

A Survey on Healthcare Image Steganography Techniques and Features

Ph.d. Scholar Arun Kumar Sonaniya, Prof. Laxmi Singh

Dept. of Electronics & Communication
RNTU,MP, India

Abstract- One of important part of human life is health and some of information storage provide such valuable data. In order to increase the trust on such type of stored data steganography technique was applied by various researchers. This paper has summarized the features of image processing and its application in different areas. This paper has detailed various models proposed by scholars of image steganography processing. It was obtained that image may undergo some set of attacks that may disturb geometrical and spatial information, so list of such attacks was also summarized in the paper. Some of algorithm measuring parameters were also mentioned in the paper.

Keywords- Image Processing, Stenography, Feature Extraction, Data hiding.

I. INTRODUCTION

The practice of putting information into another media for safe transfer is known as information hiding. Copyright enforcement, tamper detection, and concealed data transfer are just a few of the features [23].

Information hiding techniques can be split into three categories based on the goals for which they are used: cryptography, watermarking, and steganography. These are technologies that are commonly used to secure data security, authentication, and privacy (hiding), particularly when data is transmitted over a public network [1–5].

The message is encrypted in cryptography in such a way that it becomes unreadable. In watermarking, the message watermark (text, image) is embedded in the host data (image/file) in such a way that the host stays undetectable and can be validated later, whereas in steganography, the message is embedded in a host without attracting the user's attention. Intruders may be put off by the transmission of an encrypted message, but this is not the case with a stego or watermarked message in a cover signal. However, combining these methods can provide more protection [1].

Unlike encryption, steganography and watermarking take advantage of human audiovisual systems' (HAVS) perceptual deficiencies, which fail to distinguish between original and watermarked/stego-signals [6]. Watermarking approaches are used to validate the identification and validity of the digital image holders by inserting distinct material such as a signature into the host medium [24].

Steganography is the practise of hiding the presence of a hidden message inside other media, such as text, image, audio, and video, without causing unintended awareness

and at the same time achieving a high entrenching potential [21].

The payload or amount of hidden message in relation to the size of the cover image determines the steganalysis method's ability. As a result, this fact imposes an upper bound on the amount of information that can be embedded. If the hidden data is smaller than the upper bound, the carrier is safe and known statistical analysis tools cannot identify it. As a result, the main challenge in steganographic techniques is a compromise between the hiding payload of a cover picture and the detectability and, as a result, quality of a stego-image.

The steganography trinity's different impacting characteristics are capacity, security, and resilience, and they are constantly at odds with one another. The quantity of information that can be hidden in the cover image is referred to as capacity. When compared to its original counterpart, a steganographed medical image should attain the highest clinical reading clarity with the smallest perceived change.

II. RELATED WORK

Jung [7] suggested obfuscating the structure with large size files. In order to increase entrenching competence, the recommended structure uses component rate distinguishing together with smallest significant part substitution in the consistent item level. The empirical results showed that once the entrenching competency reached 1,052,641 pieces, the proposed structure maintained 32.61 dB on moderate. As a result, in the absence of misrepresentation to the lethal optical technology, the advised structure assured sturdiness backed by entrenching competence.

For optimal counting-based secret exchange, **Gutub and Al-Ghamdi [8]** proposed multimedia image

steganography. To save the optimised shares that provide comparisons for proofed remarks, the authors used multimedia image-based steganography approaches. To verify that true differences within the security analysis, the study experiments test the function of the improvements by assuming various hidden shared key sizes of 64-bit, 128-bit, and 256-bit. Experimenting with five alternative image-based steganography approaches to embed each created sharing improved the usability of the shares even more. The findings had a significant tempting effect, making the streamlined counting-based secret sharing method a potential approach for multi-user authentication security applications.

For improvement of the previous technique (Jain and Lenka in Springer Brain Inform 3:39–51, 2016), [9] proposed an improved diagonal queue medical image steganography for patient secret medical data transmission using a chaotic standard map, linear feedback shift register, and Rabin cryptosystem (Jain and Lenka in Springer Brain Inform 3:39–51, 2016). Generation of pseudo-random sequences (pseudo-random sequences are generated by linear feedback shift register and standard chaotic map), permutation and XORing using pseudo-random sequences, encryption using Rabin cryptosystem, and steganography using improved diagonal queues are the four stages of the proposed algorithm.

In [10] the research focus in this work is on maintaining the confidentiality and integrity of medical images. Encryption, in general, can provide integrity and confidentiality (a piece of cryptography). Steganography is used to add another layer of security to the medical image. The medical image is encrypted using a one-time pad encryption scheme in this paper, and the encrypted image is then implanted into a cover image to create a stego image, making the system more resistive to the attacker.

[11] Is an example. The cryptanalysis of a novel proposed colour picture encryption technique employing RT-enhanced chaotic tent map is performed in this study (CTM). The corresponding keys of the cryptosystem are successfully broken using chosen-plaintext attacks, allowing the target ciphertext picture to be decrypted. We then presented an improved encryption scheme based on the cryptanalysis. A new Logistic-tent map (LTM) is suggested and used to the enhanced encryption technique, and a secret key parameter based on the plaintext image's SHA-3 hash value is introduced to make the improved algorithm resistant against chosen-plaintext assaults.

[12] Proposes a quantum steganography approach for concealing a quantum secret image within a quantum cover image. To show the security of the embedded data, the quantum secret image is first encrypted using a controlled-"NOT" gate. Using the two most and least significant qubits, the encrypted secret image is integrated into the quantum cover image. In addition, a quantum image

watermarking method for hiding a quantum watermark grey image in a quantum carrier image is described. Arnold's cat map is used to scramble the quantum watermark image, which is then incorporated into the quantum carrier image using the two least and most significant qubits. To extract the encoded quantum watermark image, you only need the watermarked image and the key. A scenario of sharing medical imaging between two remote institutions has been used to demonstrate the intended uniqueness.

III. STENOGRAPHY ALGORITHM REQUIREMENT

Everyone is required to obey certain legislative regulations regarding the protection of medical images [6]. The mandatory parameters to be followed are confidentiality, reliability, and availability. Only authorised personnel should have access to the photographs, according to confidentiality. Original image (a) and altered image 6 with data access (b). Similarly, there are two elements to reliability: integrity, which means that the data has not been altered, and trustworthiness, which means that the data has not been tampered with. ii) Authentication, which ensures that the data is sent from the correct source and belongs to the correct patient. The term "availability" refers to the use of information obtained from the appropriate or permitted sources. [7]

The following are some significant parameters to consider while creating universal watermarking:

- Fidelity: This refers to the fact that the image's watermarking should not be apparent to humans, and that images should not alter before or after the watermarking procedure.
- Robustness refers to an image's capacity to withstand multiple processing attacks without being harmed. These assaults are frequently carried out in order to disrupt the watermark in order to complete the intended activity. Cryptographic attacks, removal attacks, geometric attacks, and protocol assaults are all examples of such attacks [15, 16]. Watermarking algorithms can't withstand all kinds of attacks. Although robust watermarking is not required in all applications, it is required in certain of them[17].
- Data Payload (or Capacity) is a notion that allows a number of bits to be buried in any image without compromising the image's quality. It's also a consideration of how many bits can be stored in a picture and simply removed when needed. The capacity for embedding may vary depending on the application.
- Security refers to an image's ability to withstand external threats. The watermarking system must be safe enough that any unauthorised individual who does not know the algorithm will be unable to extract the information. Only a trusted individual should be able to remove the watermark. [19]
- Computational Complexity: This refers to the amount

of time it takes to extract and embed the watermark. Some real-time applications are quick, but when a high level of security is required, it takes some time to use complicated algorithms.

- **Perceptibility:** This parameter indicates how much of an image is degraded when the watermark is embedded. In an invisible watermarking technique, it's best to maintain this parameter as low as feasible. [13]
- **Imperceptibility:** This phrase refers to the invisibility necessary in such watermarking systems. This feature specifies that the original and watermarked images should be similar [20], which can be accomplished by lowering capacity, robustness, or both. [19]. The basic benchmark for measuring the imperceptibility of any image is the Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) index [13].
- **Reversibility:** In the medical field, an image that has been modified during the workflow process is not trusted. Such photos are not deemed legitimate and can lead to misdiagnosis, which can put the patient's life in jeopardy. As a result, it is important to easily retrieve the original data from the watermark image [21]. Lossless and reversible approaches can tackle this problem since they ensure the image's robustness and define the watermark's capacity to maintain the image original or unaltered. However, image watermarking is not distortion-free in reversible procedures, thus the modified picture is used as the cover with the watermark, which is not intended to be used for diagnostic purposes and is only utilised for extraction purposes.

IV. FEATURE FOR IMAGE PROCESSING

1. Features for Data Hiding:

1.1 Color feature: Image is a matrix of light intensity values, these intensity values represent different kind of color. so to identify an object colour is an important feature, one important property of this feature is low computation cost .

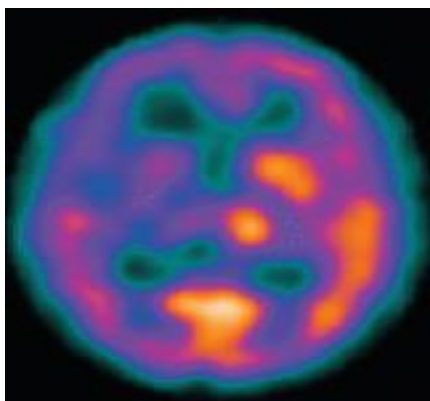


Fig 1. Represent the HSV (Hue Saturation value) format of an image.

Different Image files available in different color formats like images have different color format ranging from RGB which stand for red, green, and blue. This is a three dimensional representation of a single image in which two dimensional matrix represent single color and collection of those matrix tends to third dimension. In order to make intensity calculation for each pixel gray format is use, which is a two dimension values range from 0 to 255. In case of binary format which is a black and white color matrix whose values are only 0 or 1. With the help of this color feature face has been detected efficiently in [8].

1.2 Edge Feature: As image is a collection of intensity values, and with the sudden change in the values of an image one important feature arises as the Edge as shown in figure 4. This feature is use for different type of image object detection such as building on a scene, roads, etc [5]. There are many algorithm has been developed to effectively point out all the images of the image or frames which are Sobel, perwitt, canny, etc. out of these algorithms canny edge detection is one of the best algorithm to find all possible boundaries of an images.

1.3 Texture Feature: Texture is a degree of intensity difference of a surface which enumerates properties such as regularity and smoothness [1]. Compared to color space model, texture requires a processing step. The texture features on the basis of color are less sensitive to illumination changes as same as to edge features.

1.4 Histogram Feature: In this step image vector obtained after pre-processing is used where histogram of the image is finding at one bin. This can be understood as let scale of color in fig. 4.2 is 1 to 10, than count of each pixel value is done in the image. So as per above vector $H_i = [0, 0, 0, 4, 3, 5, 2, 1, 2, 0]$ where H represent the color pixel value count and i represent the position in the H matrix with color value.

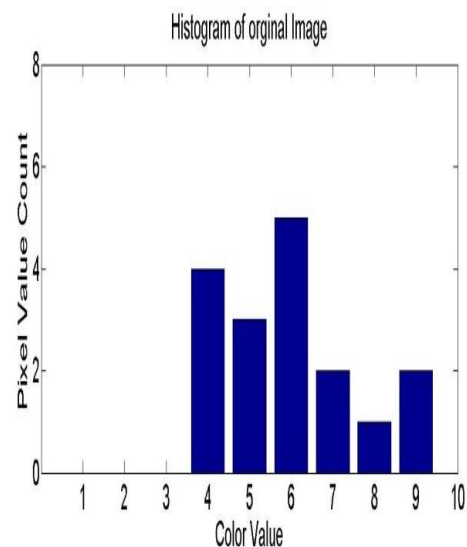


Fig 2. Histogram of the original image.

1.5 Corner Feature: In order to stabilize the video frames in case of moving camera it require the difference between the two frames which are point out by the corner feature in the image or frame. So by finding the corner position of the two frames one can detect resize the window in original view. This feature is also use to find the angles as well as the distance between the object of the two different frames. As they represent point in the image so it is use to track the target object.

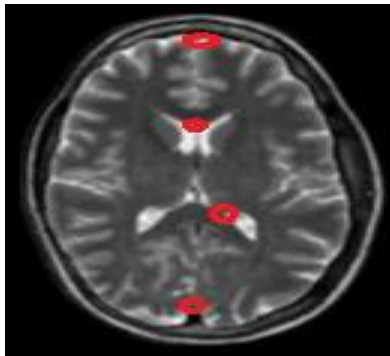


Fig 3. Represent the corner feature of an image with green point.

2. DWT (Discrete Wavelet Transform):

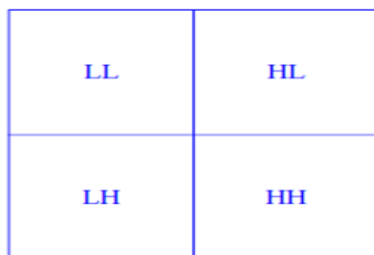


Fig. 3.11 DWT of image from [8].

- 2.1 LL:** In fig. 3 upper left part is term as LL block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain flat region of the image which do not have any edge information, so this is term as approximate version of the image.
- 2.2 HL:** In fig. 3 upper right part is term as HL block. This block of image is obtain by filtering the image rows from the high pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain horizontal edge region of the image which do not have any flat information.
- 2.3 LH:** In fig. 3 lower left part is term as LH block. This block of image is obtain by filtering the image rows from the low pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain vertical edge region of the image which do not have any flat information.
- 2.4 HH:** In fig. 3 lower right part is term as HH block. This block of image is obtain by filtering the image

rows from the high pass filter then pass same to the high pass filter but here column are filter for the analysis. This block contain diagonal edge region of the image which do not have any flat information.

V. ATTACK ON IMAGE

In data hiding video, there are many different sorts of attacks. The purpose of this is to see how tough it is to extract data from the source. All of these measures were done prior to delivering data to digital media.

1. Noise Attack:

As the video is transferred into the secret channel, some noise is generated to see if it interferes with the video's integrity and security. Gaussian pleasant attack, Salt and Pepper Noise, Speckle noise attack, and many others are examples of noise types.

2. Filter Attack:

In this attack, the video is run through several sorts of filters after the signals from the network are received. For this, the video cryptography, as well as the embedding and extraction algorithms, should be resilient. Median filter, sharpen filter, motion filter, and other filtering attacks are common.

3. Compression attack:

Here, the video is compressed using a variety of techniques that are generally used after the signal is received from the network. To protect the video from such attacks, the embed and extraction algorithms should be robust. MPEG compression, MP4 compression, and other filtering attacks are common.

4. Detection-disabling attack:

To verify the data's security, the secret message is detected by altering its correlation, making it impossible to extract the secret message from the received data. This form of attack fails when the secret message is rotated because the secret message does not have the same spatial pattern as the secret message. They frequently perform geometric distortions such as cropping or pixel permutation, temporal shift, rotation, zooming, or insertion.

5. Ambiguity Attacks:

Here, many bogus messages are introduced to confuse the detector with the true message. Several watermarks are implanted to discredit the authority of the original secret message.

The participation of a third party who produces a compressive sensing matrix ensures the privacy of any image or secret message. Some types of pixels are chosen in this type of matrix. These selected pixels are now being evaluated using a hidden message. If these pixels match the message, the message is chosen for embedding; otherwise, it is refused. On the extraction side, the image is analysed

using some calculations, and the results are accepted or rejected based on the results. The work has not taken any counter-attack measures in this area.

VI. CONCLUSIONS

The main motive of this research work is to study different types of steganography approaches adopted and proposed by various scholars of image processing. Objective of each technique is to maintain the integrity of secret healthcare data. As communication environment goes under different steps that may harm the original information so such list of attacks were also detailed in the paper.

In this paper it was obtained that steganography technique with reversible approach is less efficient. In paper image feature were discussed as most of application have different feature set as per input image format. In future scholar can propose a model that can safely extract embedded information and cover file.

REFERENCES

- [1] Mohiul Islama, Amarjit Roy b and Rabul Hussain Laskar. "Neural network based robust image watermarking technique in LWT domain". *Journal of Intelligent & Fuzzy Systems* 34 (2018) 1691–1700.
- [2] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Md. Abdur Rahman, Atif Alamri, B. B. Gupta. "Efficient quantum information hiding for remote medical image sharing". *Digital Object Identifier* 10.1109/ACCESS.2017.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 7951–7985, 2020.
- [8] K.-H. Jung, "Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 127–136, 2018.
- [9] Jain M, Lenka SK (2016) Diagonal queue medical image steganography with rabin cryptosystem. *Springer Brain Inform* 3(1):39–51.
- [10] P. A, U. R, J. N and P. S, "Securing Medical Images using Encryption and LSB Steganography," 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), 2021.
- [11] Congxu Zhu, And Kehui Sun. "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps". *IEEE Access* Volume 6, 2169-3536, 2018.
- [12] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, M. Shamim Hossain, Md. Abdur Rahman, Atif Alamri, B. B. Gupta. "Efficient quantum information hiding for remote medical image sharing". *Digital Object Identifier* 10.1109/ACCESS.2017.
- [13] Ledy 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.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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.