ISSN No:-2456-2165

Steganography Techniques for Medical Images: A Recommender Paper

[.1]Inam Ul Haq, [2]Ahmad Ali, [3]Bilal Shabbir Qaisar, [4]Hafiz Muhammad Adnan, [5]Mubasher Hussain, [6]Muhammad Nauman
[1,2,3,4,5,6] Faculty of Computing University of Okara 56300, Pakistan
[3,5] MLC Lab University of Okara, Pakistan

Abstract:- Communication always needs privacy and security for many reasons and hence it increases the need for securing the secret message. Image steganography is the process of concealing secret media within any format of the transmitter. In image steganography, a cover image is used in both the embedding and extracting processes. Through a systematic literature review, we have an analyzed mage steganography technique. We also have presented advantages and weaknesses along with some applications i.e., LSB, PNSR, DWT, 3D images steganography. The main challenges of image steganography in spatial and transform domains are presented. In the end, findings for future scope are also presented.

Keywords:- *Data Hiding, Encryption, Image, Steganography, Stego-File*

I. INTRODUCTION

Traditionally, "steganography" conceals a secret message in another message. For example, a personal statement in computing can be a file, text, image, audio, or video hidden within another file, text, image, audio, or video. Steganography originates from the Greek word steganographia, which combines steganos, "covered or concealed," and graphia, meaning "writing."

The supremacy of steganography over the method cryptography is very clear as the secret information is not meant to attract hacker attention like an encrypted message in cryptography. Hence, the plaintext is visible in cryptography, even when encrypted, no matter how unbreakable. Below is the block diagram of the generic process of Image Steganography.

Figure 1 shows the original image as a cover image that serves as a hidden information carrier. The secret message is the information to be hidden, and the stego image is the source image in which the message is successfully embedded using the stego key algorithm.

Steganography incorporates steganographic coding within a media picture, as media images are perfect for transmission because of their huge size. Usually, a sender selects picture media and modifies the color of each hundredth pixel compared within the pixel set. This alter is so subtle that somebody who is not particularly trying to find it is impossible to detect this modification.

The basic motivation of writing this paper is to present the image steganography techniques and related material in a more generalized way so that different useful utilization may be achieved. For this, following research questions have been formulated. RQ1; what peculiar cutting-edge steganography techniques are related to medical image. RQ2; presenting the usefulness of different image steganography techniques. RQ3; investigating potential applications and challenges of medical image steganography techniques. As a result, the primary goal of this paper is to provide a general understanding of what image steganography techniques have accomplished in medical information concealment and what potential challenges exist in medical image steganography.

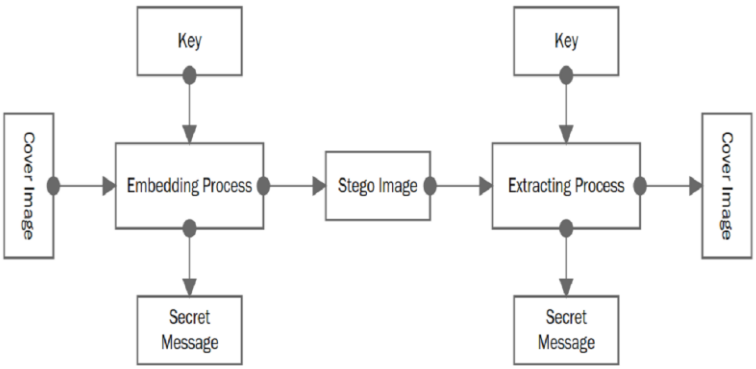

Fig. 1: Block Diagram of Generic Process of Image Steganography

ISSN No:-2456-2165

II. SHORT HISTORY

History records have revealed the existence of steganography. The recorded events can be traced to ancient Greece. "When Herodotus narrated two examples in his Stories, but the first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book about magic. Initially, the author decided not to print it and even destroyed large parts of it, believing that they should never have seen the light of day, but the text continued to circulate in the form of a provisional draft and was published posthumously in 1606". Afterward, people have utilized steganography in various styles and shapes to deliver messages safely throughout history. Spies have used garments and fabric to hide secret messages.

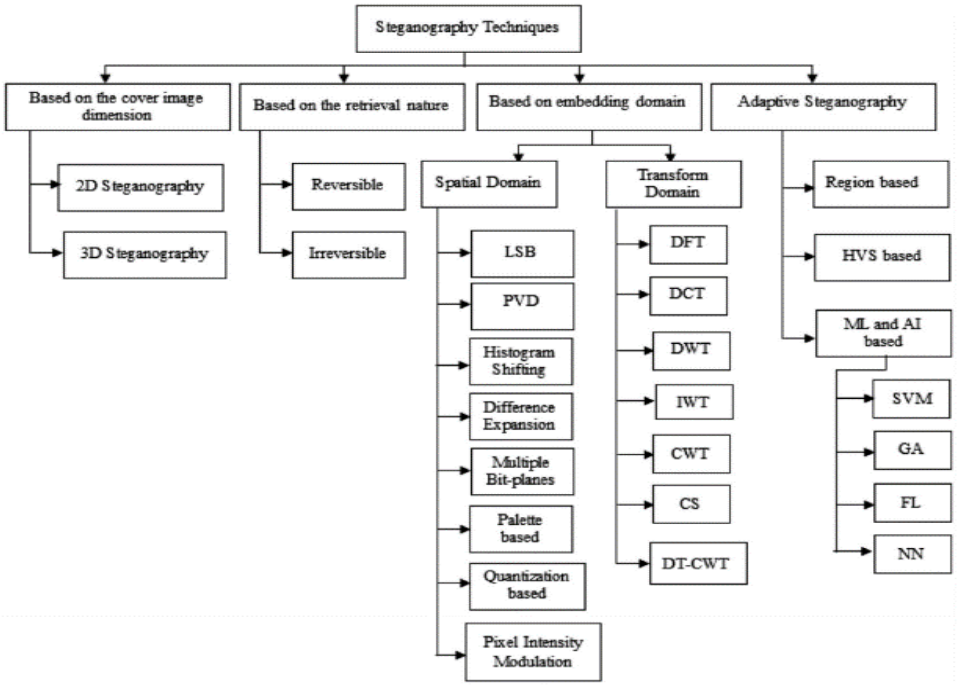

Fig. 2: Categories of Image Steganography Techniques [1]

The Figure 2 presents the categories of image steganography techniques. Particularly, the spatial and transform domains have been discussed. Mainly the techniques related to LSB, PVD, Difference expansion, Pixel Intensity Modulation, Morphology, DFT, DCT, DWT are discussed.

Some of the main challenges in image steganography are described here. The Least Significant Bit technique is widely used but it provides poor defense against geometrical, compression, and statistical attacks. Hence it lacks security requirements. In transform domain technique of image steganography, a few change space strategies do not appear subordinate to the picture organize and they may have beaten lossless and lossy organized changes. Another issue in discrete cosine transform is that it has less embedding capacity, security and robustness against attacks. In JPEG steganography, because redundant bits are eliminated in JPEG, any hidden data would be lost. Many distortions-based techniques are also used in image steganography and it does not seem useful, as the receiver must have access to the original cover media. Many other challenges have also been presented under Challenges section.

The structure of this research paper is as follows: Section 1 is Introduction, Section 2 is Steganography Techniques, Section 3 is about Applications, Section 4 is Challenges, Section 5 is Findings for Future Scope and Section 6 is Image Steganography Techniques.

III. LITERATURE REVIEW

All this data has been gathered through the systematic literature review process and a pictorial representation is given in the Figure 3. Most of the research papers are retrieved from journal articles through Google Scholar and ResearchGate since 2018. In the initial search query, nearly 17,700 results are found of which 241 are not related. It is also to note that only very few articles were selected after strict exclusion and inclusion criteria. A pictorial or schematic representation of systematic literature review (SLR) is presented in the Figure 3.

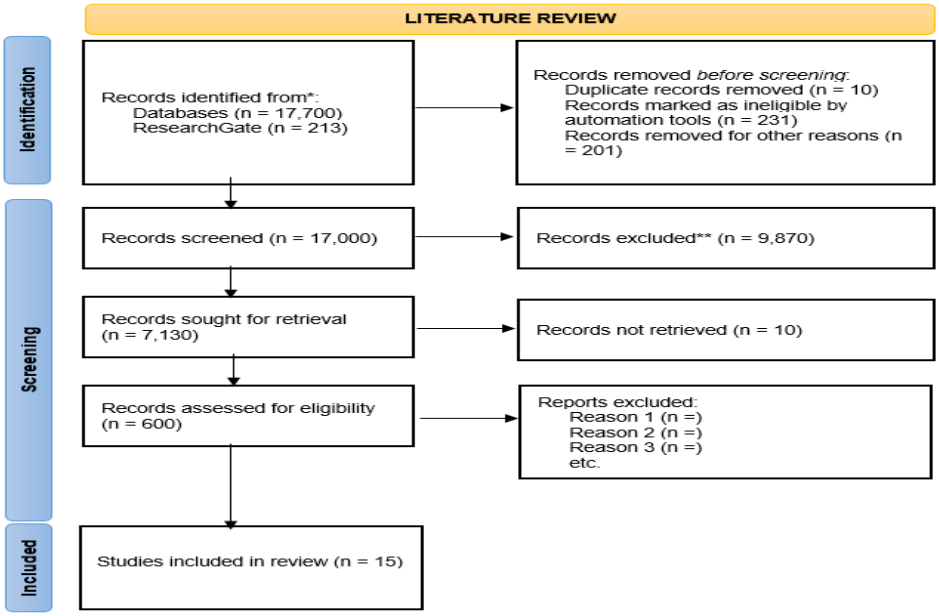

Fig. 3: Systematic Literature Review Process

*Google Scholar, Scopus, Compendex, and ResearchGate. **Not Related

Details of Table 1 are provided below. In cryptography, they used their proposed encryption algorithm known as MJEA (Modified Jamal Encryption Algorithm). MJEA is an asymmetrical cipher algorithm based on 64-bit block cipher with a 120-bit key. In steganography, they used a simple technique that masks patient content by bit-by-bit XOR. Prior to transmitting, they blended with a scrambling algorithm. They also adopted various simulation measurements such as (PSNR), (MSE), and histogram distribution analysis to evaluate MJEA's performance. All experimental results have demonstrated the strength of MJEA.[2].

A comprehensive review of what LSB-based steganography techniques have accomplished in medical images has been presented. If the cover image is modified, it fails in achieving the goal of telemedicine. Therefore, they proposed that encrypting the information before hiding provides an extra security level. This is the main requirement of security in (DICOM). Moreover, they provided comprehensive state-of-the-art achievements and weaknesses of image steganography on medical data [3].

Hackers are constantly trying to attack information in transit in an insecure network. As a result, they presented a novel approach to medical image encryption based on cyclic coding. In the chosen ciphertext attack, they successfully tested decrypting the original content from encoded data. They also demonstrated the efficiency of encryption using correlation coefficients to encode multiple medical images efficiently[4].

Designing an efficient image steganographic system is facing many challenges including imperceptibility, low capacity, and less robustness. To address these issues, a novel and secure Pixels Contrast technique, as well as the eight neighbor's method and the Huffman coding algorithm, are proposed. The results were evaluated based on different parameters such as Histogram Analysis Structural Similarity Index (SSIM) and PSNR etc [5].

For authentication difficulties, they presented a modified LSB approach for simultaneously securing and disguising medical data. This image steganography method employs a logical bit shift operation and is implemented in *MATLAB* version 2018a. The results of the proposed method show that the modified DSL image steganography surpasses the standard DSL methodology, with higher PNRs and lower MSE.

The results suggest that the proposed method may successfully obtain medical information without leaving a false stego image. [6].

They have successfully presented a stego-hiding scheme for a medical image using a unique nuclear spin generator system. A detailed literature review comprising theoretical, as well as experimental analysis, has been provided. They have used PSNR, histogram analysis, statistical package analysis, and key space calculation in their proposed algorithm. The results show comparatively better performance of the new medical image steganography technique [7].

This short paper presents a comparative analysis of 10 different Steganography techniques for data (image, text, audio, video, etc.) for image security. These techniques include LSB, DCT, LSB Genetic Algorithm, IMNP, DE, EMD, and random function few of them [8].

They have proposed an encryption technique in which the high-capacity data was encrypted using the DNA encoding technique. Afterward, it is reduced by lossless compression. The medical images were segmented into the background, GM, WM, and tumor by a single level DWT

using k-means and db4 filter. The message is hidden in the labeled tumor image's non-tumor region[9].

The researchers highlighted that while evaluating medical image Steganography algorithms, the specific predictors related to machine-based auto-diagnosis and teleradiology in medicine are not given consideration. This automated diagnosis was evaluated using SVM image classification of Chest X Rays Scan of controlled and Pneumonia patients[11].

It is essential for digital watermarking that accurate and unmodified recovery of the embedded watermark must be guaranteed. In this research, a temper detection method is introduced named "*Constant Correlation Spread Spectrum (CCSS)*" for medical images. In the CCSS method, a bit is used to watermark the patient record and that is distributed in the medical image sub-block for all watermarked sub-blocks [12].

Table 1: Various Image steganography Techniques

Authors	Technique	Usefulness
JNB Salameh et al. [2]	Modified Jamal Encryption Algorithm	The proposed MJEA can recover original medical images at the receiver side successfully
BA Shtayt et al.[3]	SLR on Steganography of Medical Images	A comprehensive comparison for benefits and weaknesses of medical images based on the LSB Techniques has been presented
B Bose et al.[4]	Novel Technique using Cyclic Coding	They have successfully proved to decipher the original content from encrypted data in chosen cipher text attack
MM Hashim et al.[5]	Pixel Contrast Method	Different values of PSNR for the image are obtained using three kinds of embeddings with different EP
RO Ogundokun et al.[6]	Modified LSB Technique	The proposed method has the potential to get medical-related information successfully without a perceptible falsification in the stego-image
B Stoyanov et al.[7]	Innovative algorithm for the output of pseudo-random bytes using the nuclear spiner.	Results show better performance of proposed medical image steganography scheme
A Tiwari et al.[8]	A Comparative Analysis	A great number of analysts have proposed solutions for the security issue; but still cannot provide total security
R KARAKIŞ et al.[9]	Morphology, (DWT), k-means Algorithms	The proposed technique unites all the high-capacity data of the patients into a single file hence increasing the security and recording space of medical data
P Eze et al.[10]	Support Vector Machine	The proposed technique is helpful in the automated diagnostic through a steganographic security algorithm
Peter U et al.[11]	Constant Correlation Spread Spectrum	(1) by reducing the BER to Zero, the watermark detection can be improved (2) tamper detection at block-level within a single computational process
S Jeevitha et al.[12]	Syndrome Trellis Code & Hamming Code	Syndrome Trellis Code method is a better technique to hide a large amount of confidential information
Hari Mohan et al.[13]	Pixel Value Differencing	In the proposed method, the PSNR value needs to adjust at the 57,98 dB up to 10KB secret text and requires to decrease MSE at 0.05 for the microscopic image of the high-density object
RL Biradar et al.[14]	Bitmask Oriented Genetic Algorithm	Authors have reviewed different techniques of steganography for encrypting the patient information
S Gulia et al.[15]	Performance comparison	Performance comparisons are performed on a variety of statistical measurements, including mean square error, peak to noise ratio, structural similarity, correlation, and structural content.
M Jain et al.[16]	Literature Survey	The authors have successfully proposed a comparison based on characteristics of various steganography algorithms used in medical images

Patient information is crucial data that needs security as well as confidentiality. The patient medical images contain medical biomarkers that are to be kept unmodified while storing or exchanging the data. In this security paradigm, the confidential message is normally converted into ciphertext by using a chaos encryption algorithm. Moreover, the performance evaluation of the various encryption techniques has been analyzed in this paper. However, it is shown that the Syndrome Trellis Code Hamming Code Steganography techniques enhance the secret image quality. It also provides more embedding capacity as compared with the RSA and AES [13].

The researchers have successfully implemented image steganography to hide text data in medical images. This process helps secure medical information while transmitting through the telemedicine system. In this case, confidential medical information is concealed in medical images using the PVD algorithm[14].

To keep medical data secure, various steganographic techniques are reviewed. The authors of this paper.

IV. APPLICATIONS

Although comparatively less scientific literature is available on applications of image steganography techniques. LSB is one of the simplest and most widely used methods to hide data into a cover file. Usually, the LSB insertion technique is used to convert the binary data and overwrite the least significant bit of each byte of the cover image. As a 25-bit color image contains a huge amount of pixel data so the amount of change will be minimal and hence cannot be detectable.

There are two very famous techniques, masking, and filtering, which are normally used on colorful 24-bit media images and greyscale images. They perfectly work digital watermarks for their potential usage, as it is evident that the masking technique is more potent than LSB insertion technique. Masking techniques usually embed content in the least significant regions so that the hidden information looks almost identical to the cover image hiding it in the noise region [17].

Adaptive LSB is a steganography technique and the integrity of the secret message data is preserved with high capacity. The adaptive image LSB was proposed to avoid irregular changes in edge areas. In this way, this technique also works a lot to obtain a better quality of the stego-image.

Texture, brighten, and edge-based adaptive LSB is a more improved version of the previous simple LSB technique. The supremacy of this technique is that it

Combining Pattern Bits using LSB is another useful steganography technique that provides improved security of hidden information.

PVD using LSB works on edges with an adaptive LSB smooth method that provides high hidden capacity with good visual quality. With an improved version, information hiding is excellent on both cover image and stego image.

Hybrid Edge Detection using LSB uses a combination of canny and fuzzy features. It provides high hidden capacity with a high PSNR value.

Steganography of any type has been utilized successfully by militant associations in order to communicate secret messages for different purposes. A long time ago, a US special forces officer from the FBI filed a complaint against a few Russian attackers, alleging that they were using steganography to conceal secret messages The use of 3D cover picture models can be more useful than 2D images for high capacity. It has also been observed that criminal organizations use 2D cover images for steganographic processes. As a result, the advancement of steganography calculations using 3D image models is critical for the efficient operation of defense organizations[18].

Shamir's Secret Sharing algorithm is used to hide secret message to protect encryption keys. This secret message is segregated into multiple chunks normally called shares. At receiving end, these shares are utilized to reconstruct the original secret message. The proposed method can store longer Electronic Health Record (EHR) with better authenticity and confidentiality [201].

In this paper, the authors have proposed a medical image encryption method for mobile health systems, particularly for Android. The proposed method combines three algorithms namely RSA, logistic chaotic encryption, and steganography technique. They have implemented a simple application on the Android platform to evaluate its performance [202].

This paper proposes the effective use of the cloud for medical information concealment via steganography. A compelling visual saliency technique in the proposed framework was used to detect the region of interest in the medical image. Secret information is seen and used in a host image, resulting in a stego image that is encrypted and sent to the cloud. The cloud encrypts the image and sends it back to the client as an encrypted, marked image because it has a lot of resources. The client can then extract the selectively encrypted region of interest and combine it with the non-interesting section to produce a selectively encrypted image that can be delivered. [203].

Biometric traits are being used to identify people, which is a new trend. Biometric recognition has gotten a lot of press over the years because of its security implications. Fingerprints are one of the most practical biometrics currently available. Techniques such as watermarking and steganography have been used to improve the security of biometric data. Watermarking is traditionally defined as the process of embedding data into a carrier file to protect copyright in music, video, or image files, whereas steganography is the art of concealing data. This paper provides an overview of the steganography techniques used to protect fingerprint biometric data. We also discuss the benefits and drawbacks of targeted and blind steganalysis procedures, which is novel. [204].

We present a method for integrating a QR code with data that can be utilized to personalize a patient. This is done to ensure that the image to be transmitted is not considerably different from the original. The QR-code is dispersed throughout the image by modifying numerous pixels based on a threshold value calculated from the average value of nearby pixels surrounding the region of interest. The findings show that the code can be embedded and fully retrieved with very minor modifications in the UIQI index - less than 0.1 percent [205].

This paper discusses a new approach to transmitting sensitive patient medical records data. Using RGB and alpha RGBA picture and decision tree, the secret medical data is hidden inside scanned grey MRI medical images. To improve the hiding capacity, the alpha channel from the RGBA image is extracted and blended with the grey medical image. The medical data is encrypted using the RSA cryptosystem, and the blocks are separated using a dynamic key. It is required to organize the grey-alpha channel medical cover image into several blocks using the dynamic key as part of the steganography procedure. Breadth-First Search and decision trees are used to allocate secret cipher blocks to grey-alpha channel medical cover picture blocks for data embedding [206].

Because the suggested method is for spatial domain image steganography, some of the most important spatial domain methods are briefly presented here. Because the content contained in spatial domain steganography is susceptible to alteration if the image is tampered with, it is also known as fragile steganography. In previous research works, the scientists apply the spatial domain information concealment technique to ensure that the image being conveyed is accurate. The dynamic key creation utilizing graph 3 coloring distinguishes our suggested solution. The algorithm's strength is the dynamic nature of the key, which aids in the embedding of changing bits. The cover picture is recovered once the secret information bits are extracted from the stego-image, making our suggested approach reversible [207].

The main goal of this research is to develop an efficient method for image steganography in the biomedical area so that security can be provided to the patient's valuable confidential sensitive data while also exploding the high security of the precious brain information from intruders. Patient electronic recorded and personal identity information can be saved and transmitted securely. When sensitive medical data is communicated asynchronously, the data structure queue plays a dynamic role in resource sharing between many communication participants. Because it is computationally secure against a chosen-plaintext attack and demonstrates the complexity of integer factoring, the Rabin cryptosystem is employed for confidential medical data writing. The cryptosystem's output is divided into various blocks and dispersed into sub-blocks. Various brain disease cover images are grouped into blocks of diagonal queues throughout the steganography process [208].

This research paper proposes an imperceptible digital steganography approach for hiding EHR in a without altering the image's critical components. Since the human visual system is comparatively less sensitive to any changes in high contrast areas of images, hence this method uses edge detection to identify and embed hidden data in sharp regions of the image. Furthermore, a Hamming algorithm that embeds three secret message bits into four bits of the cover picture is used to improve the quality of the images created. To preserve the decision region, i.e., the Region of Interest (ROI), we hide EPR in the Region of Non-Interest (RONI) [209].

This work presents a preliminary investigation of the degradation of medical photographs encoded with several steganographic algorithms, employing a range of widely used platforms. Image quality is assessed using a variety of commonly used metrics that are also used in other aspects of image processing. The findings lead to the conclusion that traditional data embedding can result in numerical and perceptual inaccuracies in an image. The more robust a data concealing is, the more errors it is likely to produce [210].

For the security of medical images, the suggested technique provides an efficient and secure storing technique. We suggested a promising steganography technique based on the Integer Wavelet Transform (IWT) for converting an MRI medical image into a single container image. The dummy container image was created by taking the container image and flipping it to the left. The secret image of the patient's medical diagnostic was then taken and Arnold transform was applied, yielding a scrambled secret image. The scrambled secret picture was embedded into the dummy container image in the first scenario, and a dummy secret image was created using Inverse IWT. The container image was taken and fused with the dummy secret image in the second scenario, yielding a stego image [212].

V. STEGANOGRAPHY TYPES

Steganography, watermarking, and cryptography are the three types of information concealment technologies. Watermarking and steganography are divided into two categories.

A. Fragile Steganography

The fragile approach entails embedding information in a cover in such a way that any changes to the host file will destroy all embedded data. Because it can be readily erased from a career, it is not a good choice for copyright protection, but it can be used as evidence of file originality in legal proceedings. Fragile approaches are easier to implement than robust ones.

B. Robust Steganography

Bit manipulation of robust methods, in contrast to fragile approaches, will not be simply erased from the host file. Even though no technique can guarantee that embedded data will not be changed, a robust method is defined as one that requires a significant amount of work to destroy information. To protect the security of embedded data, discovery must be extremely difficult. Fingerprinting and watermarking are two types of robust steganography. Fingerprinting is used to place a mark on a specific file for a specifically authorized customer. This unique mark can be used to prove which customer has broken copyright laws and disseminated a specific copy of a file [213]

The use of overlapping blocks is offered as an edge detection approach. Then, using an XOR operation, it embeds two secret bits into three coefficient bits to reduce the difference between the cover and stego images. The experimental findings show that the suggested method achieves a good balance of stego picture security, embedding capacity, and visual quality [214].

To prevent illegal manipulation of medical images, it is critical to check their integrity. We use the SHA method to calculate the cryptographic hash function of the ROI (Region of Interest) to ensure its integrity. The discrete wavelet transform will be used to incorporate the hash value (H1) in the RONI. One can check the integrity of a medical digital image by comparing the hash value at the receiver end. The hash function does not match if there is any tampering. This study presents a novel approach to enhancing security. By using spatial reversible steganography technology, the updated medical image is inserted in an ordinary-looking image. It aids in the concealment of sensitive medical information. It assures that eavesdroppers will not suspect that a medical image is being concealed [215].

One of the most well-known domains of application in medicine, where remarkable development has been seen in a variety of associated medical fields.

Steganographic calculations can be used to hide the patient's medical history and other sensitive information from reports created on a 3D model of human organs.

VI. CHALLENGES

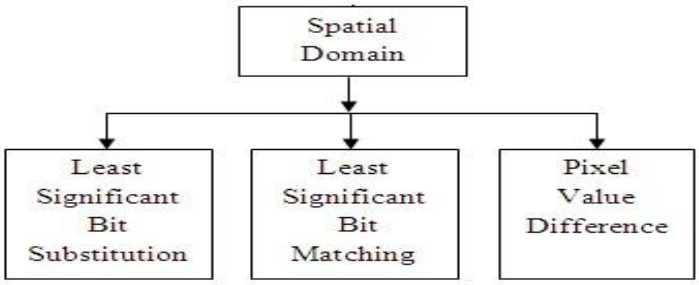

Fig. 4: Classification of Spatial Domain

"*Image steganography has two main domain such as spatial domain and frequency domain. Traditionally the frequency domain steganography is based on the transform coefficients of the cover image. However, the four most popular methods in frequency domain image steganography is Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Contourlet transform (CT)"* [207].

A. Spatial Domain Techniques

There are numerous adaptations of the spatial steganographic area as shown in Fig 4 as; all these are based on altering a few bits within the picture pixel values in the information. The Least Significant Bit based steganographic process is one of the best methods that stows a promising approach without extra payload and computation. It also provides optimal security and secret information is almost invisible by human eyes. [19]. The Least Significant Bit technique is widely used but it provides poor defense against geometrical, compression, and statistical attacks. Hence, it lacks security requirements.

B. Transform Domain Techniques

This can be a more complex method of embedding data in an image. Different calculations and changes are utilized on the image to embed data in it. Change space inserting can be named as a space of implanting strategies for which several calculations have been suggested. The method of implanting information within the recurrence space of a flag is much more grounded than implanting standards that work within the time-space. Most of the solid steganographic frameworks nowadays work inside the change space. The Change space methods have an advantage over spatial space methods as they stow away data in areas of the picture that are less uncovered to compression, trimming, and picture handling. A few change space strategies do not appear subordinate to the picture organize and they may have beaten lossless and lossy organized changes [19].

- **Discrete Cosine Transform:** Although it is better than DFT but possesses comparatively lesser embedding capacity, little security, and poor robustness against attacks. DWT is more secure than DCT and provides moderate embedding payload capacity and it needs high supplementary data to achieve reversibility. DT-CWT provides an accurate coefficient that should be selected to avoid loss of data during embedding and extraction processes.
- **JPEG Steganography**: It was believed that steganography would be impossible to employ with JPEG photos because of the lossy compression used by JPEG. As previously discussed, steganography can leverage redundant bits in a picture to embed data; however, because redundant bits are eliminated in JPEG, any hidden data would be lost [204].
- **Transformed into Discrete Wavelets (DWT)**: The DWT has recently turned out to be the preferred field of study in the area of concealing information. This is due to its widespread use in the new JPEG2000 image compression standard, as well as its ability to cope with capacity and robustness. DWT, in contrast to DCT, provides a frequency and a spatial description of an image. If the signal is integrated, for instance, it will have a local impact on the image. Because it separates high-frequency and low-frequency information on a pixel-by-pixel basis, wavelet transformation is considered more appropriate for data concealment. DWT divides pixel values in sub-bands based on their frequency. [204].
- **Hiding Biometric Information**: Develop biometric-based steganography strategy. The biometric feature used to implement steganography is the skin color area of photographs. The suggested method involves the integration of data into the skin areas of the photographs. Before integration, the complexion is detected with the

HSV color space (Tint, Saturation and Value). Additionally, data integration is implemented using the Frequency Area - DWT (Discrete Wavelet Transform) method. The hidden data is inserted following the skin pixels in one of the high-frequency DWT sub-bands. [204].

- **Many distortions**: Based techniques are also used in image steganography and it does not seem useful, as the receiver must have access to the original cover media. Hence, if the attacker has the original cover file, it can easily trace and detect the secret message. Most of the substitution systems such as LSB substitution have comparatively low robustness, lossy compression attacks and format file dependent.
- **Hybrid Technique**: Singular Value Decomposition - The Singular Value Decomposition (SVD) is regarded as one of the linear algebra's most useful techniques, with applications in picture compression, data concealing, and a variety of other signal processing fields:

"*Note T is used to denote the transpose of the matrix.*
$A = U * S * V^T$

Where U is an m x m orthogonal matrix, V is a n x n orthogonal matrix, and S is an m x n matrix made up of diagonal elements, which represents the singular values of the image" [204].

C. Image Steganography

The integration of secret information in the pixel values in 2D and 3D images is done on vertices. In contrast to pixel values, vertices and sides are subject to many intentional or unintended changes in transmission (for example rotation, uniform scaling of 3D meshes, cropping, and many more). In comparison, there are more attacks on the 2D stego frame. Hence, the extraction process of the secret message must consider all these parameters, and alteration of data in 3D mesh might be needed before the actual extraction process can take place [18].

Pixel Value Differencing - Although it provides high embedding capacity yet it has a poor defense against geometrical, compression, and statistical attacks. Histogram Shifting – it limits payload capacity, less defense against certain attacks. Difference Expansion – it needs a large amount of data for extracting secret information. It possesses lesser control of capacity. Pixel Intensity Modulation – it provides low payload capacity and poor defense against noise attacks.

D. Adaptive Steganography Region-Based

- **HVS:** Although it is very difficult to detect the embedding process in HVS, it provides a poor embedding rate. Genetic Algorithm is traditionally used to produce optimal solutions that can be obtained through a great number of computational stages and results in poor search speed in finding precise embedding locations.
- **Fuzzy**: It aids the system by rapidly selecting exact image patterns and decreasing irreversible complications, allowing the scheme to be used in real-world scenarios with correct imperceptibility. It does, however, come at a higher expense of modeling complexity.
- **Neural Networks**: Its classification capabilities are outstanding. It contributes to the system's great robustness and imperceptibility. However, training data has extremely high requirements, and accuracy is dependent on it.

VII. FINDINGS FOR FUTURE SCOPE

Some conclusions may be drawn from the literature review, which is listed below:

- When compared to 2D image steganography techniques, 3D image steganography approaches have a higher payload carrying capacity.
- The geometrical domain is used in the majority of techniques because it has a higher embedding capacity than topological or representation domain-based algorithms.
- When the geometrically based technique is combined with the representation-based approach and the topological based approach, the algorithm's embedding capacity increases.

There is a need to create a clever steganography algorithm that can withstand various attacks. Mesh simplification, vertex reordering, rotation, scaling, and translation transformation are some of these attacks.

We intend to study other important detection techniques in the future to more efficiently detect the return on investment and thus reduce the amount of secret data. We will also examine how to use sparse representation to effectively hide data and evaluate performance using various quality measures such as peak signal-to-noise ratio, standardized cross-correlation, and quality index. In addition, for safe wireless capsule endoscopy and secure visual contents retrieval for individualized video libraries, the existing system can be integrated with video summarizing schemes and other data hiding.

ACKNOWLEDGEMENT

Special thank goes to University of Okara for providing the IT services, Lab and Servers provisions for smoothly writing the manuscript.

REFERENCES

[1.] J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299–326, Mar. 2019, doi: 10.1016/j.neucom.2018.06.075.

[2.] Shtayt, N. H. Zakaria, and N. Harun, "A Comprehensive Review on Medical Image Steganography Based on LSB Technique and Potential Challenges," Baghdad Sci. J., vol. 18, p. 0957, Jun. 2021, doi: 10.21123/bsj.2021.18.2(Suppl.).0957.

[3.] J. Bani Salameh, "A New Approach for Securing Medical Images and Patient's Information by Using A hybrid System," Int. J. Netw. Secur., vol. 19, pp. 28–39, Apr. 2019.

[4.] "A Novel Medical Image Encryption using Cyclic Coding in Covid-19 Pandemic Situation - IOPscience."

https://iopscience.iop.org/article/10.1088/1742-6596/1797/1/012035/meta (accessed Feb. 25, 2022).
[5.] M. M. Hashim, A. A. Mahmood, and M. Q. Mohammed, "A pixel contrast based medical image steganography to ensure and secure patient data," Int. J. Nonlinear Anal. Appl., vol. 12, no. Special Issue, pp. 1885–1904, Dec. 2021, doi: 10.22075/ijnaa.2021.5939.
[6.] "A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography." https://www.hindawi.com/journals/ijdmb/2021/8827055/ (accessed Feb. 25, 2022).
[7.] S. Gulia, S. Mukherjee, and T. Choudhury, "An extensive literature survey on medical image steganography," CSI Trans. ICT, vol. 4, no. 2, pp. 293–298, Dec. 2016, doi: 10.1007/s40012-016-0118-8.
[8.] Stoyanov and B. Stoyanov, "BOOST: Medical Image Steganography Using Nuclear Spin Generator," Entropy, vol. 22, no. 5, Art. no. 5, May 2020, doi: 10.3390/e22050501.
[9.] Santoso, "Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm," J. Phys. Conf. Ser., vol. 1175, p. 012057, Mar. 2019, doi: 10.1088/1742-6596/1175/1/012057.
[10.] "Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm - IOPscience." https://iopscience.iop.org/article/10.1088/1742-6596/1175/1/012057/meta (accessed Feb. 25, 2022).
[11.] Tiwar, "Comparative Analysis of Different Steganography Technique for Image Security," vol. 8, no. 2, p. 4, 2021.
[12.] R. Karakiş, K. Gürkahraman, B. Çiğdem, İ. Öztoprak, and A. Topaktas, "Evaluation of segmented brain regions for medical image steganography," J. Fac. Eng. Archit. GAZI Univ., vol. 36, no. 4, 2021, doi: 10.17341/gazimmfd.753989.
[13.] P. Eze, U. Parampalli, and R. Evans, "Medical Image Watermark and Tamper Detection Using Constant Correlation Spread-Spectrum Watermarking," Apr. 2018, doi: 10.1999/1307-6892/10008924.
[14.] J. Sankaran and A. P. Nagarajan, Performance analysis of encryption algorithm in medical image security. 2018.
[15.] S. Jain, S. Dubey, and V. Singhal, "Review of Steganography Techniques for securing Patient Information embedded in Medical Image," vol. 9, no. 2, p. 3.
[16.] M. M. Hashim, M. S. Taha, A. H. M. Aman, A. H. A. Hashim, M. S. M. Rahim, and S. Islam, "Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography," in 2019 7th International Conference on Mechatronics Engineering (ICOM), Oct. 2019, pp. 1–6. doi: 10.1109/ICOM47790.2019.8952061.
[17.] R. Doshi, P. Jain, and L. Gupta, "Steganography and Its Applications in Security," p. 5, 2012.
[18.] Girdhar and V. Chahar, "Comprehensive Survey of 3D Image Steganography Techniques," IET Image Process., vol. 12, Aug. 2017, doi: 10.1049/iet-ipr.2017.0162.
[19.] R. L. Biradar and A. Umashetty, "A Survey Paper on Steganography Techniques," vol. 4, p. 11.
[20.] Ulutas, M., Ulutas, G., & Nabiyev, V. V. (2011). Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of Systems and Software, 84(3).