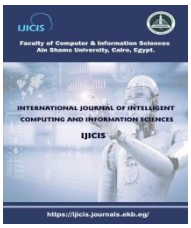
IJICIS, Vol.21, No.1, 119-131
DOI: 10.21608/ijicis.2021.66278.1067

International Journal of Intelligent Computing and Information Sciences

https://ijicis.journals.ekb.eg/



MEDICAL IMAGES WATERMARKING SCHEMES, A REVIEW

Alaa H. ElSaadawy
Computer Science department, Computer and Information Science, Ain Shams University, Cairo, Egypt
Alaa_Elsaadawy@cis.asu.edu.eg

Ahmed S. El-Sayed
Computer Science department, Computer and Information Science, Ain Shams University, Cairo, Egypt
Ahmed_Salah@cis.asu.edu.eg

M. N. Al-Berry
Scientific Computing department, Computer and Information Science, Ain Shams University, Cairo, Egypt
Maryam_nabil@cis.asu.edu.eg

Mohamed Roushdy
Computer Science departement, Computer and Information Science, Ain Shams University, Cairo, Egypt
mohamed.roushdy@fue.edu.eg

Received 2021- 3-5; Revised 2021-5-1; Accepted 2021-5-9

Abstract: As a result of internet expansion, the popularity of sharing medical documents between specialists in different medical institutes and hospitals has increased. Accordingly, protecting the transmitted patient's data against any modification or accessing from unauthorized people is a must. One of the popular solutions for protecting patient's data against tampers like copy-past, text addition and content removal and various geometric attacks like crop, rotate and resize and signal attacks like histogram equalization, Gaussian noise, median filter, and sharpening is watermarking techniques. Watermarking techniques can be classified according to many perspectives like Robustness, Human Perceptivity, Task Performed, Domain Type, Extraction Process and Secret Keys. Medical image can be in the spatial domain and transform domain. This paper presents a review of recent watermarking techniques of medical images and a comparison between various types of transform domains and the different purposes of medical images' watermark. A proposed scheme is presented in this paper.

Keywords: *Watermarking, Spatial domain, Transfer domain, Tamper localization, Attacks.*

1. Introduction

Spreading of computer networks has facilitated sharing medical images in some services like telediagnosis, telemedicine and teleconsultation. To avoid misdiagnoses and understanding diseases, sharing patients' information among specialists in different hospitals is a must [1] [2] [3]. Nowadays, watermarking

* Corresponding author: Alaa H. ElSaadawy

Computer Science department, Computer and Information Science, Ain Shams University, Cairo, 11566, Egypt
E-mail address: Alaa_Elsaadawy@cis.asu.edu.eg

techniques contribute to protecting transferred medical images against any unauthorized access or corruption [4].

Medical images can be watermarked by embedding the patient's data in it. Keeping medical image without distortion after embedding patient's data in it is essential to ensure the confidentiality of the transmitted images [5] [6]. The main purposes of medical images watermarking are: ensuring that the source is valid and belongs to the right person, which is called authenticity and make sure that there is no modification on the transmitted image, which is called integrity control. Integrity control is important since modifying medical images may lead to misdiagnosis. [7] [8] [9].

Encrypting the medical image is considered as one of the main steps to ensure patient's data is secure. There are several encryption techniques [10], Elliptic-Curve-based encryption (ECC), International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), Advanced Encryption Standard (AES), private key encryption standards, and public key standards such as Rivest-Shamir-Adleman (RSA).

Huge long-term storage space is required to store transmitted medical images, that is why compressing the medical image before transmission is also an essential phase. There are two types of image compression algorithms, namely, lossless used in case we need to restore the original data without any loss. And for achieving a high compression rate, lossy algorithms are used [11].

As shown in Figure 1, watermarking process is based on host image, which is the image to be transferred and in our case is the medical image, and the watermark image, image used to watermark the host image before transferring. Transformation technique is applied on host and watermark image then watermarking technique is applied to embed the watermark image in the host image [12].

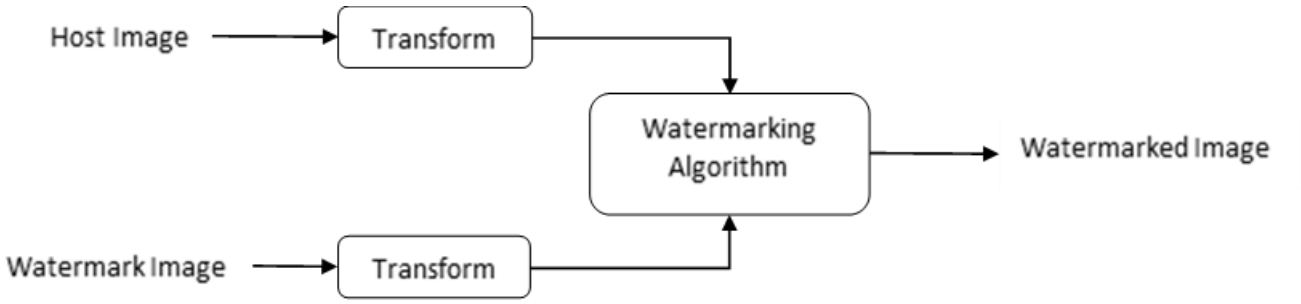


Figure. 1: Watermarking Process

2. Advantages of Medical Images Watermarking

Memory and bandwidth saving, detachment avoidance, confidentiality and security are the main advantages of medical images watermarking [1].

- Memory and Bandwith Saving: means to reduce the bandwidth needed for telemedicine applications by integrating the Electronic Patient Record (EPR) in the medical image.
- Detachment Avoidance: Allocating wrong EPR for the medical image is called misplacement or detachment. Detachment results from sending EPR and medical image separately. Integrating EPR in the medical image has solved the detachment problem.
- Confidentiality: By integrating EPR into the medical images, it ensures the prevention of unauthorized access of the patient's data.
- Security: For preventing the patient's data or medical image from attackers modifications and tamper, watermarking techniques are used for hiding patient's data in the medical image.

3. Digital Watermarking Classification

In this section we discuss several classification taxonomies of digital watermarking techniques. In the next section we present a detailed survey of watermarking techniques classified according the used domain. Digital watermarking techniques can be classified according to many perspectives [13], such as, robustness, human preceptivity, the task performed, the work domain, the extraction process and the Secret keys. Figure 2 summerizes these classifications.

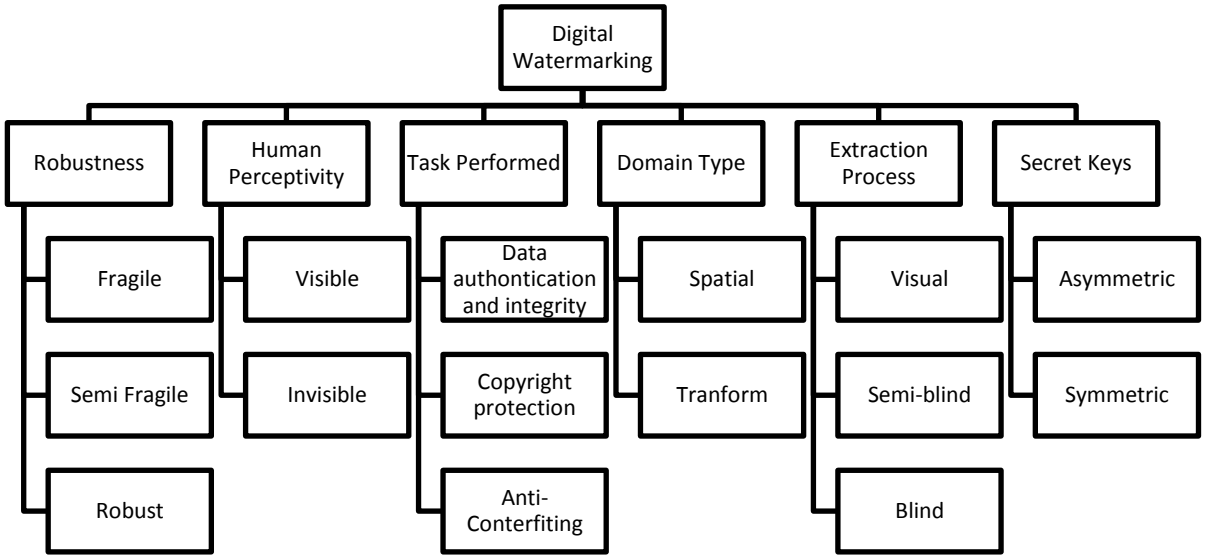


Figure. 2: Digital Watermarking Classification

3.1. According to Robustness

- Fragile watermarking: Is sensitive to signal changes and every possible pixel value change can be detected using fragile techniques, that is why it is used in integrity protection[13] [14].
- Semi-Fragile watermarking: Some schemes are tolerant of certain distortions like the addition of noise attacks and JPEG or wavelet compression. Semi-fragile watermarking provide authentication with a degree as a softer evolution [13] [14].
- Robust watermarking: Can easily detect any kind of attacks like geometric and signal attacks [13].

3.2 According to Human Perceptivity

- Visible watermarking: Can be seen by eyes like logos. It is not convenient for today's digital applications as it destroys media presentation [13].
- Invisible watermarking: Is used to insert secret information that is not seen by human eyes [13].

3.3 According to Task Performed

- Data authentication and integrity watermarking: Is to ensure that the image belongs to the right patient and keep the content of the image which ensures that it has not been modified [1] [13].
- Copyright protection watermarking: Is to protect the watermarked image against any attack. And try keeping the watermark as it is after attacks [15].
- Anti-Counterfeiting watermarking: Is used to prevent paper notes like Quick Response (QR) from being copied and can be detected after printing [13] [16].

3.4 According to Working Domain

- Spatial domain watermarking: Randomly chooses one or two subsets to embed the watermark information directly. To preserve the quality of the image, choosing the Least Significant Bit (LSB) to embed the watermark is the most popular technique. These methods are fast, simple and provide high capacity for embedding watermarks. Spatial domain watermarking can be easily attacked [1][13].
- Transform domain watermarking: It is also called frequency domain watermarking [13]. The transform is applied to the host image before embedding the watermarking information. Some popular transform that can be used include Discrete Fourier transform (DFT), Discrete-Wavelet Transform (DWT), Singular Value Decomposition (SVD), Discrete-Cosine Transform (DCT) and Dual-Tree Complex Wavelet Transform (DTCWT). The watermarking data is embedded in the transform coefficients [1].

3.5 According to Extraction Process

- Visual watermarking: It is called private or non-blind watermarking. It has the strongest robustness. During the extraction process, the host image is required. Its applications are limited [1][13].
- Semi-Blind watermarking: In extraction process watermark information or side information is required [1].
- Blind watermarking: No need for any additional information, watermark information or host image in the extraction process. In this case, higher watermark technology is required [1][13].

3.6 According to Secret Keys

- Asymmetric watermarking: Different keys are used in embedding and extracting watermark information [13].
- Symmetric watermarking: For embedding and extraction process the same key is used [13].

4. Spatial and transform domain watermarking techniques

Watermarking can be done in different domains. Spatial and transform domain are the two main domains for watermarking techniques [1][17].

4.1 Spatial Domain Techniques

In the spatial domain, a cover image (host) image are used as a domain for directly embedding the information of watermark in the pixel value of the host image. Least significant bits of host image are used for embedding the watermark values to keep image quality. These methods provide high capacity for embedding watermarks besides they are fast and simple [1][18].

One of the drawbacks of spatial domain is that it is weak against lossy compression and noise [17]. Also modifying the watermarked image by third parties becomes easy. Least Significant Bit (LSB) is the simplest spatial domain techniques. It is based on replacing the most right bit in the binary value of each pixel of the medical image with watermark value. At the end, the modified binary pixel value is converted to a decimal value [1].

Local Binary Pattern (LBP) is another method in the spatial domain category [19]. LBP method is used in many applications like face recognition, texture analysis and crowd estimation [20]. In LBP, the local pixel contrast is computed by measuring the spatial ratio between the center pixel and its neighbouring pixels after splitting the image into non-overlapping blocks,. Then used rule mentioned in for embedding the watermark in these pixels. Despite being robust against contrast adjustment and luminance change, LBP is fragile to other attacks like blurring and filtering. That is why LBP is considered as a semi-fragile watermarking technique and is preferred over LSB [1].

Taking the global characteristics of the host image in consideration for embedding the watermark is one of the spatial transform methods called histogram modification [21]. In the data-hiding phase, values are shifted between the minimum and maximum points in the histogram as the main step [22]. From the advantages of this method is besides being easy to be implemented, the side information generated is varied. But on the other hand, the limitation of the embedding capacity according to the number of maximum points is a drawback of this method [1].

4.2 Transform Domain Techniques

Transform domain techniques depend on transforming the host image, then embedding the watermark in the coefficients of the transformed image [23][24]. The original signal is retrieved by inverting the modified coefficients. It has been proven that transforming the host image before embedding the watermark makes it robust against some attacks like JPEG compression [24][25]. Transform domain methods are also used to protect the watermarked images against signal processing attacks. singular Value Decomposition (SVD), Discrete Wavelet Transforms (DWT), Discrete Cosine Transforms (DCT) and Discrete Fourier Transforms (DFT) are examples of transform domains that can be used in watermarking techniques. Providing higher robustness and imperceptibility and protecting watermarked images against signal processing attacks distinct these methods from other methods. On the other hand, spatial domain computational cost is less than transform domain techniques [26]. A comparison between the advantages and disadvantages of different transform domain methods is presented in Table 1 [26].

Table 1 Transform Domain Methods Comparison

Technique	Advantages	Disadvantages
SVD	Strength against signal and geometric attacks Energy compaction is high Computation cost is low	Computation expense is raised in case of lonely used False-positive problem
DCT	Execution time is reasonable Compared with DFT, DCT is easier computation Fast with JPEG compression	Visibility of the blocks due to the higher compression ratio

	standard Good imperceptibility	
DWT	Good in spatial localization, frequency analysis time and energy compaction Strength against signal processing attacks	Weakness against geometric attacks High computation complexity
DFT	Strength against rotation and scaling attacks	Weakness against shearing and cropping attacks The difficulty of analysis due to loss of frequency analysis time

A Comparison between spatial and transform domain techniques is shown in Table 2 [26].

Table 2 Spatial and Transform Domain Techniques Comparison

Characteristics	**Spatial Domain**	**Transform Domain**
Capacity	Low	High
Imperceptibility	Yes	Yes
Robustness	No	Yes
Speed	Fast	Slow
Time Spending	No	Yes
Cost of Operation	Low	High
Simplicity	Yes	No
Security	No	Yes
Computational Load	No	Yes

5. Attacks

As shown in Figure 3, digital image watermark attacks are classified into five categories [27] [28].

- Simple attacks: Correction and cropping are examples of signal attacks. It does not make any effort to isolate watermark information, it modifies the whole image to damage the embedded watermark information [27].
- Removal attacks: The complete removal of the watermark information is the goal of the attacks without cracking the encryption technique. That is recovering watermark information from attacked image becomes impossible. Blurring, histogram equalization, noising and sharpening are examples of these attacks [27].

- Geometric attacks: These attacks aim to make detection of the watermark impossible. Some geometric attacks are made on the image like zooming, rotation, removal, cropping and shift in spatial. Using increased intelligence of the watermark detector can make the extraction of the watermark possible [27].
- Protocol attacks: As a copyright protection solution, protocol attacks target the entire concept of using watermarking techniques. Copy attack is one of the protocol attacks, copy attack copies an estimated watermark instead of destroying it [27].
- Cryptographic attacks: Embedding several additional watermarks to discredit the authority of the watermark information is a way to misleading the watermark detector by extracting fake watermark information [28].

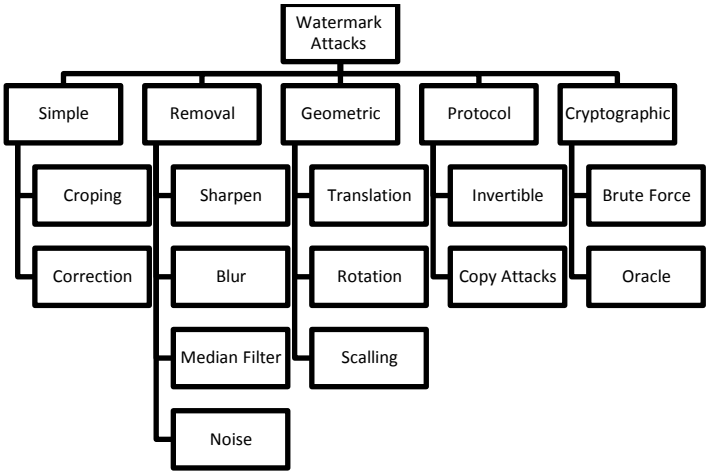


Figure.3: Watermark Attacks Categories

6. Watermarking Systems Requirements

In addition to fidelity, robustness, data payload (capacity), security, computational complexity (speed) and perceptibility, which are basic requirements for digital watermarking requirements, imperceptibility, reversibility, integrity control and authentication are requirements for medical systems watermarking [1].

Here we will explain each requirement [1]:

- Fidelity: Measures how the watermarking technique affects the medical image. It measures the similarity between the image before and after embedding the watermark.
- Robustness: Protecting the watermarked images against malicious and innocent attacks. Attackers use malicious attacks like geometric distortion and noise addition to disabling watermark. When processing digital watermarking, innocent attacks like compression, resizing and cropping commonly happen.
- Data Payload (Capacity): Data payload is inversely proportional to robustness and directly proportion to perceptibility. Data payload is the maximum amount of data that can be added to the host image while keeping the quality of the image. One of the main factors in data payload is the host image size, the watermark applicable size increases when the resolution of the image increases.
- Security: Protecting the watermarked images from unauthorized persons. Only an authorized person can extract the watermark from the image. Public and private keys are kinds of security keys.

- Computational Complexity (Speed): Computational complexity of embedding and extracting the watermark depends on the complexity of the used algorithm. In real-time applications, computational complexity time plays an important role. So it is important to keep computational complexity as low as possible. In security applications, we focus on the security more than time so embedding and extracting processes usually consume more time.
- Perceptibility: It means how the watermark insertion visually distorts the medical image. This factor should be small in invisible watermarking applications.
- Imperceptibility: The structural similarity index measure (SSIM) and Peak signal to Noise Ration (PSNR) are used in measuring imperceptibility. Imperceptibility measures the similarity between the watermarked image and non-watermarked images. As the imperceptibility increases, the invisibility of watermark increases.
- Reversibility: The used watermarking technique is reversible if the original medical image can be extracted besides of extracting watermark image. This requirement helps keep image quality.
- Integrity Control: Protecting the watermarked image from unauthorized modifications.
- Authentication: Protecting the transferred image from unauthorized access and making sure that the image belongs to the correct patient.

7. State-of-Art

In this section, the most important relevant studies to our research topic are presented and discussed in terms of the used techniques, and the achieved accuracy.

Table 3 shows a summarized comparison between some of the related studies, in terms of the main points of comparison which are: 1) Embedding technique; 2) Data payload (Capacity); 3) Encryption technique; 4) Compression algorithm; 5) Number of geometric and signal processing attacks that can be detected; 6) Can localize tamper?; 7) Can restore original image besides watermark image; 8) Dataset used; 9) Calculated PSNR; 10) Calculated SSIM.

Table 3 A brief survey on the key studies for medical images watermarking

	Embedding Technique	**payload**	**Encryption**	**Compression**	**#Attacks**	**Localize Tamper?**	**Restore Original Image?**	**Dataset**	**PSNR**	**SSIM**
A. Shehab et al. [29]	LSB & SVD	-	-	-	-	Yes	Self recovered tampered image	12 grey medical images with size 512×512	36.24 dB	-
F. Abbasi et al. [30]	IWT, AE & LSB	0.593 bpp	-	-	0	No	No	Not mentioned	32.23 dB	-
A. Sharma et al. [31]	2nd DWT level on ROI & RONI	33 character in 512×512 image	RSA	Hamming code	8	No	Yes	MRI, CT Scan and ultrasound images with size 512×512 [32]	ranges from 36.420885 to 51.833272 dB	-
S. Gull et al. [33]	LSB	1 bpp, 8192 bytes in 256×256 image	-	-	10	Yes	No	14 grey x-ray images with size 256×256 from OPENi dataset [34]	51.26 dB	0.9950
K.J. Kavitha et al. [35]	IWT	0.343262 bpp	-	-	0	No	No	Different bit planes of the United State (US) medical images	52.007 dB	0.64
V. Kaya et al. [36]	DWT, DCT, DFT & LSB	-	-	-	11	No	No	3 different MR medical	39.19 dB	-

								images		
R.P. Singh et al. [37]	IDWT	-	-	-	4	No	No	Samples of X-rays and CT-Scan greyscale medical images	-	-
Y. AL-Nabhani et al. [38]	Three DWT levels & Probabilistic Neural Network(PNN)	Image with size 64x64 in host image with size 512×512	-	-	5	No	No	Sample on a greyscale image with size 512×512	71 dB	-
L. Laouamer et al. [39]	LSB	Watermark image with size 85×85 in host image with size 255×255	-	-	5	Yes	No	8 grey-scale images with size 255×255	65.2 dB	-
M.E. Moghaddam et al. [40]	ICA	-	-	-	3	No	No	Different images with size 512×512	45.63 dB	-
R. Thanki et al. [4]	Fast Discrete Curvelet Transform (FDCuT) & DCT	-	-	-	11	No	No	Various medical images such as X-ray, US, MRI, and CT. With size 1024 × 1024 pixels.	45 dB	-
S. Nithya et al. [41]	ROI & RONI	256 Byte in 512x512 image	AES	Arithmetic lossless compression	0	No	Yes	CT-scan, MRI, X-ray, Barium study, Mammogram and USG with different file format DICOM, GIF, TIF a BMP with break 10 image for each format	25.1782dB	-
S. Liew et al. [42]	ROI & RONI	256 Byte in 512x512 image	AES	Arithmetic lossless compression	0	No	Yes	CT-scan, MRI, X-ray, Barium study, Mammogram and USG with different file format DICOM, GIF, TIF a BMP with break 10 image for each format	25.1782dB	-
T. Agung B.W et al. [43]	LSB & ROI & RONI	ROI is embedded in RONI	-	RLE	3	Yes	Yes	-	between 56 dB and 61 dB	-
A. Wakatani [11]	ROI & RONI	1 bpp	-	HS	0	No	No	-	22.3 dB	-
A. K. Singh [44]	LWT & DCT	Watermark image with	MD5	-	8	No	No	Coloured images with	34.72 dB	-

		size 64x64 and patient report with 80 characters in a colour image with size 512x512						various sizes are selected from [45]		

8. Conclusion and Proposed Watermark Scheme

In this paper, a survey of watermarking techniques is presented. Also, to help in the new research in this area, we present a comparative and brief analysis of image watermarking techniques. Different classification schemes of watermarking have been discussed with an emphasis on spatial and transform domain techniques.

The following observations can be concluded from the existing studies in the literature as discussed in the previous section: most of the existing studies can't localize tampers. Only a few numbers of the existing studies apply an encryption and compression phase. It is also noted that most of the existing student is irreversible, which means that it allows the recovery of the watermark image only without the original medical image.

After this analysis, we propose a watermarking, as shown in Figure. ***1***, scheme which depends on embedding watermark image in the host image using LSB algorithm, after that applying RSA to encrypt the transmitted image then Huffman encoding compression algorithm is applied to reduce the size of the transmitted image. The advantages of the proposed scheme are that it reduces the size of the transmitted watermarked image, encrypt the watermarked image before transmission to protect patient's data and it is reversible so it can retrieve the host and watermark images. The proposed method is robust against geometric and signal attacks, as the proposed scheme is based on LSB embedding technique which is sensitive against changes.

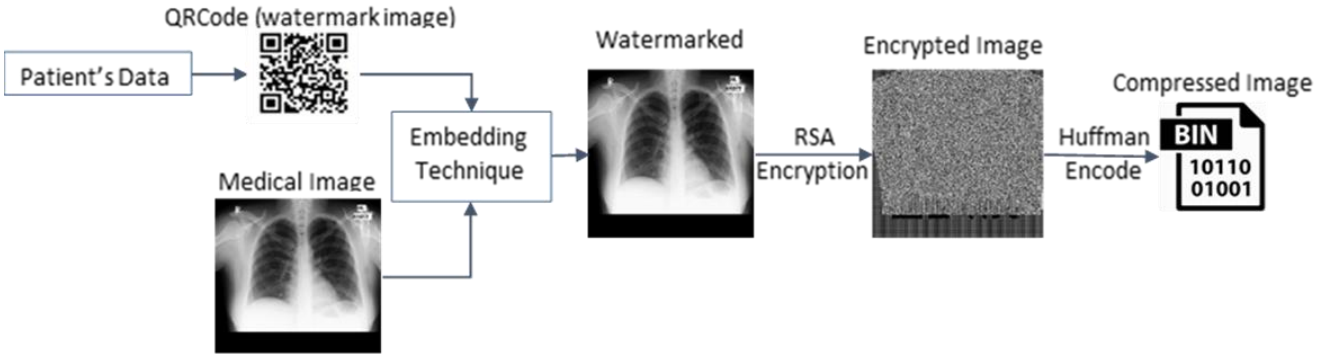


Figure. 1: Architecture of Proposed Watermark Scheme

References

1. Seyed Mojtaba Mousavi, Alireza Naghsh, S. A. R. Abu-Bakar, "Watermarking Techniques used in Medical Images: a Survey," in J Digit Imaging, 2014.
2. Kuang LQ, Zhang Y, Han X, "A Medical image authentication system based on reversible digital watermarking, in Information Science and Engineering (ICISE)," in 1st International Conference, 2009.
3. Bhatnagar G, Jonathan WU QM, "Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform," Futur Gener Comput Syst., vol. 29, no. 1, p. 182–195, 2013.
4. Rohit Thanki, Surekha Borra, Vedvyas Dwivedi, Komal Borisagar, "An efficient medical image watermarking scheme based on FDCuT–DCT," Engineering Science and Technology, an International Journal, vol. 20, no. 4, pp. 1366-1379, 2017.
5. K. A. Navas, S. Archana Thampy, and M. Sasikumar, "EPR Hiding in Medical Images for Telemedicine," International Journal of Electronics and Communication Engineering, vol. 2, no. 2, pp. 223-226, 2008.
6. H. Munch, U. Engelmann, A. Schroter, H.P. Meinzer, "The Integration of Medical Images with the Electronic Patient Record and their WebBased Distribution," Academic Radiology, vol. 11, no. 6, pp. 661-668, 2004.
7. Atta Ur Rahman, Kiran Sultan, Dhiaa Musleh, Nahier Aldhafferi, Abdullah Alqahtani, Maqsood Mahmud, "Robust and Fragile Medical Image Watermarking: A Joint Venture of Coding and Chaos Theories," Journal of Healthcare Engineering, 2018.
8. V. S. Jabade and S. R. Gengaje, "Literature review of wavelet," International Journal of Computer Applications, vol. 31, no. 1, pp. 28-35, 2011.
9. W. A. W. Adnan, S. Hitarn, S. Abdul-Karim, and M. R. TamJis, "A review of image watermarking, in Research and Development," Proceedings of Student Conference, 2013.
10. Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle," Journal of Electrical and Computer Engineering, 2012 .
11. Akiyoshi Wakatani, "Digital Watermarking for ROI Medical Images by Using Compressed Signature Image," in Proceedings of the 35th Hawaii International Conference on System Sciences, 2002.
12. Sangeetha Nagarajan, Anita X, Vijayarajan Rajangam , "Medical Image Watermarking: A Review on Wavelet-Based Methods," in Signal and Image Processing Techniques for the Development of Intelligent Healthcare Systems , 2020, pp. 203-221.
13. Upasana Yadav, J.P.Sharma, Dinesh.Sharma, Purnima K Sharma4, "Different Watermarking Techniques & its Applications: A Review," International Journal of Scientific & Engineering Research, vol. 5, no. 4, pp. 1288-1294, 2014.
14. Shilpi Saha, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, "Security on Fragile and Semi-fragile Watermarks Authentication," International Journal of Computer Applications, vol. 3, no. 4, pp. 23-27, 2010.
15. Mahbuba Begum, Mohammad Shorif Uddin, "Digital Image Watermarking Techniques: A Review,"

in information, 2020.

16. Rongsheng Xiea, Chaoqun Honga, Shunzhi Zhua, Dapeng Taob, "Anti-counterfeiting digital watermarking algorithm for printed QR barcode," in Neurocomputing, 2015.
17. Zain JM, Clarke M, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," Int J Comput Sci Netw Secur, vol. 7, no. 9, p. 19–28, 2007.
18. Wu N-I, Hwang M-S, "Data hiding current status and key issues," Int J Netw Secur, vol. 4, no. 1, pp. 1-9, 2007.
19. Chang JD, Chen BH, Tsai CS, "LBP-based fragile watermarking scheme for image tamper detection and recovery," NextGeneration Electronics (ISNE), p. 173–176, 2013.
20. Shu, L., F. Wei, A.C.S. Chung, and Y. Dit-Yan, "Facial expression recognition using advanced local binary patterns, yallis entropies and global appearance features," Image Processing, p. 665–668, 2006.
21. Ni Z, Shi Y-Q, Ansari N, Su W, "Reversible data hiding," IEEE Trans Circ Syst V Technol, vol. 16, no. 3, p. 354–362, 2006.
22. Kaur M, KAUR R, "Reversible watermarking of medical images authentication and recovery-a survey," J Inf Oper Manag, vol. 3, no. 1, pp. 241-244, 2012.
23. Hung-Hsu Tsai, Yu-Jie Jhuang, Yen-Shou Lai, "An SVD-based image watermarking in wavelet domain using SVR and PSO," Applied Soft Computing, vol. 12, no. 8, pp. 2442-2453, 2012.
24. S S Bedi, Ashwani Kumar, and Piyush Kapoor , "Robust Secure SVD Based DCT – DWT Oriented Watermarking Technique for Image Authentication," International Conference on IT to celebrate S. Charmonman's 72nd birthday, pp. 46.1-46.7, 2009.
25. Shinfeng D. Lin, Shih-Chieh Shie, J.Y. Guoa, "Improving the robustness of DCT-based image watermarking against JPEG compression," Computer Standards & Interfaces, vol. 32, no. 1-2, pp. 54-60, 2010.
26. Tanya Koohpayeh Araghi, Azizah BT Abdul Manaf, Mazdak Zamani, Sagheb Kohpayeh Araghi, "A Survey on Digital Image Watermarking Techniques in Spatial and Transform Domains," International Journal of Advances in Image Processing Techniques– IJIPT, vol. 3, no. 1, pp. 6-10, 2016.
27. Ensaf Hussein, Mohamed A. Belal, "Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey," International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 7, pp. 1-8, 2012.
28. Dr. Sanyam Agarwal,Priyanka,Usha Pal, "Different Types of Attack in Image Watermarking including 2D, 3D Images," International Journal of Scientific & Engineering Research,, vol. 6, no. 1, pp. 841-845, 2015.
29. ABDULAZIZ SHEHAB, MOHAMED ELHOSENY, KHAN MUHAMMAD, ARUN KUMAR SANGAIAH, PO YANG, HAOJUN HUANG, GUOLIN HOU, "Secure and Robust Fragile Watermark-ing Scheme for Medical Images," Digital Object Identifier, vol. 6, pp. 10269-10278, 2018.
30. Fatima Abbasi, Nisar Ahmed Memon, "Reversible Watermarking for the Security of Medical Image Databases," in IEEE, 2018.
31. Abhilasha Sharma, Amit Kumar Singh, Satya Prakash Ghrera, "Robust and Secure Multiple Watermarking for Medical Images," Wireless Pers Commun, p. 1611–1624, 2017.
32. [Online]. Available: http://www.bangahospitals.com/mandav_hospital.php..

33. Solihah Gull, Nazir A. Loan, Shabir A. Parah, Javaid A. Sheikh, G. M. Bhat, "An efficient watermarking technique for tamper detection and localization of medical images," in Journal of Ambient Intelligence and Humanized Computing, 2018.
34. "OPENi Medica Image dtabase," [Online]. Available: https://openi.nlm.nih.gov/. [Accessed 15 5 2020].
35. K.J. Kavitha, Priestly B. Shan, "An efficient medical image watermarking technique using integer wavelet transform and quick/fast response codes," International Journal of Intelligent Systems Technologies and Applications, vol. 18, no. 3, pp. 271-280, 2019.
36. Volkan Kaya, Ersin Elbasi, "Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms," in IEEE, 2018.
37. Ram Pratap Singh, Mr Shyam Shankar Dwivedi, "Advanced Medical Image Watermarking Technique of Hiding Patient Information for Medical Image Authentication," International Journal of Engineering and Technical Research (IJETR), vol. 8, no. 5, pp. 22-29, 2018.
38. Yahya AL-Nabhani, Hamid A.Jalab, Ainuddin Wahid, and Rafidah MdNoor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," Journal of King Saud University - Computer and Information Sciences, vol. 27, no. 4, pp. 393-401, 2015.
39. Lamri Laouamer, Muath AlShaikh, Laurent Nana, and Anca Chrisitine Pascu, "Robust watermarking scheme and tamper detection based on threshold versus intensity," Journal of Innovation in Digital Ecosystems, vol. 2, no. 1-2, pp. 1-12, 2015.
40. M.E. Moghaddam, N. Nemati, "A robust color image watermarking technique using modified imperialist competitive algorithm," Forensic Sci. Int, vol. 233, no. 1, pp. 193-200, 2013.
41. S. Nithya, K. Amudha, "Watermarking and Encryption in Medical Image Through Roi-Lossless Compression," in International Conference on Communication and Signal Processing, 2016.
42. Siau-Chuin Liew, Siau-Way Liew and Jasni Mohd Zain, "Reversible Medical Image Watermarking For Tamper Detection And Recovery With Run Length Encoding Compression," World Academy of Science, Engineering and Technology , vol. 4, no. 12, pp. 674-678, 2010.
43. Tjokorda Agung B.W, Adiwijaya, Febri Puguh Permana, "Medical Image Watermarking with Tamper Detection and Recovery Using Reversible Watermarking with LSB Modification and Run Length Encoding (RLE) Compression," in IEEE, 2012.
44. A. K. Singh, "Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image," Multimedia Tools and Applications, 2019.
45. "MedPix™ Medical Image Database," [Online]. Available: https://medpix.nlm.nih.gov/.