# Review Paper on Digital X-Ray Image and Steganography

Manisha Rani[1], Er.Gaurav Deep [2]
[1]*Punjabi University, Patiala, Punjab, India*

***Abstract*** **-** The steganography is a technique to hide the digital data into another container data that enhance the security of crucial information. The emerging growth in usage of internet for sending or receiving precious information over the network leads to misuse of crucial data especially patient medical information. Therefore, different methods have been proposed so far for concealing information in different digital cover media. In this paper, the process of Integrating the information produced by Digital X-ray reports in itself has been proposed that will ultimately benefit to the patient, as Physicians will be having better access to images and reports allowing them to make a faster diagnosis from anywhere in the world. In result, patients can potentially obtain faster and more effective care. Image steganography is used to hide the sensitive patient information into the carrier medical image to ensure confidentiality.

***Keywords*** **-** *Digital X-Ray; Steganography; Steganalysis; Stego medium; Stego image ; k mean*

## I. INTRODUCTION

The X-ray is a medical imaging technique used in radiology to diagnose, monitor, and treat many medical conditions like fractures, tooth decay, enlarged heart, arthritis etc. It helps physicians to view inside the body without having to make an incision. Although the advancement of new technologies like computed tomography (CT), ultrasound imaging and magnetic resonance imaging (MRI), the X-rays remain an important tool for the diagnosis of human internal body parts. In this a beam of X-rays, generated by an X-ray generator, is passed through the part of the body to be scanned. The X-rays are absorbed by the part of body as they pass. X-rays that are not absorbed pass through the object and are recorded on X-ray sensitive film.

Now a day digital X-ray sensors are used over conventional X-ray sensors because digital X-rays expose patient to very less radiation and ease of use i.e. images can be immediately enlarged to see bone and/or soft tissue in a single exposure. Another benefit include time efficiency by bypassing chemical processing and the capability to digitally transfer and enhance image quality. Digital X-ray images are having enhanced image quality due to its standard like DICOM.

DICOM standard not only permits the transfer of medical images in a multi-vendor environment. It also supports the process of integrating information produced by the various medical applications to produce the patient's Electronic Health Record (EHR)[15]. We can enhance the digital image quality by alter brightness and contrast. Digital X-ray produces large images that are enough space to store patient information and it do not leads to image degrade effect due to having enhanced image quality. DICOM chose to map values into a perceptually linear range, that is, one that a human observer would perceive as a line. As a result, the images look alike. When a radiologist sends an image to a physician, both see the same grayscale presentation[15].

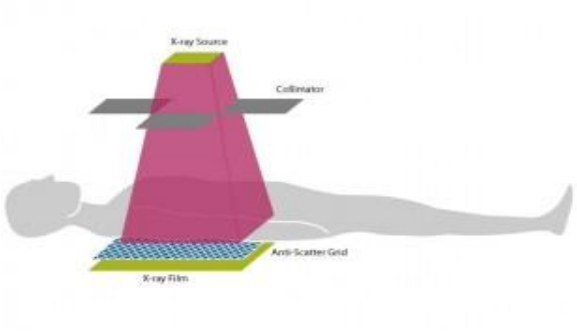


Fig1: The basic setup for X-ray imaging[15]

Digital X-ray images may contain some patient's confidential data that needs to be protected against intruders while data traverse in open network and stored in hospital servers[16]. So, the patient's medical and personal information can be integrated in digital X-ray report itself using image steganography technique which ensures data security. Secondly to provide two layer security patient information can be encrypted before embedding into the image, So that if somebody access the concealed information even than it is not understandable to intruder. The benefits will ultimately falls to patients as Physicians have secure access to images and reports allowing them to make a faster diagnosis anywhere in the world. In result, patients can potentially obtain faster, more effective care.

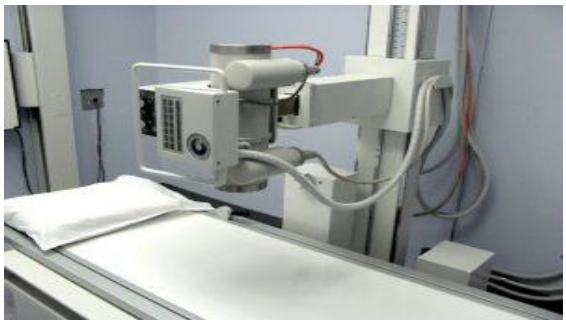

Fig2: Digital X-ray Scanner[15]

## II. PREVIOUS WORK

In medical field, not much work is done previously on medical image steganography.In Sept. 2010 **Shuhong Jiao, Robert Goutte** proposed that the information of patient and another related textual records can be concealed in 2D black and white image of any modality. Author uses the AES encryption algorithm to encrypt the patient information and then hiding 2D cover medical image using DCT transform domain steganography technique[1].

**Orooba Ismaeel Ibraheem Al-Farraji," Hiding The Results of Medical Test in Medical Digital Image".** In this paper author shows the assessment of image steganography in medical digital image. Brief on the need of steganography in medical field. It used BMP format image to hide patient information. Proposed a scheme in which medical image in BMP format is divided into block. Find the position to hide the byte of the text. In results it gives a proposed system to transfer the medical image with the high security of results related to medical test[2]. **Rafael A. Sampaio, Marcel P. Jackowski,"Assessment of Steganographic Methods in Medical Imaging".** In this author introduced the DICOM image that is known as digital imaging and communication in medicine. This paper gives brief introduction about the DICOM image that is used in medical field. DICOM is a standard of storing, printing and transmitting medical image information . It proposed the investigate and embedding DICOM tag information into their respective images. In this article , he explored three Steganography methods for embedding textual information in medical images. DICOM images having two main components a header that contains confidential patient information and another is grayscale matrix which represent image intensities. It uses Mean change Modified Method to hide information that provides and efficient technique to hide information inside the image pixel. In this message that hides not encrypted[3]. **Gurinder Singh, Gaurav deep," MRI Medical Image and Steganography"**. In this paper author implemented the steganography and cryptography combination in the medical field by choosing MRI images as cover object. In this author proposed the method of storing data into Region of Non- Interest (RONI) firstly divided the image into two part one is ROI and RONI. Then uses Elliptic Curve cryptography method to encrypt the text message. The encrypted message is embedded into the RONI using spatial encoding technique. The results of the proposed model have been obtained of the given dataset in the form of the image quality parameters of MSE and PSNR[4].

## III. STEGANOGRAPHY IN DIGITAL X-RAY

Steganography is the art and science of writing hidden messages in such a way that no one, except from the sender and receiver suspects the existence of the message, a form of security through obscurity[5]. These days because of the wide access of internet to the common man, digitally transferred data has a high risk of being attacked or destroyed [6].So, that's why a secure transmission of information is required. The main goal of steganography is to hide information in the other cover media so that other person or intruders will not notice the existence of the information [7]. Steganography is the leading method in the Internet to protect data secrecy, privacy and copyright so that intruder could not be able to misuse the information. Cryptography is also used for the same purpose but the advantage of steganography besides cryptography is that the secret information or data does not pay any attention to itself as an point of security [8]. Another an impactful advantage of steganography over cryptography is, the contents of message is protected alone but steganography concerned with concealing the fact that a secret message is being sent in addition to hide the content of the message only. The interesting thing in steganography is we could hide the information or data in any kind of digital media such as image, text, sound and video regarding to the cover capacity, the wanted security level and robustness. There are several methods, which can be used to hide the crucial information from the straight visuals of human. Nowadays, the combinations of steganography and cryptography methods are used to ensure data confidentiality [9] and to improve information security. Table 1 shows the comparison of various secret communication techniques used nowadays[9].

TABLE I
COMPARISON OF SECRET COMMUNICATION TECHNIQUES

| Secret Communication Techniques | Confidentiality | Integrity | Un-removability |
|---|---|---|---|
| Encryption | Yes | No | Yes |
| Digital Signatures | No | Yes/No | No |
| Steganography | Yes/No | Yes/No | Yes |

Finally, The following formula provides a very generic description of the pieces of the steganographic process:

*cover_media + hidden_data + stego_key = stego_media*

- **Hidden data:** The data or information that needs to be protected against untrustworthy users is called as secret data or secret information. The secret data can be in any form either be a text or a digital image or a video or audio, that needs to be saved or secured.
- **Cover Media:** The Media in which secret data or information is concealed called as cover media. Cover media can be in various forms like video, audio, signal, image, etc.
- **Stego Key:** The secret key that is used to encrypt the hidden data by the mean of using efficient cryptography methods in order to boost the security level is called as Stego Key.
- **Stego-media:** The cover media after embedding hidden data is known to be stego-media, which contains the secret data or hidden data without any special focus on the information in that media.

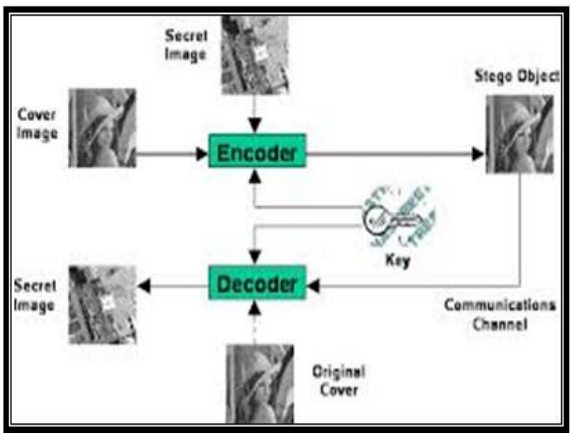


Fig.3: Process of steganography [9]

## IV. REQUIREMENTS OF HIDING INFORMATION DIGITALLY

There are number of steganography techniques that are used to conceal the information in a given object. However all the techniques must satisfy a number of requirements while implementing Steganography[1]. The general specification for the requirements that must kept in mind are described below:

*a) Quality of Cover Media:* The embedded data must not downgrade the supremacy of cover media. Quality of cover media should not seems to be eccentric, looks as original cover media. The media size should not increase tremendously as it can look suspicious to the casual viewer. It must have good Peak Signal to Noise Ratio measurement.

*b) Size of Cover Media:* A cover file must be of ample size so that it can conceal big amount of message without the need of compression.

*c) Integrity of data:* Integrity of data should be maintained, it must be robust enough so that it must not be modified in between the way.

*d) Retreival of data:* The hidden message must be undetectable during steganalysis process except to the responsible party.

## V. CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

There are different approaches used to classify steganography techniques. The first approach is to classify the Steganographic methods according to the type of cover channel used. The second approach is to classify the Steganography methods according to the modification performed on the embedding process in the cover medium.

Steganography can used for almost all digital file formats, but the formats with high degree of redundancy are more recommended. Redundancy is defined as the bits of an object that contribute accuracy preferably greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily . Image and audio files are mainly satisfy with this prerequisite while research has also uncovered other file formats that can be used for concealing information . There are four types of file formats that can be used for Steganography shown in fig.4[10].

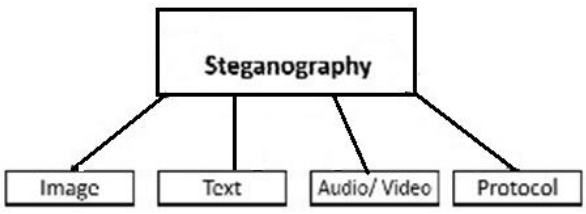


Fig.4: Types of Steganography[10]

In this paper we emphasizes on image steganography techniques. The basic and mainly used image steganography embedding techniques are described below.

***Least Significant* Bit (LSB)** It is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all the bits inside an image is changed to a bit of the secret message the technique for increased capacity of information hiding in LSB method gives better performance in all the parameters and is a safe technique for embedding secret messages[11].

For example a grid for 3 pixels of a 24- bit image can be follows[11]:-

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is embedded into the Least Significant Bit of this part of the image, the resulting grid is as follows:

(00101101 0001110**0** 01011110)
(10100110 1110010**0** 00001100)
(11011010 1010110**1** 01101011)

Despite the number was embedded into the first 8 bits of the grid, only the underlines bits(3) needed to be changed according to the message. So, in this method some of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

***Most significant bit (MSB)*** It is a common approach to encrypt information in a cover image. The most significant bit that is the 1st bit of some or all the bits inside an image is changed to a bit of the secret message. For example a grid for 3 pixels of a 24- bit image can be follows[11]:-

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is encrypted into the Most Significant Bit of this part of the image, the result is as follows:

(**0**0101101 **0**0011100 01011110)
(**1**0100110 11100100 00001100)
(**1**1011010 **1**0101101 01101011)

Although the message was embedded into the first 8 bits of the grid, only the 5 underlines bits needed to be changed according to the embedded message.

## VI. METHODOLOGY

There are several schemes exist to hide data in digital images but in this paper a new steganography algorithm has been proposed for hiding patient confidential information in that uses Digital X-ray image as its cover media object. It utilizes the benefits of cluster based segmentation technique.
Segmentation is the advanced technique in which a digitalized image is partitioned or segmented into numerous segments or parts based on the values of pixel [12].There are many methods for segmenting an image that has been proposed by researchers.
In this we have used clustering technique, clustering is a method in which objects are defined into groups based on their characteristics. Clustering is the process of organizing the objects in such a way that objects within the cluster are similar to each other and dissimilar to other objects [13]. There are

many clustering algorithms that are designed to create clusters in digital images. We have proposed the use of K-mean clustering scheme into this section. K-mean algorithm that partitions the input data into numerous classes on the basis of their inseparable distance from each other[12]. The algorithm requires a digital image as input. K is the number of clusters and a centroid will be assumed for each cluster. The main benefit of this scheme are is that, it is quite easy to understand, robust and fast The another advantage is that it provides best results when the data is discrete.

Further in order to retain the information of the region of interest (ROI), the embedding of secret data is only performed using the Region of Non-Interest (RONI) so that embedding process do not degrade the quality of medical reports. In addition, to enhance the security of secret information embedded into digital cover media needs to be encrypted. For encryption purpose encryption algorithm is used to encrypt the secret data. Basically Encryption algorithms are mostly used to ensure data confidentiality and integrity in different communication systems and networks. Public or private encryption keys can be used, depending on the specific of each service and application[14].

The following is the proposed algorithm design that is basically divided into two parts one is responsible for encryption process and other is responsible for the image segmentation and embedding process at sender side and at receiver side one will be responsible for decryption process and other will responsible for the data extraction from Stego image .

***A. At Sender side:*** The algorithms that are required to hide data by using this technique are defined as follows:

**Algorithm 1: Data Hiding Algorithm**

1) Acquire the cover object i.e. Digital X-ray image(DICOM) in which secret data has to be embed.
2) Apply the clustering (K- mean) on the acquired image.
3) Select the ROI(Region of Interest) and RONI(Region of Non Interest) from achieved clusters.
4) Embed the secret encrypted data returned by Encryption Algorithm into largest cluster among RONI using the suitable data embedding method.
5) Stego-Image will be returned that can be sent over network and the secret message will be extracted at receiver side.

**Algorithm 2: Encryption Algorithm**

1) Acquire the data to be hide in the cover image.
2) Apply cryptography technique on the acquired data.
3) Encrypted data will be returned.

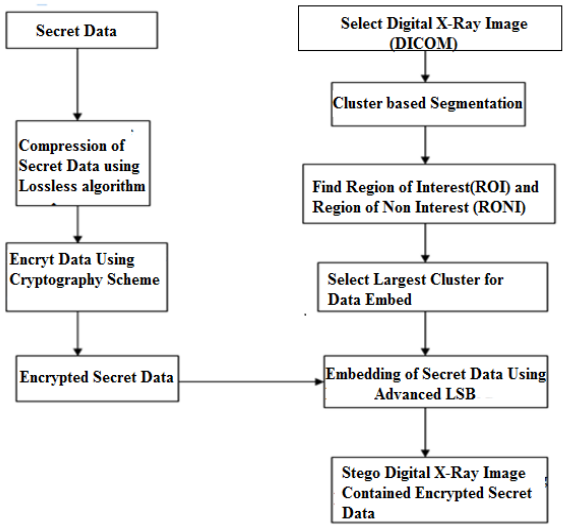


Fig 5: A general mechanism of generating stego-image from input Image

***B. At Receiver side:*** The algorithms that are required to extract hidden data from Stego-image by using this technique are defined as follows:

**Algorithm 1: Data Extraction Algorithm**

1) Acquire the Stego image in which secret data is hidden.
2) Apply the clustering (K- mean) on the acquired image.
3) Select the ROI(Region of Interest) and RONI(Region of Non Interest) from achieved clusters.
4) Identify the largest cluster in which information is hidden.
5) Extract the hidden data and call Decryption Algorithm as to decrypt the original data.

**Algorithm 2: Decryption Algorithm**

1) Acquire the data to be decrypt extracted from the Stego image.
2) Apply cryptography technique on the acquired data as to get the original form of data.
3) Original or decrypted data will be returned.

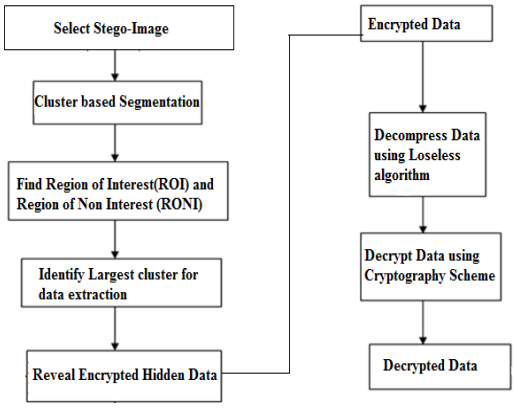


Fig 6: A general mechanism of extracting data from stego-image

## VII. CONCLUSION

In this paper new method to hide medical information in Digital X-Ray image has been presented. In this scheme , in order to preserve the content of clinical information, the region of interest (ROI) is preserved and the embedding is only performed in the Region of Non-Interest (RONI). In accordance with Health Insurance Portability and Accountability Act (HIPAA) the patient's privacy and security is important in the protection of healthcare privacy. So, The scheme of using Digital image steganography enhances medical image security, confidentiality and integrity. The hospitals and patients can fully reap the benefits from digital image steganography scheme which employed to protect the secret information as all communication that contains medical information will be secured. The scheme of integrating medical information in Digital X-Ray image to produce the patient's Electronic Health Record (EHR) will ultimately beneficial to the patients. Doctors have better access to images and reports allowing them to make a faster diagnosis, potentially from anywhere in the world despite of having any risk. In result patients can potentially obtain faster, more effective care.

## VIII. REFERENCES


[1] Jiao, Shuhong, and Robert Goutte. "A secure transfer of identification information in medical images by steganocryptography." International Journal of Communications, Network and System Sciences 3.10 (2010): 801.

[2] Orooba Ismaeel Ibraheem Al-Farraji," Hiding The Results of Medical Test in Medical Digital Image", International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015,ISSN 2091-2730.

[3] Rafael A. Sampaio, Marcel P. Jackowski,"Assessment of Steganographic Methods in Medical Imaging", Department of Computer Science,Institute of Mathematics and Statistics,University of S˜ao Paulo, Brazil,rsampaio, mjackg@ime.usp.br

[4] Gurinder Singh, Gaurav Deep," MRI Medical Image and Steganography", International Journal of Modern Computer Science (IJMCS) Volume 4, Issue 2, April, 2016, ISSN: 2320-7868.

[5] Cachin , "An Information-Theoretic Model for Steganography", 2nd Workshop on Information Hiding (D. Aucsmith, ed.) (pp. 1-12). Springer.

[6] Joseph, Princymol, and S. Vishnukumar. "A study on steganographic techniques." Communication Technologies (GCCT), 2015 Global Conference on. IEEE, 2015.

[7] Channalli, Shashikala, and Ajay Jadhav. "Steganography an art of hiding data." arXiv preprint arXiv:0912.2319 (2009).

[8] Ronak Doshi, Pratik Jain, Lalit Gupta, " Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.

[9] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques" , International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.

[10] Shelke, Falesh M., Ashwini A. Dongre, and Pravin D. Soni, "Comparison of different techniques for Steganography in images." ,International Journal of Application or Innovation in Engineering & Management 3.2 (2014): 171-176.

[11] Kanika Anand, Rekha Sharma," DATA SECURITY USING LSB &MSB IMAGE STEGANOGRAPHY", IJEEE, Vol. 1, Issue 6 (December, 2014)

[12] Sharma, Priyansh, and Jenkin Suji. "A Review on Image Segmentation with its Clustering Techniques." International Journal of Signal Processing, Image Processing and Pattern Recognition 9.5 (2016): 209-218.

[13] Zhang, Zhenya, et al. "Clustering aggregation based on genetic algorithm for documents clustering." Evolutionary Computation, 2008. CEC 2008.(IEEE World Congress on Computational Intelligence). IEEE Congress on. IEEE, 2008.

[14] Scripcariu, Luminita. "A study of methods used to improve encryption algorithms robustness." Signals, Circuits and Systems (ISSCS), 2015 International Symposium on. IEEE, 2015.

[15] Bidgood Jr, W. Dean, et al. "Understanding and using DICOM, the data interchange standard for biomedical imaging." Journal of the American Medical Informatics Association 4.3 (1997): 199-212.

[16] Sankari, V & Nandhini, "Steganography technique to secure patient confidential information using ECG signal", 2014 International Conference on Information Communication and Embedded Systems, ICICES 2014. . 10.1109/ICICES.2014.7033925.

[17] Hayat Al-Dmour, Ahmed Al-Ani, Hung Nguyen, "An efficient steganography method for hiding patient confidential information", Engineering in Medicine and Biology Society (EMBC) 2014 36th Annual International Conference of the IEEE, pp. 222-225, 2014, ISSN 1557-170X.

[18] Joshi, Kamaldeep, and Rajkumar Yadav. "A new LSB-S image steganography method blend with Cryptography for secret communication." Image Information Processing (ICIIP), 2015 Third International Conference on. IEEE, 2015.

[19] Artz, Donovan. "Digital steganography: hiding data within data." IEEE Internet computing 5.3 (2001): 75-80.

[20] Meghrajani, Yogesh K., and Himanshu S. Mazumdar. "Hiding secret message using visual cryptography in steganography." India Conference (INDICON), 2015 Annual IEEE. IEEE, 2015.

[21] Gomathi, S. "A cryptography using advanced substitution technique and symmetric key generating algorithm." Intelligent Systems and Control (ISCO), 2014 IEEE 8th International Conference on. IEEE, 2014.