International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 130 – 135, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1016

# Data Hiding Techniques Using Steganography in Biomedical Media

Neetika Soni
Department of Engineering and Technology
GNDU Regional Campus
Jalandhar, Punjab India

**Abstract:** In e-healthcare paradigm it is important to secure the patient's personal details along with his biomedical information when shared over the insecure public channels. This paper discusses various techniques of data hiding in biomedical media including biomedical images and signals and discusses steganography techniques for ECG signal specifically.

**Keywords:** Data Hiding, Steganography, Spatial Domain, Transform Domain, Embedding Capacity, BER

## 1. INTRODUCTION

Remote healthcare monitoring systems and point of care technologies have become popular for homebound patients. These e-healthcare solutions are more reliable in emergency services as patient's medical information can be sent immediately to the doctors and appropriate actions can be taken without any delay. These services provide a platform where the advice from the globally available experienced doctors can be utilized anytime and anywhere. It also helps in reducing the medical labour cost and in decreasing the traffic at hospitals. The patient's biological signals such as Electrocardiogram (ECG), Electroencephalogram (EEG), Electromyogram (EMG) and images like Magnetic Resonance Imaging (MRI), Computed Tomography (CT) scans, Positron Emission Tomography (PET) images, ultrasound etc. which need to be diagnosed are recorded and sent to the hospital server. These biomedical signals are transmitted over the channel through internet. Patient's personal information such as name, age, sex, identity number, his clinical reports such as temperature, blood pressure, glucose level etc. and medical history is also tagged along with these signals. Hence, to maintain the secrecy of the personal information, only authorised doctors and certain administrative personals has the right to access the information. But since the communication between the two parties is over long distance, using public network, there is always a threat of an unauthorised access and personal details of the patient could wind up in wrong hands. Therefore security of patient's sensitive data is a major issue in e-health care systems [1].

Different techniques are used to secure the secret information from eavesdroppers like cryptography (encryption/decryption), steganography and watermarking are given in figure 1.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 130 – 135, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1016

- Cryptography – It is a process of encryption where both the parties communicate in secret. The key is required to make the information accessible. Since the final data is stored in the encrypted format so this method is unable to conceal the fact that there is a message inside.
- Steganography – It embeds the secret message in the cover media in such a way that it hides the fact that there is any message inside. It provides a means of secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data will be confidential unless an attacker can find a way to detect it.
- Watermarking – In watermarking, some identification information is directly embedded into the host signal without affecting the usage of the original host signal and is hard to perceive by ordinary perception systems. The embedded information is mostly related to the host signal [2].

Cryptography based techniques results in large computational overhead whereas in steganography based techniques the sensitive information is hidden inside another insensitive host data, thus does not incur any increase in the host data size and computational overhead [2].

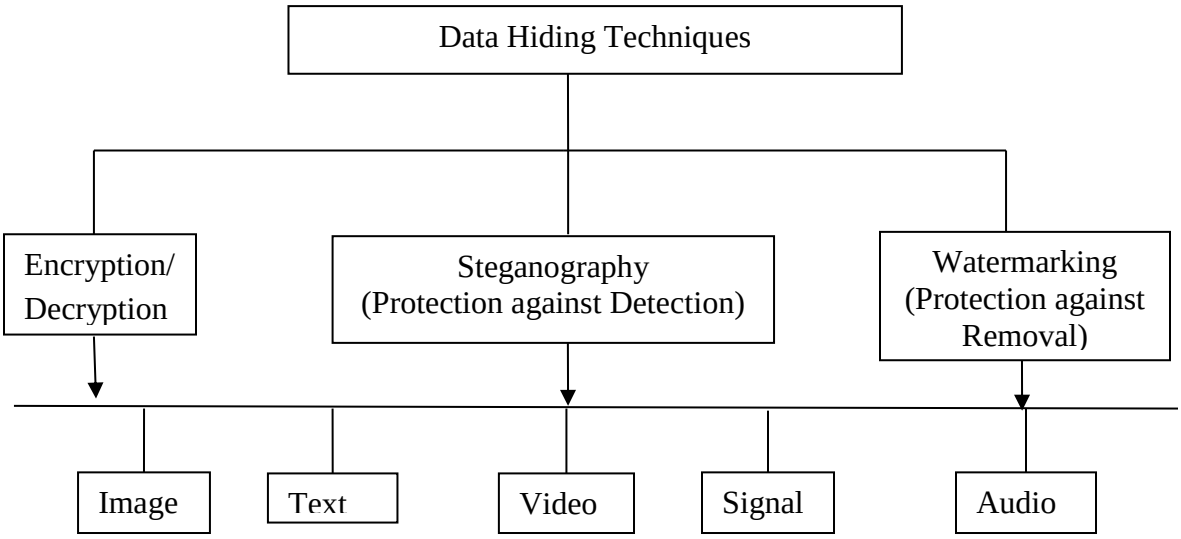


**Figure 1 Data Hiding Techniques**

## 2. DATA HIDING IN BIOMEDICAL MEDIA

Though all the above said methods are good for hiding the secret information but in biomedical applications steganography is preferred as any doctor can check the steganographed biomedical signal and possibly make a decision in case of an emergency but only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential information stored inside the host signal

A lot of research has been done to hide data in biomedical images and signals. In [4] R. Acharya

et al. interleaved patients text files into X-ray and MRI images by sharing last bits of discrete cosine transform (DCT) coefficients. M.S. Nambakhsh et al. used PET images to watermark patient ID and ECG signal using multi-resolution wavelet decomposition [5]. In [6] encryption of medical images based on the cosine number transform is done. Further, A.Ibaida et al. using wavelet transform embed patients clinical details into ECG signal while maintaining 99% accuracy of the ECG signal [1].S.E.Jero decompose ECG signal using Discrete Wavelet Transform and employ singular value decomposition technique to embed secret information in decomposed 2-D ECG signal[7]. Later he used curvelet transform to steganograph personal information in ECG signal [8]. Curvelet Transform is a new member of wavelet transform family that provides optimal sparse representation of the edges and compute the coefficients from different scale, translation and orientation.

## 2.1 Steganography in ECG signals

Due to the living style of the people and their exhaustive work culture, the life has become so stressful that it has direct effect on their heart. The most commonly used monitoring system to keep track on the electrical activity of the heart is Electrocardiogram (ECG). It is a diagnostic tool where each heartbeat is displayed as a series of electrical waves characterized by peaks and valleys. The deviations in the normal electrical patients indicate various cardiac disorders. Since, with the advancement in cardiac pathology and cardiovascular diagnostic system, it has become easy to acquire ECG signal and to transmit with the hand held devices. Also, the size of the ECG signal is large enough that it can easily host other small size information. Therefore ECG signal has been chosen here as a cover signal to embed patient's personal information for steganography.

In steganography, when we embed information bits inside the cover signal it gets distorted. Any constraints or significant changes in patient's diagnostics signals may cause error in diagnosis and treatment with possible life threatening consequences. To preserve the fidelity of the host signal its significant regions should be kept intact. Various attributes that affects its performance are [3]

- **Security:** It implies that embedding algorithm should be robust enough to be accessed by the attackers. Security in steganography is the ability to assure secrecy and integrity of the steganographed information and protects it from malicious attacks.
- **Imperceptibility:** It means that the secret information should not be noticeable to the viewer besides having high embedding capacity and capability to withstand against stego attacks.
- **Embedding Capacity:** It is defined in terms of number of secret bits that can be embedded in cover signal. Ideally it should be as high as possible while maintaining the acceptable quality of stego-image.

There is always a trade-off among these three attributes. As we increase the capacity of the secret bits, the robustness strength and/or imperceptibility decreases.

## 3. PERFORMANCE EVALUATION PARAMETERS IN STEGANOGRAPHY

**3.1 Bit Error Rate (BER):** It is the ratio between the extracted secret information and the original secret information. BER increases with the increase in data loss [8].

**3.2 Embedding Capacity (EC):** It is the hiding capacity of the host media and is defined as the ratio between the total number of hidden secret bits and the total number of bits in the cover image[1].

**3.3 Distortion Measurement Parameters:** To evaluate the statistical properties of the reconstructed and original ECG signal various performance parameters can be used. For example: Peak Signal to Noise Ratio (PSNR) [8], Percentage Root mean Square Difference (PRD) [8], Kullback Leibler Divergence (KL Divergence)[8], Structural Similarity Index Measure (SSIM) [9], Normalized Cross-Correlation (NCC) [10].

## 4. CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

Data hiding techniques used in steganography can be broadly classified into Spatial domain, and Transform domain (Figure 2).Each domain has its own advantages and disadvantages in regard to embedding capacity, robustness, execution time etc.

### 4.1 Spatial Domain Steganography

In Spatial domain, the secret information is directly embedded into the host media. Spatial Domain techniques are easy to implement with less computational complexity.

### 4.2 Transform Domain Techniques

Since the digital media (image or signal) is combination of low and high frequency components where the smooth regions represents the low frequency whereas sharp curves and edges represents the high frequency components. . Low frequency regions are more sensitive and any change in these components will be transparent to human visual system [1], so cannot be modified. In Transform domain steganography, the host media is decomposed into its high and low frequency coefficients and secret information is embedded in high frequency region according to some embedding algorithm The signal is reconstructed by taking the inverse transform. The transform domain methods are more immune to processing operations and are less susceptible to stego attacks.

## 5. CONCLUSION

Since biomedical media images or signals contains very sensitive information and any modification in the features of the media can change its morphology which can lead to wrong diagnosis. There it is utmost important to perform steganography in such a way that

the diagnostic features of the media remain intact.

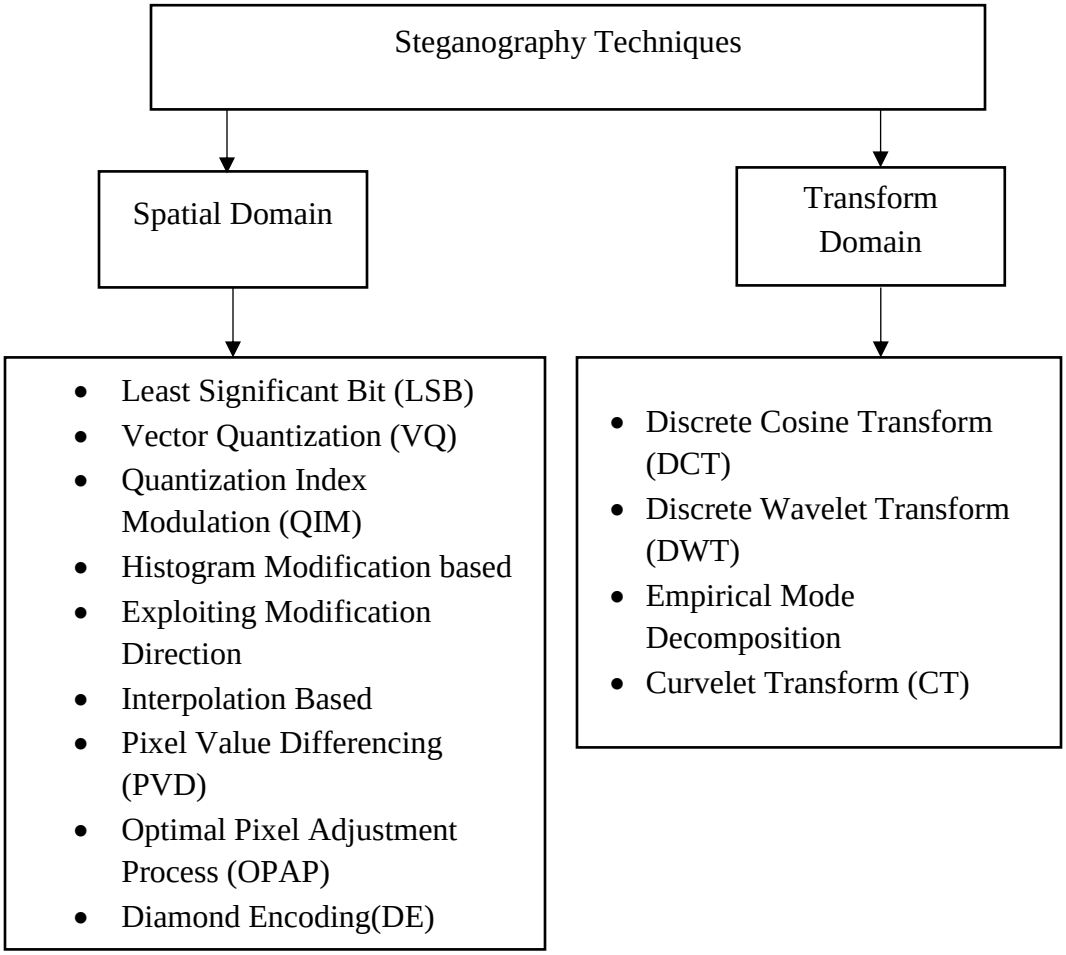


**Figure 2. Different Techniques used to perform Steganography**

## REFERENCES

1. A.Ibaida, I.Khalil,"Wavelet Based ECG Steganography for Protecting Patient Confidential Information In Point –Of– Care Systems ",*IEEE Transactions on Biomedical Engineering,* Vol 60, No 12, December 2013.
2. A. Khan, A. Siddiqa,S. Munib and A. Malik,"A recent survey on watermarking techniques", *Information Sciences,*vol 279, pg 251-272, April 2014.
3. M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review,* vol. 13-14, pp. 95-113, Oct 2014.

**4.** R. Acharaya U, U.C.Niranjan, S.S. Iyengar and N. Kannathal,"Simultaneous storage of patient information with medical images in the frequency domain",*Computer Methods and Programs in Biomedicine,*vol 76, pg 13-19 February 2004.

**5.** M.S.Nambakhsh, A. Ahmadian and H. Zaidi, "A contextual based double watermarking of PET images by patient ID and ECG signal ," C*omputer Methods and Programs in biomedicine,*vol. 104,pg 418–425, August 2010.

**6.** J.B.Lima, F. Madeiro and F.J.R.Sales,"Encryption of medical images on the cosine number transform",*Signal Processing: Image Communication,* vol 35, pg 1-8, March 2015.

**7.** S.E Jero, P.Rammu and S. Ramakrishnan,"Discrete Wavelet Transform and Singular Value Decomposition Based ECG Steganography for Secured Patient Information Transmission", *J. Medical Systems,* vol 38, pg 132(1-11), September 2014.

**8.** S.E Jero, P.Rammu and S. Ramakrishnan, "ECG steganography using curvelet transform", *Biomedical Signal Processing and Control,* vol 22, pg 161-169, July 2015.

**9.** S.Sidhik, S.K. Sudheer and V.P.Mahadhevan,"Performance and Analysis of high capacity Steganography of color images involving Wavelet Transform",*Optik,* vol 126, pg 3755-3760, August 2015.

**10.** A. Phadikar,"Multibit Quantization index modulation: A high –rate robust data hiding method",*Journal of King Saud University-Computer and Information Sciences,* vol 25,pg 163-171, November 2012.