI were compared to authenticate the medical image.

2.1 Fragile Embedding Watermark

The algorithm of the proposed fragile watermarking is discussed in Algorithm 1.

Algorithm 1: Fragile embedding watermark

```
Input: Medical Image
Step 1:   Determine the ROI and eight RONI coordinates in the medical images
Step 2:   The ROI image is computed by SHA-256 hash function.
Step 3:   The hash values are converted into binary number; and thus its numbers are scrambled by Arnold transform
Step 4:   The embedding location are randomly determined by using Mersenne Twister in the selected RONI region.
Step 5:   The encrypted hash values are embedded by using LSB technique based on the selected embedding location.
Output:   Watermarked Image
```

The least significant bits of ROI are used to authenticate the originality of the medical image. The selected RONI area is used to save the least of significant bits of ROI for authentication and it also used to store seventh most bits of ROI for recovery the ROI image. The watermark authentication algorithm is discussed in the next sub-section.

2.2 Watermark Authentication Algorithm

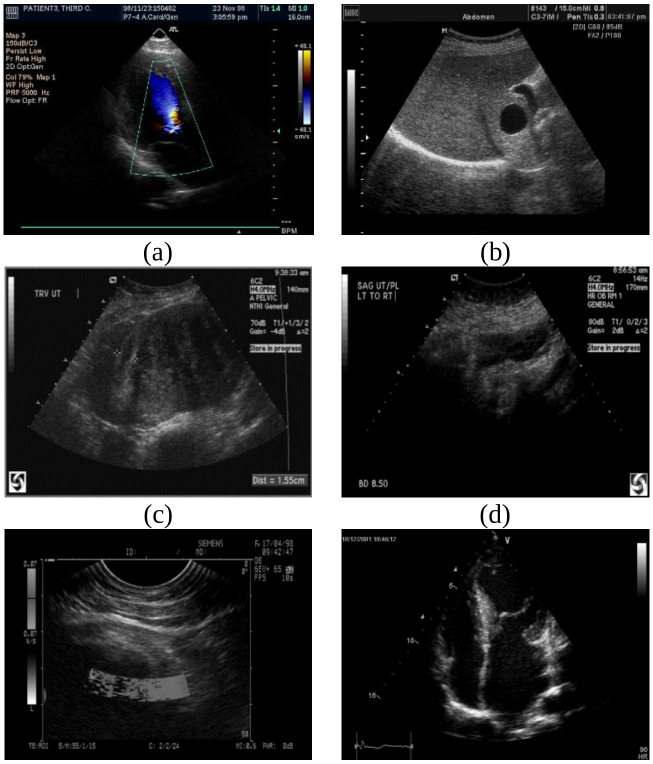
The step-by-step of authentication watermark medical image is explained in Algorithm 2.

Algorithm 2: Authentication process

```
Input: Watermarked Medical Image
Step 1:   The watermarked medical image is divided into ROI and RONI regions.
Step 2:   The ROI of watermarked image is computed by SHA256 hash function to generate hash value. Thus, the hash value is converted into binary numbers.
Step 3:   The embedded h values in RONI are extracted based on the x, y coordinates of embedding locations.
Step 4:   Perform inverse Arnold transform to the h value from RONI. Thus, the h values are converted into binary numbers.
Step 5:   Compare h values obtained from the ROI of watermarked image and h values obtained from the RONI.
Step 6:   If the result is same, it means that there is no tampered image. If the result is not same, the tampered image is detected.
Output:   Originality: True or False
```

3. EXPERIMENTAL SETUP

These experiments used six medical images with the format file (.bmp) to test the proposed fragile watermarking scheme. The sample medical images used were ultrasound images with the size 480×640 pixels. Six sample medical images are shown in Figure 3. The visual illustration of ROI and RONI regions are shown in Figure 4.



(a) (b)

(c) (d)

(e) (f)

Figure 3: (a)Sample 1; (b)Sample 2; (c)Sample 3; (d)Sample 4; (e)Sample 5; (f)Sample 6

Figure 3 shows the sample of medical images that will be tested by Tallor and proposed fragile watermarking schemes. All medical images were in bmp format with the file sizes of 800 Kb.

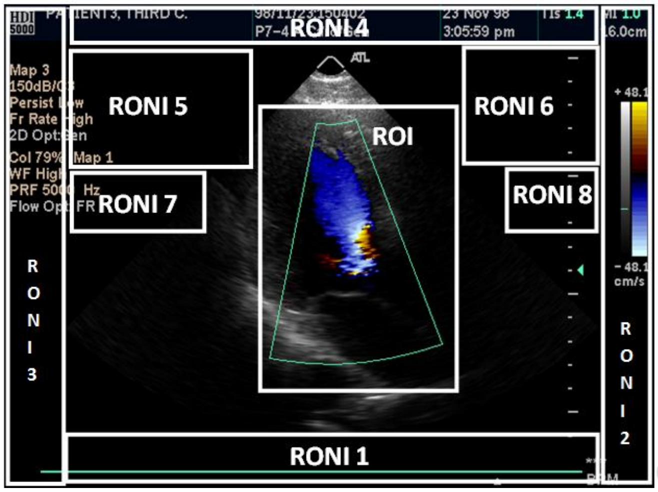


Figure 4: ROI and Eight RONI regions

According to Figure 4, each sample of medical image was divided into ROI and RONI. The ROI image was used as watermark information that will be embedded in RONI for authentication.

4. EXPERIMENTAL RESULTS

The imperceptibility results of the proposed scheme in terms of PSNR value of the watermarked image are listed in Table 1.

Table 1: Comparison of PSNR value between Tallor and proposed scheme.

Medical Images	Tallor Scheme [17]	Proposed Scheme
Sample 1	52.925	86.667
Sample 2	52.316	86.842
Sample 3	49.479	82.213
Sample 4	49.553	81.606
Sample 5	48.365	81.766
Sample 6	47.988	81.899
Average	50.104	83.499

Table 1 presents the comparison of PSNR value obtained from proposed watermarking scheme and Tallor scheme for six medical images. The proposed scheme improved by 39.99% (((83.499-50.104) / 83.499) ×100%) of average PSNR value. The proposed scheme produced minimum distortion of the watermarked image. The visual comparison of PSNR values between Tallor and the proposed fragile watermarking is shown in Figure 5.

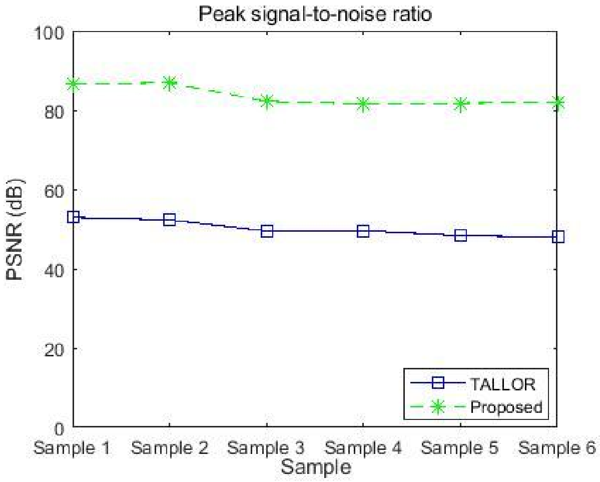


Figure 5: PSNR values of the proposed scheme for six sample medical images

According to Figure 5, the proposed scheme produced superior PSNR values for six images. The average PSNR value for six sample images was about 83dB. The proposed fragile watermarking is able to produce high quality and closer to the original medical image. The proposed scheme was also evaluated by means square error (MSE). The MSE value of the proposed scheme is shown in Table 2.

Table 2: Comparison of MSE value between Tallor and proposed scheme.

Figure	Tallor Scheme [17]	Proposed Scheme
Sample 1	0.3316	1.40E-04
Sample 2	0.3815	1.35E-04
Sample 3	0.733	3.91E-04
Sample 4	0.7206	4.49E-04
Sample 5	0.9473	4.33E-04
Sample 6	1.0334	4.20E-04

Table 2 shows the MSE value of the watermarked image obtained from Tallor scheme and the proposed scheme for six medical images. The proposed fragile watermarking scheme produced minimum MSE values comparable to the Tallor scheme. It can be noticed that the proposed fragile watermarking scheme was able to produce minimum distortion in the watermarked image and it was closer to the original medical image.

The proposed fragile watermarking scheme was also evaluated based on the computational time for embedding and authenticating the medical images. Tallor method embedded hash value as a vector in RONI area, as irresponsible persons may easily replace the hash value and so the tampered medical images were not detected. The proposed scheme provides additional security, especially random embedding the hash value in RONI region. Attackers are not able to update embedded hash value; it can make authentication process more secure than other existing schemes. The comparison of the embedding time between Tallor scheme and the proposed scheme is shown in Table 3.

Table 3: Embedding time between Tallor and proposed methods

Medical Images	File Size (KB)	Tallor Scheme [17]	Proposed Scheme
Sample 1	893	105.437	1.812
Sample 2	901	135.828	1.828
Sample 3	302	38.875	1.640
Sample 4	302	31.484	1.687
Sample 5	302	38.234	1.812
Sample 6	302	40.890	1.843
Average		65.125	1.770

Referring to Table 3, shows that the proposed fragile watermarking scheme required minimum embedding time for six medical images. The proposed scheme required 1.770ms to embed the watermark in RONI region. The proposed scheme consumed less computational time than Tallor scheme. The authentication is the process to verify the originality of medical images. Authentication time plays an important role to provide information certainty. The comparison of the authentication time between Tallor and the proposed scheme is listed in Table 4.

Table 4: Authentication time between Tallor and proposed schemes.

Medical Images	File Size (KB)	Tallor Scheme [17]	Proposed Scheme
Sample 1	893	1.7344	1.7969
Sample 2	901	1.8438	1.7188
Sample 3	302	1.7500	1.5469
Sample 4	302	1.8750	1.7500
Sample 5	302	1.5625	1.6094
Sample 6	302	1.6563	1.7188
Average		1.737	1.690133

According to Table 4, the proposed fragile watermarking scheme required 1.69 ms to verify the originality of the medical images. The embedded hash values of ROI had an important role for image authentication. If the embedded hash values in RONI are like the hash value of ROI in the watermarked image, it means the medical image is marked as authentic. The visual comparison of authentication time for six medical images is shown in Figure 6.

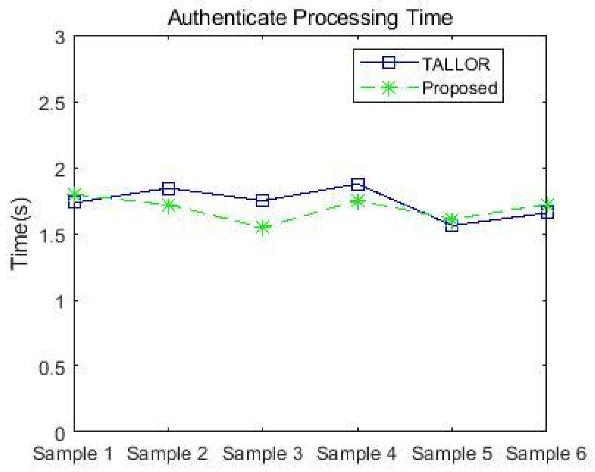


Figure 6: Comparison between the Tallor and proposed schemes for authenticating the medical images

As visualised in Figure 6, the proposed scheme required minimum time taken for authenticating the medical images with different file sizes. Both Tallor and the proposed schemes can successfully verify the originality of the medical image.

5. CONCLUSION

This paper presented fragile watermarking scheme for medical image authentication based on SHA-256 and mersenne twister. The proposed scheme presented encrypted watermark bits and the randomly embedding location in RONI. The experimental results showed that the proposed scheme was able to perform faster embedding, by detecting the tampered image, and authenticating the originality of image more than the scheme by Tallor. The proposed scheme produced high PSNR value, successfully maintaining the quality of the original medical image. The proposed scheme was able to fast authenticate the medical image against tampered image.

ACKNOWLEDGEMENT

This work was supported by UMP Research Grant Scheme (RDU190370) from Universiti Malaysia Pahang, Malaysia.

REFERENCES

1. F. Ernawan, M.N. Kabir. **A block-based RDWT-SVD image watermarking method using human visual system characteristics.** *Visual Computer*, vol. 36, no. 1, 19-37, 2020.
2. F. Ernawan, M.N. Kabir. **A blind watermarking technique using redundant wavelet transform for copyright protection.** *14th IEEE International Colloquium on Signal Processing and its Application*, pp. 221-226, 2018.
3. F. Ernawan. **Tchebichef image watermarking along**

the edge using YCoCg-R color space for copyright protection. *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 1850-1860. 2019.

4. F. Ernawan, M.N. Kabir. **A blind watermarking technique using redundant wavelet transform for copyright protection**. *IEEE 14th International Colloquium on Signal Processing & Its Applications* (CSPA), pp. 221-226, 2018.
5. F. Ernawan, D Ariatmanto. **Image watermarking based on integer wavelet transform-singular value decomposition with variance pixels**. *International Journal of Electrical and Computer Engineering*, vol. 9, no. 3, pp. 2185-2195, 2019.
6. M. Batikas, J. Claussen and C. Peukert. **Follow the money: Online piracy and self-regulation in the advertising industry**. *International Journal of Industrial Organization*, vol. 65, pp. 121-151, 2019.
7. V. Khanduja. **Database watermarking, a technological protective measure: Perspective, security analysis and future directions**. *Journal of Information Security and Applications*, vol. 37, pp. 38-49, 2017.
8. Z. Zhang and B. B. Gupta. **Social media security and trustworthiness: Overview and new direction**. *Future Generation Computer Systems*, vol. 86, pp. 914-925, 2018.
9. A. Pramila, A. Keskinarkaus and T. Seppänen. **Increasing the capturing angle in print-cam robust watermarking**. *Journal of Systems and Software*, vol. 135, pp. 205-215, 2018.
10. D. Renza, D. M. B. L. and C. Lemus. **Authenticity verification of audio signals based on fragile watermarking for audio forensics**. *Expert Systems with Application*, vol. 91, pp. 211-222, 2018.
11. B. B. Haghighi, A. H. Taherinia and A. H. Mohajerzadeh. **TRLG: Fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA**. *Information Sciences*, vol. 486, pp. 204-230, 2019.
12. A.F. Qasim, F. Meziane and R. Aspin. **Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review**. *Computer Science Review*, vol. 27, pp. 45-60, 2018.
13. N. Sasikaladevi, K.Geetha and A.Revathi. **EMOTE – Multilayered encryption system for protecting medical images based on binary curve**. *Journal of King Saud University - Computer and Information Sciences*, 2019.
14. Y. Peng, X. Niu and Z. Yin. **Image authentication scheme based on reversible fragile watermarking with two images**. *Journal of Information Security and Applications*, vol. 40, pp. 236-246, 2018.
15. S. Sinha, A. Singh, R. Gupta and S. Singh. **Authentication and tamper detection in tele-medicine using zero watermarking**. *Procedia Computer Science*, vol. 132, pp. 557-562, 2018.
16. P. Singh and A. K. Pradhan. **Medical Image Watermarking for Authentication, Confidentiality, Tamper Detection and Recovery.** *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, pp. 1-7, 2019
17. S.-C. Liew, S.-W. Liew and J.M. Zain. **Tamper localization and lossless recovery watermarking scheme with ROI**. *Journal of Digital Imaging*, vol. 26, pp. 316-325, 2012