Madhu Macker, 2021, 9:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Survey on Medical Image Water Marking Features and Techniques

Phd Scholar Madhu Macker, Associate Prof. Dr. Sunil Phulre
Department of Computer Science and Engineering,
LNCT University, Bhopal, M.P., India.

Abstract- The medical images can easily be manipulated whether knowingly or unknowingly, such acts can take place both inside and outside of the medical system environment. This happen during examine, extracting, transmitting of images. Many reputed organizations have invested a lot in Picture Archiving and Communication Systems so as to achieve greater data security. In this paper detail survey of various approaches adopted or proposed by researcher was summarized. Basic requirement of watermarking algorithm was also detailed in the paper as algorithm should be useful. Popular image features used for watermarking was list as per various scholar proposed work. Embedded image should be robust against some attacks, so list of common image attacks were also mention in paper.

Keywords- Data Hiding, DIP, Information Embedding, Information Extraction, LSB, MSB.

I. INTRODUCTION

With the arrival of computer networks it has made possible to send digital medical image services such as tele-consultation, diagnosis, telemedicine, and radiology across the world. It has helped the patients to get a piece of advice from specialists around the world by sharing their medical history in form of these digital images. But of all such advantages, the security issue of the patient data has become a major issue.

There may be chances that the hackers may hamper the patient's data. So the main motive is to develop some perfect solution to maintain the integrity and authenticity of these medical images. [1, 2]

It is always been difficult to maintain the privacy of patient's medical records. Such medical records are valuable because it holds several crucial data such as clinical diagnosis, treatment, research, education, and other non-commercial and commercial implementations which are required by both government and non-government organizations. DWM or digital watermarking is the process that embeds data within a host signal called to cover in The form of video, audio, or image is the prominent way in multimedia information management [3]. (I) Several attempts have been made to maintain security [5] so that the medical images that are sent on the digital platform cannot be retrieved by any unauthorized parties, (ii) received image have not tampered on the duration of its transfer, (iii) images emerges from the correct source and reach its target destination (authentication).

Such watermarking methods are quite useful for this health care business. They embed the data of the patient with an invisible watermark to secure the data. Such watermarks may include the information of the doctor or something related to the patient's medical data. Such watermarking practices are common in medical images [4].

Digital watermarking is the technique in which data is embedded in any multimedia content electronically. These digital [1] watermarks are used to identify the originality of any image or content. Such watermarks may be in form of images or text [5, 6]. The document is embedded in such images by giving slight alteration to the structure of the image or content like for example inter word spacing or modulation of line width or sometimes modification in character fonts.

© 2021 Madhu Macker. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

The watermark will still be present if the image is passed lossy jpeg compression, low pass filter, or re-sampling. Thus watermarking is a technique to modify the source image slightly to embed any information in the image. It is similar to a digital signature which gives authenticity and ownership to the data [7].

III. RELATED WORK

Usha Verma et. Al. in [8] had shown different digital watermarking methods in both frequency and hybrid domain to obtain better results in medical images. In this process, the host image is called the patient's medical image while the watermark is called the patient's information which is embedded. This embedded information should not be of low quality as it will make the doctor's work difficult and there can be chances of misdiagnosis by them. In this paper LSB, SVD, DCT, DWT techniques, and Hybrid techniques (DWT+SVD) are used in embedding and extracting the embedded watermark.

The performance of this process was checked by PSNR and CRC and SSIM were used to check the robustness of the process. The attack types which were used are rotating, cropping, Gaussian noise, paper, and salt, Poisson, and speckle. Results have shown that DWT provides higher values of PSNR but it is robust for only a limited number of attacks, although it has less value of PSNR than that of DWT. Thus a hybrid technique was used which involves the benefits of both SVD and DWT to get optimal values of PSNR and SSIM and to preserve the integrity and security of medical images effectively.

G. Nagaraju et. al. in [9] this paper has introduced two new processes for encryption of images named DNA Encoding and Spatiotemporal Chaos Algorithm while the hybrid transformation of NSCT, SED, and RDWT for embedding the images in cover images. The study focused on improving the security, robustness, and imperceptibility of medical information without using any physical model which takes time and involves more money, and creates the risk of hacking partners. The theoretical model had demonstrated that this technique is quite successful to achieve the desired goals.

Pooja Prakash. M et. al. in [10] discussed the current medical watermarking techniques for protecting the medical data. The perpetual designing technique was discussed in designing the watermark. The finally designed watermark was embedded in the image in the wavelet domain.

To shape the watermark a perpetual model has been designed. The paper also discussed the degradation of medical images with several types of watermarks. The image quality was also seen with widely used matrices that have been used on different image processing.

The watermark can also be compressed before embedding which can provide additional security to the images and provides resistance to hackers. As a result, it has shown that medical watermarking is an open platform where one can research and select the best watermark from several different watermarks that fits the best in a medical image.

Srivastava Kumar Sumit et. at. Iin [11] This paper proposed to use watermarking techniques and cryptography combined to achieve a secured transmission of the medical data. It uses Elliptic curve DiffieHelman cryptography for encryption purposes and DCT and DWT for watermarking.

Ledya Novamizanti et. al. in [12] used the Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and Fast Discrete Curve let Transforms (FDCuT) methods in the watermarking process. In this process, the medical image of the host was transformed by FDCuT to obtain three sub bands and a high frequency of sub bands was used for DCT and SVD application. The SVD process was also used in the meantime for the watermarking process. The singular value of the watermark was compared with a singular value of the host image. Such insertion of tears by an exchange of the singular value does not degrade the quality of the image.

Xin Zhong et. al. in [13] presented a fragile, high-capacity reversible, and blind watermarking process for watermarking the medical images. The study also showed to used a bottom-up saliency detection algorithm to locate multiple arbitrary shaped regions of interest to generate the different sizes of a square for shape decomposition of non-interest regions iterative square production algorithm was made.
All such processes effectively increase the overall watermarking capacity along with maintaining the quality of the images.

III. WATERMARKING ALGORITHM REQUIREMENT

There are certain legislative rules regarding the security of the medical images that everyone has to follow [6]. Confidentiality, reliability, and availability are the compulsory parameters that have to be followed.

Confidentiality clearly means that only authorized people should access the images.

- Original image
- Manipulated image 6 which has the data access.

Similarly, reliability comes in two aspects) integrity which indicates that the data is not changed ii) Authentication which means the data belongs to the right patient and is sent from the right source. Availability is using of the information from the right or authorized persons. [7]

Some important parameters for designing general watermarking includes-

1. Fidelity:

It means the watermarking of the image should not be visible to humans or there should be no changes in images before and after the watermarking process.

2. Robustness:

It is the ability of an image to bear several processing attacks without getting damaged. These attacks are often done to disturb the watermark for fulfilling the desired operation. Cryptographic attacks, removal, geometric, and protocol [15, 16] are major types of such attacks. Watermarking algorithms are unable to bear all types of attacks. It is not important to put robust watermarking in all applications but essential in some of them [17].

3. Data Payload (or capacity):

It is the concept that accommodates a number of bits that can be hidden in any image without degrading the quality of the image. It is also the factor that how many bits can one embed in any image which can easily be extracted when needed. Such embedding capacity may differ from application to application.

4. Security:

It is the capacity of an image to resist external attacks. The watermarking scheme has to be secured so that any unauthorized person s unable to extract the information without the knowledge of its algorithm. Only an authorized person should be able to extract the watermark. [19]

5. Computational Complexity:

It is the time period required for extracting and embedding the watermark. Some real-time applications are fast but it needs some time in using complex algorithms when a high level of security is required.

6. Perceptibility:

It shows the amount of degradation that happens to any image while embedding the watermark. It is good to keep this parameter lowest as possible in such an invisible watermarking scheme[13]

7. Imperceptibility:

Means invisibility which is required in such watermarking schemes. This feature says that the original and watermarking image should be similar [20] and one can achieve it by reducing capacity or robustness or both. [19].

Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) index [13] is the standard benchmark to measure the imperceptibility of any image.

8. Reversibility:

If an image is changed during the workflow process such an image is not trusted in the medical field. Such images are not considered valid images and lead to misdiagnosis which can be dangerous to the lives of the patient. So it is necessary to retrieve the original data from the watermark image without any problem [21].

Lossless and reversible methods can solve this problem as they guarantee the robustness of the image and defines the capacity of the watermark to keep the image original or unmodified.

But in reversible techniques image watermarking is not distortion-free and so the modified image is used as the cover which carries the watermark which is not intended to use for diagnostic purpose and is used for extraction purpose only.

V. FEATURE FOR IMAGE WATERMARKING

1. Discrete Wavelet Transform (DWT):
It divides the image into 4 parts:

- **HH:** Diagonal details coefficients matrix
- **HL:** Horizontal details coefficients matrix
- **LH:** Vertical details coefficients matrix
- **LL:** Approximation coefficients matrix.

The LL sub-band can be obtained after applying a low pass filter to filter the rows and columns to obtain a rough explanation of the image. The HH sub band uses a high pass filter in both directions which has high-frequency components in the diagonal region.

The HL and LH are obtained by applying a low pass filter from one side and high pass from the other side. The image is processed by wavelet transform after this. The LL image determines most of the information of the host image. While LH contains the vertical detail corresponding to horizontal edges. And HL determines the horizontal detail from vertical edges.

2. Color Feature:
The intensity value of any image represents the kind of color of the picture. One has to use a low computation cost method to determine the color of the object. Several images have different types of color which can be identified through standard RGB (red, green, blue). It is the representation of the two-dimensional image. In the third dimension which is the collection of the matrix.

To calculate, the intensity of the picture gray format is used which is in two dimensions ranging from 0 to 255. It is 0 and 1 in the case of black and white photos. With this method, one can effectively determine the color of any image. [8]

3. Edge Image:
As the image is a collection of intensity values and sudden changes in it introduce the edge feature. Figure4. This feature uses different types of features to detect the types of image and object detection in roads, scenes, etc [5]. Sobel, canny, and per with h are such algorithms that detect that point out the difference in the image. Out of them canny was found the best for edge detection or finding the boundaries in the image.

4. Texture Feature:
Determine the difference in texture quality of any image such as smoothness and regularity. [1] Texture requires a step-by-step process, unlike the color determination process. The texture feature is similar to the edge feature and is less sensitive than the color feature.

5. Histogram Feature:
In this, the image vector is found out after pre-processing the image to find the bins. It can be considered as a let scale of the color in fig 4.2 ranging from 1 to 10. So as per this Hi= [0, 0, 0, 4, 3, 5, 2, 1 2, 0] in which the I represents the position in the H matrix together with the color value and H is the color pixel value.

VI. ATTACK ON IMAGE

There are many types of attack which are done in data hiding video. The reason behind this is to check how much difficult to extract the data from the source. These are all the precautions taken before sending the data to the digital media.

1. Noise Attack:
As the video is passed into the secret channel some sort of noise is generated into the channel to see whether it hampers the integrity and security of the video. Types of noise are Gaussian nice attack, Salt and Pepper Noise, Speckle noise attack, and many more.

2. Filter Attack:
In this attack, the video is passed through different types of filters and the process is done after receiving the signals from the network. The video cryptography and the embedding and extraction algorithm should be robust for this. Some popular types of filtering attacks are median filter, sharpen filter, motion filter, etc.

3. Compression Attack:
Here are video is passed through several compression techniques which are normally done after signal reception from the network. The embed and extraction algorithm should be robust to save the video from such types of attack. Some popular filtering attacks are MPEG compression, MP4 compression, etc.

4. Detection-Disabling Attack:

In this to check the security of the data the secret message is detection is done by changing its correlation to make it impossible to extract the secret message from the received data. This type of attack fails when the rotation of scaling is done on the secret message because the secret message does not share the same spatial pattern.

In many cases, they perform some types of geometric distortion such as cropping or pixel permutation, the shift in the temporal direction, rotation, zooming, or insertion.

5. Ambiguity Attacks:

Here there is the introduction of several fake messages to confuse the detector with the actual message. This is done to discredit the authority of the original secret message several watermarks are embedded.

Privacy of any image or secret message is the inclusion of a third party that develops a compressive sensing matrix. In this type of matrix, some types of pixels are selected. Now, these selected pixels are analyzed based on a secret message. If it is found that these pixels match with the message then it is selected for embedding otherwise rejected. Now on the extraction side, the image is evaluated under some calculation and is accepted or rejected based on the obtained values. Here the work has not taken any measures on attacks.

VI. CONCLUSIONS

The main motive of this research work is to study different types of watermarking techniques. There are many types of watermarking algorithm which can be applied to the medical image. Such an algorithm provides data integrity, recovering the original image without degrading it, the confidentiality of medical data, and helps inefficient data management.

It was found that frequency domain embedding has better outcomes as compared to spatial domain model. Paper has summarized attacks on embedded watermark image and it was found that spatial attacks are most destructive attack as watermark extraction from that image was tough.

In future image was scholar can proposed a more robust algorithm that can extract watermark under different attack environment.

REFERENCES

[1] Pawe Korus, Student Member, IEEE, and Andrzej Dziech. “Efficient Method for Content Reconstruction with Self-Embedding”. IEEE Transactions On Image Processing, Vol. 22, No. 3 March 2013.

[2] Hanieh Khalilian, Student Member, IEEE, And Ivan V. Bajic Video “Watermarking With Empirical PCA-Based Decoding” IEEE Transactions On Image Processing, Vol. 22, No. 12, December 2013.

[3] S. Huang, W. Zhang, W. Feng and H. Yang, Blind watermarking scheme based on neural network, Proceedings of the 7th IEEE World Congress on Intelligent Control and Automation (2008), 5985–5989.

[4] H. Peng, J. Wang and W. Wang, Image watermarking method in multi wavelet domain based on support vector machines, Journal of Systems and Software 83(8) (2010), 1470–1477.

[5] H.Y. Yang, X.Y. Wang and C.P. Wang, A robust digital watermarking algorithm in undecimated discrete wavelet transform domain, Computers and Electrical Engineering 39(3) (2013), 893–906.

[6] MohiulIslama,∗, Amarjit Royb and Rabul Hussain Laskar. “Neural network based robust image watermarking technique in LWT domain”. Journal of Intelligent & Fuzzy Systems 34 (2018) 1691–1700.

[7] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Md. Abdur Rahman, AtifAlamri, B. B. Gupta. “Efficient quantum information hiding for remote medical image sharing”. Digital Object Identifier 10.1109/ACCESS.2017.

[8] Usha Verma, Neelam Sharma. "Hybrid Mode of Medical Image Watermarking To Enhance Robustness and Imperceptibility". International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-1, November 2019.

[9] G. Nagaraju, P. Pardhasaradi, V. S. Ghali, G.R.K Prasad. "Secure Hybrid Watermarking Technique in Medical Imaging". European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 07, Issue 05, 2020.

[10] Pooja Prakash.M, Sreeraj.R, Fepslin AthishMon, K. Suthendran. "Combined Cryptography And

Digital watermarking For Secure Transmission of Medical Images in EHR Systems". International Journal of Pure and Applied Mathematics, Volume 118 No. 8 2018, 265-269.

[11] Srivastava Kumar Sumit, Pandey Harikesh. "Medical Image Watermarking with Patient Details as Watermark". International Journal of Advance research, Ideas and Innovations in Technology, Volume2, Issue6, 2016.

[12] Ledya Novamizanti, Ida Wahidah, Ni Putu Dhea Prameiswari Wardana. "A Robust Medical Images Watermarking Using FDCuT-DCT-SVD". International Journal of Intelligent Engineering and Systems, Vol.13, No.6, 2020.

[13] Xin Zhong and Frank Y. Shih. "A High-Capacity Reversible Watermarking Scheme Based on Shape Decomposition for Medical Images". International Journal of Pattern Recognition and Artificial Intelligence Vol. 33, No. 01, 2019.

[14] C. Fung, A. Gortan, and W. G. Junior, "A review study on image digital watermarking," in The Tenth International Conference on Networks, 2011, pp. 24-28.

[15] R. Ridzoň, D. Levický, and Z. Klenovičová, "Attacks on watermarks and adjusting PSNR for watermarks application," in Radioelektronika 2004: 14th international Czech-Slovak scientific conference, 2004, pp. 27-28.

[16] S. Voloshynovskiy, S. Pereira, V. Iquise, and T. Pun, "Attack modelling: towards a second generation watermarking benchmark," Signal processing, vol. 81, pp. 1177-1214, 2001.

[17] M. Durvey and D. Satyarthi, "A review paper on digital watermarking," International Journal of Emerging Trends & Technology in Computer Science, vol. 3, pp. 99-105, 2014.

[18] P. Arya, D. S. Tomar, and D. Dubey, "A Review on Different Digital Watermarking Techniques," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 8, pp. 129- 136, 2015.

[19] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, "Properties of digital image watermarking," in Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on, 2013, pp. 235-240.

[20] R. Patel and P. Bhatt, "A Review Paper on Digital Watermarking and its Techniques," International Journal of Computer Applications, vol. 110, pp. 10-13, 2015.

[21] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," Information sciences, vol. 279, pp. 251-272, 2014.