Indian Journal of Science and Technology, Vol 8(16), DOI: 10.17485/ijst/2015/v8i16/61974, July 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images

Nawlesh Kumar* and V. Kalpana

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India;
nawlesh08ballia@gmail.com, kalpana@cse.sastra.edu

Abstract

Nowadays security of information became an important issue. So it is mandatory to preserve the security of data that need to be transmitted in telemedicine application for proper and cost effective diagnosis. Steganography plays an important role in telemedicine application by providing confidentiality and integrity. This paper proposes a steganography technique which hides patient information inside medical images using a key dynamically generated by graph3 coloring and pixel count of cover image. Steganography is done along with cryptography by encrypting the patient information using RSA algorithm to strengthen the level of security. This proposed method maintains reversibility that the original medical images can be losslessly restored after the extraction of data from stego medical image. Experimental results show that this novel method is more secure as compared to other information hiding methods against various parameters such as computational complexity in key generation by unauthorized person and quality measure of reversed image in terms of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

Keywords: Chromatic Polynomial, Dynamic Key, Graph Coloring, Hash Value, Region of Interest, Reversible Steganography

1. Introduction

Steganography is an information hiding technique which is used to embed information in another object known as cover by tweaking its properties. The fast growing technology and internet have changed the human life in such a way that all their requirements are easily available on a single click.

Nowadays where treatment is too costly, telemedicine plays an important role by using internet and other technology to provide services to the patients who are far away from the doctor. It has several benefits such as advanced access to medical information, care delivery access and cost effective treatment. Even though it has above advantages it has certain limitations such as preserving the security of the patient information transmitted and quality of medical image received.

It is important to keep patient's information confident along with medical images of the patient and transmit it securely. There are several image formats in use but this paper focuses mainly on Digital Imaging and Communication in Medicine (DICOM)[1] which is a standard format for medical images. Information of patient is stored in DICOM image formats as metadata.

In spite of data hiding techniques employed in DICOM images, it is still prone to external influence and alterations. In this paper the level of security related to information of the patient and his medical image need to be transmitted is addressed through steganography. This method is based on the key generated by graph[3] coloring with pixel count. In this technique patient information is hided in the medical image of the patient instead of sending patient information and medical image separately.

This proposed work ensures reversible graph three

*Author for correspondence

coloring steganography technique in which the patient data is hided in the medical image of the patient. The original medical image of the patient is known as cover image in which information of the patient is embedded with the help of dynamic key generated from the graph coloring and pixels count. The graph which is needed to be color is different for differentmedical imagesbased on the number of pixels of the image. So the key generated from the graphcoloring is dynamic. The key generated from the graphcoloring in the proposed method is used to embed the information bit in the pixel of the image to generate stego image. Similarly in the receiver side the same key is generated using graph coloringto extract the patient's information from received stego image. Since this is reversible steganography technique the original medical image is recovered after extraction of information from the stego image.

2. Literature Survey

In telemedicine application doctor checks patient's medical image along with the data which is received from remote places. For proper diagnosis security parameters such as confidentiality, authentication and integrity for the medical image as well as patient information should be managed carefully. In this proposed method graph coloring steganography technique is used along with cryptography to increase level of security.

Generally hiding information is done by steganography and watermarking[2]. Steganography is used to transmit information which is known by sender and receiver whereas watermarking is used for the protection of information. It has two types, visible and invisible watermarking. Invisible watermarking is a steganography technique which is used to hide patient information in medical images.

Steganography can be done in two ways that is either in spatial domain or in frequency domain. Frequency domain steganography is fully based on image transform coefficient. Some of the popular different transforms which are used in frequency domain are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Contourlet Transform (CT).

Spatial domain steganography is a weak technique whose content can be modified when the cover image is corrupted. Integrity of the images which has been transmitted can be verified using spatial domain information hiding techniques.

Wong[3] proposed a method in which public key watermarking method is used in spatial domain to check the image integrity. In this method embedding is done on the basis of secret key which is designed by the sender and known to receiver to extract the embedded message. If intruders try to extract with random key then output is noise instead of message.

An improved method in[4] involves a two dimensional block that uses a longer m-sequence. In this method the information is extracted by comparing the original cover image with the stego image. Errorsoccurring during transmission can be easily found by simply comparing those images.

Walton[5] proposed a method in spatial domain as Least Significant Bit (LSB) algorithm in which information is embedded in the LSB of each pixel. The Most Significant Bit (MSB) of the pixel is used to find the checksum which is used to check the integrity of the image which is transmitted.

Bouslimi[6] proposed a method in which cryptography and watermarking are performed together for the security of image as well as data. During the embedding stage both cryptography and watermarking are done simultaneously but during extraction both are performed separately. In this method message bits are added with the help of a code book. This proposal is a slow method that ensures more security and image reliability.

SHA-1 algorithm employed by Hajjaji et al.[7] generates digital signature to concatenate hospital data and patient information. This concatenated information is embedded in the particular portion of the medical image by identifying its edge through edge detection technique.

J. Fridrich[8] method is based on lookup table. In this method patient information is embedded in the LSB of each pixel of the image by matching with the lookup table. It shares secret key with the receiver to generate lookup table for extracting the message. Since this method is very much sensitive to noise it is impermeable to a block analysis attack.

Fridrich modified above method9 used 64×64 block cipher instead of lookup table which opposes block analysis attack. In this method embedding is done by choosing a 32×32 block from the cover image. It requires more computation for choosing pixels from their commensurate block.

Lim et al.[10] proposed a web based method in which a web server is used to check the integrity and authenticityof the image being transmitted. Message bits are embedded in LSB of pixels. Once the bits are embedded the image is converted into watermarked image. When it is uploaded to the web server, server starts detecting the watermark. If extracted watermark does not match with original a warning message is displayed.

Thiyagarajan[11] used graph colouring to generate the secret key for embedding of data in medical images. But sometimes Region of Interest (ROI) of two medical images have the same number of pixels so the key generated for both images are same. The patient information is embedded in the medical imagesas plain text,so once the intruders get the information they can easily understand the text information.

Mritha Ramalingam and Nor Ashidi Mat Isa[12] improve data security over video images using a steganography approach based on random key encoding function. Secret data is hided in the Red Green Blue (RGB) pixels value of video images with the help of encryption key.

B. Srinivasan et al.[13] used an algorithm to divide the cover image into a number of pieces of different size. Secret data is embedded in each segment using randomized secret sharing algorithm. This algorithm provides different patterns for embedding process.

Video steganography by Ramalingam et al.[14] used an algorithm based on Integer Wavelet Transforms (IWT) and Least Significant Bits (LSB) to hide and extract secret data in Red Green Blue (RGB) pixels value of video files.

Haider Ismael et al.[15] presented an audio steganography method based on Lifting Wavelet Transform (LWT) and Least Significant Bits (LSBs) substitution. To increase the level of security, they proposed a simple encryption using dynamic key.

After analysing all these above methods of spatial domain steganography in medical field, some limitations are stated below:

- The keys which are used for embedding and extracting are not strong.
- Same sequence or pattern is followed for embedding all bits.
- Many of the spatial domain steganography are not reversible.
- Two images may have the same key.

In this proposed method all the above limitations have been rectified and it increases the security level by using cryptography before spatial domain steganography.

3. Proposed Method

In this proposed method keys are generated randomly for medical images are different for each image. Each image has a unique graph and by coloring the graph key is generated which is also unique. On the other hand security is strengthened by encrypting the patient information before embedding. Moreover this method is reversible because after extraction of information the cover image is restored without any error in the sensitive part.

The proposed method mainly involves four stages like encryption, embedding, extraction and decryption. Embedding and extraction are followed by region iden-

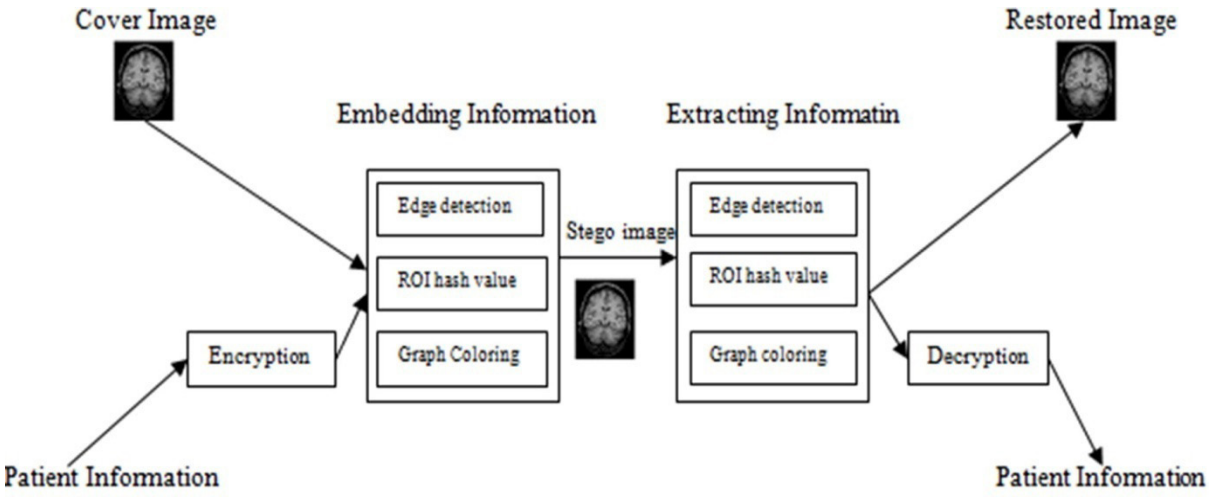

Figure 1. Reversible Steganography Architecture.

tification to separate Region of Interest (ROI) and Non Region of Interest (NROI), Hash value calculation from ROI and Graph identification to generate key. Figure 1 shows the system architecture of the proposed method.

3.1 Region Identification

All medical images have two parts ROI and NROI. While diagnosis needs only ROI partwhich is very sensitive part in medical images. Even a little change in ROI is not acceptable for diagnosis so this region needs to be highly preserved. Remaining portion is non region of interest which can be used to hide the patient information.

Using edge detection technique we can separate ROI and NROI. Various edge detection methods are there like[16] Gabor filter, Canny Edge Detector and Marr-Hildreth edge detector to distinguish ROI and NROI. In digital images points are identified by these methods at which the brightness of the image changes and separate the region. In this paper Gabor filter and Canny Edge Detector are used to extract the feature. The proposed method is implemented in Java. Figure 2 shows the region of interest and non-region of interest using Gabor filter on a brain image. White and black parts are used to separate the ROI and NROI.

Figure 2. Separated ROI and NROI.

3.2 Hash Value Calculation from ROI Region

Hash value is calculated only for the region of interest. It can be done in two steps.

- Count the number of pixels in ROI.

ROI = (p_1, p_2, p_3,....,p_n).

p indicates pixel and n indicates number of pixel of image.

- After counting apply MD5 hash function to ensure the security

Hash Value = MD5($\sum_{i=1}^{n}$ pi).

Pixels count is used to generate the key for embedding and extraction. Table 1 which contains graph index and graph represented as array in embedding and extracting module. Bipartite graph is used in the experiment to generate key. In shared table graph is represented as Gr,n where r, n indicate the root vertices and number of leaf node respectively. Graph is decided for the medical images based on its pixel count. Graph index is obtained from the pixel count and number of entries in shared table (n_e). Graph index is calculated as:

Graph index = (Hash value) mod 'n_e'.

Table 1. Shared table between sender and receiver

Graph Index	0 1 2 3 4 5 - - n-1
Graph $G_{r,n}$	$G_{2,20}$ $G_{2,22}$ $G_{2,25}$ $G_{3,20}$ $G_{3,24}$ $G_{3,28}$ $G_{2,30}$ $G_{2,32}$ $G_{1,35}$

Based on the calculated graph index graph is decided from shared table for given image. As the number of entries is more in shared table different graphcan be obtained for different images. Number of vertices increase the toughness of key which is explained in next section.

3.3 Graph Identification and Coloring the Graph to Generate Key

Count the NROI and ROI pixels which are used to find the hash value and graph index. With the help of graph index graph can be obtained from the shared table to generate key by coloring the graph. Graph coloring algorithm has the following advantages such as key need not to be transferred, no need to store the key in database and more toughness to generate key. Coloring of vertices are done in such a way that the adjacent node should

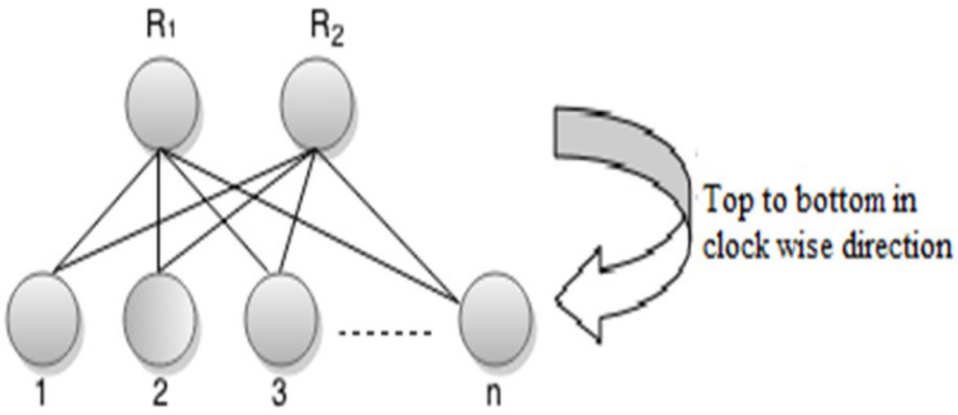

Figure 3. Coloring of vertices from top to bottom in clock wise direction.

not have the same color. It can be done in many ways but the same procedure must be followed in both embedding and extracting side. Three colors (0, 1, 2) are used to color the vertices from top to bottom in clock wise direction as shown in Figure 3. First of all the vertices are assigned with 0 if 0 is not possible then 1 and finally with 2 which is described in algorithm.

3.3.1 Algorithm to Generate Key

Input: Graph.
Output: Key.

Begin

- Color all the vertices (Vi) of graph in order (0, 1, 2) $1 \leq i \leq n$ where n is number of vertices from top tobottom in clockwise direction.
- Color (Vi) ≠ Color of Connected (Vi).
- Pattern P = Sequence of color (Vi)from top to bottom in clockwise direction after coloring all vertices.
- Resultant pixel (RP) = |Number of ROI Pixels - Number of NROI Pixels|
- K = (RP) mod 3.
- Key = KPK where K ∈ (0, 1, 2).

end.

Once all the vertices are colored then the sequence of colors from top to bottom in clockwise direction is taken as Pattern (P). After and before P add one color either of (0, 1, 2) based on the difference of ROI and NROI pixels with mod 3 to generate key and this will result dynamic key for embedding and extracting.

3.4 Encryption

The patient information is encrypted to cipher text using encryption algorithm. In this paper RSA algorithm is used to convert the patient information into cipher text before embedding.This algorithm was given by Rivest, Shamir and Aldeman in year 1977. In[17] used product of two prime numbers to generate public and private key and further these keys are used as encryption and decryption key. Following steps are performed in RSA algorithm:

Step 1. Select two prime numbers, x and y. Consider $n = x \times y$.

Step 2. Calculate f (n) as f (n) = (x - 1) (y - 1).

Step 3. Choose a number e such that $1 < e < f(n)$ randomly and relatively prime to f (n).

Step 4. Find a number d as d = e-1 (mod f (n)).

Step 5. Encrypted text c = me(mod n).

m - Indicates plain text.

3.5 Embedding

ROI portion is highly sensitive so NROI pixels are used to hide the patient information such as patient id, name, age, address and doctor's name. ROI pixel should not be changed during transmission for proper diagnosis. Hash value of ROI is embedded in the NROI pixel to make sure that there is no change in the pixel of ROI. Hash value is embedded in the pixels of NROI which follow the series as A, A+d, A+2d, ...A+(n-1)d to reduce the computation cost.

A - First pixel count to embed hash value.

d - Difference between pixels count.

n - Number of pixels to embed all hash value.

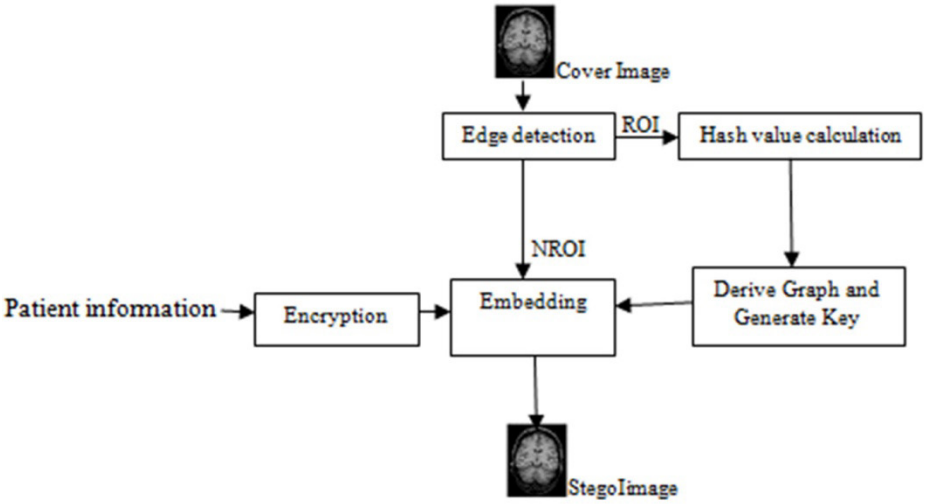

Figure 4. Embedding Process.

The pixels in which hash value is embedded will not be used to embed the patient information. Remaining pixels are assigned with color of the key in a sequential way. Even though key values areassigned to pixels are sequential, embedding is not sequential because some pixels which are assigned with 0 is free from embedding. One bit of information is embedded in the pixel where the pixel value is 1 and two bits if pixel value is 2. When all the bits of information are embedded then cover image is converted to stego image. Figure 4 shows the embedding process for reversible steganography using graph coloring with encryption.

3.5.1 Algorithm for Embedding

Input: Medical image, key, Patient information.
Output: Stego image.

Begin

- Embed hash value in NROI Pixel in series A, A+d, A+2d,… A+(n-1)d where A is first number within the NROI pixel's count, d is the common difference and n is the number of pixels needed to embed hash value.
- Encrypt and convert information into bits.
- For i = 0 to m, j = 0 to n where m, n are the number of rows and columns in NROI until all bits are embedded.
- All pixels are assigned with key's value in rotation way except the pixels embedded with hash value.
- If pixel's value is 0 then no change, if 1 then embed one bit and if 2 then embed two bits of information end.

3.6 Extraction

At receiver side the user extracts the patient information from the stegoimage. As discussed earlierthe ROI and NROI are detected in the medical image using edge detection. Edge detected in both original medical image and stego image are similar which is shown in Figure 5.

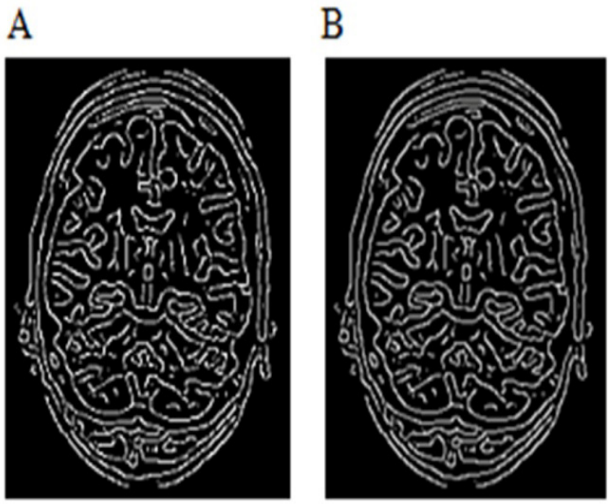

Figure 5. Edges of (A) Cover image and (B) Stego image containing patient information.

After receiving stego image the user checks the integrity of image for any error occurred during transmission. If any error found in the medical image then a warning message is displayed and extraction is continued. Transmission error is checked by comparing the hash value of ROI with the extracted hash value from NROI pixels. If more than half of the extracted hash value is same as ROI hash value then the error is negligible. If more than half of extracted hash value is different fromthe ROI hash value then there is an error in ROI and key generated from graph is wrong and the extracted information is junk data.

Hash value is calculated from ROI pixels. With the help of hash value graph index is calculated and then graph is selected for respective graph index from shared table. Extraction key is generated by coloring the selected graph. It maintains confidentiality because only receiver can generate key from the graph. Figure 6 shows the extraction process of the proposed algorithm.

3.6.1 Algorithm for Extraction

Input: Stego Image.
Output: Patient Information, Cover Image.

Begin

- Separate ROI and NROI, count their pixels and calculate hash value.
- Extract hash value from NROI and match with calculated hash value if does not match more than half then display warning message.
- Generate key and assign key's value to NROI pixels in same way as embedding.
- Extract two bits if pixel's value is 2, 1 bit if Pixel's value is 1 and no extraction if pixel's value is 0.

end.

3.7 Decryption

The extracted patient information isdecrypted to make it readable form. The key which is used for encryption using RSA algorithm is also needed for decryption.

After extraction cipher text is decrypted by $m = c^d \bmod n$.

4. Performance Analysis of Proposed Method

The proposed method has been implemented in Java. The performance of proposed algorithm has been measured in the terms of computational complexity in generating the key and the quality measure ofthe image after embedding the data in terms of PSNR and MSE. The testing of proposed method is done onmany medical images asshown in Figure 7.

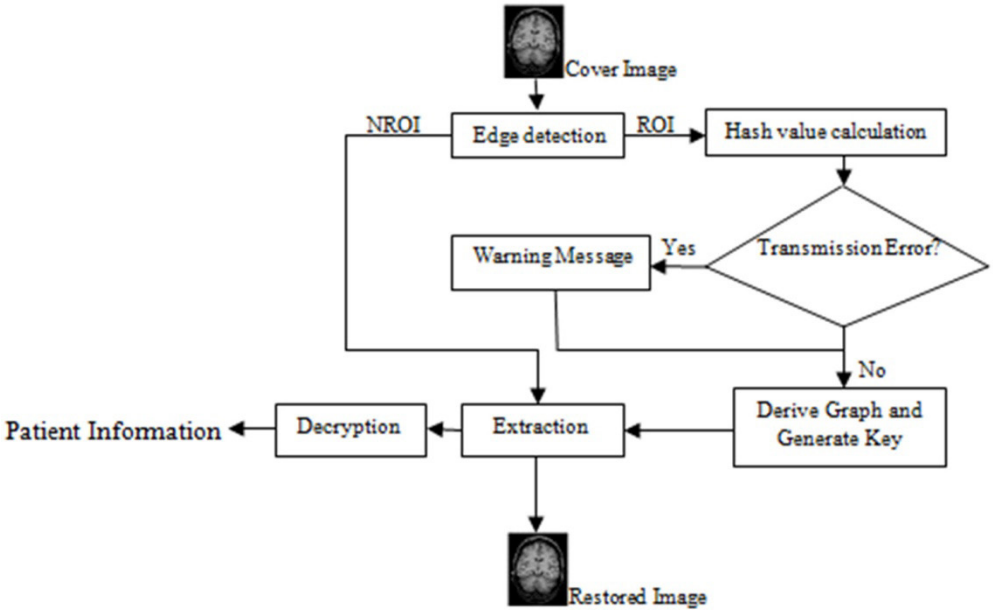

Figure 6. Extracting Process.

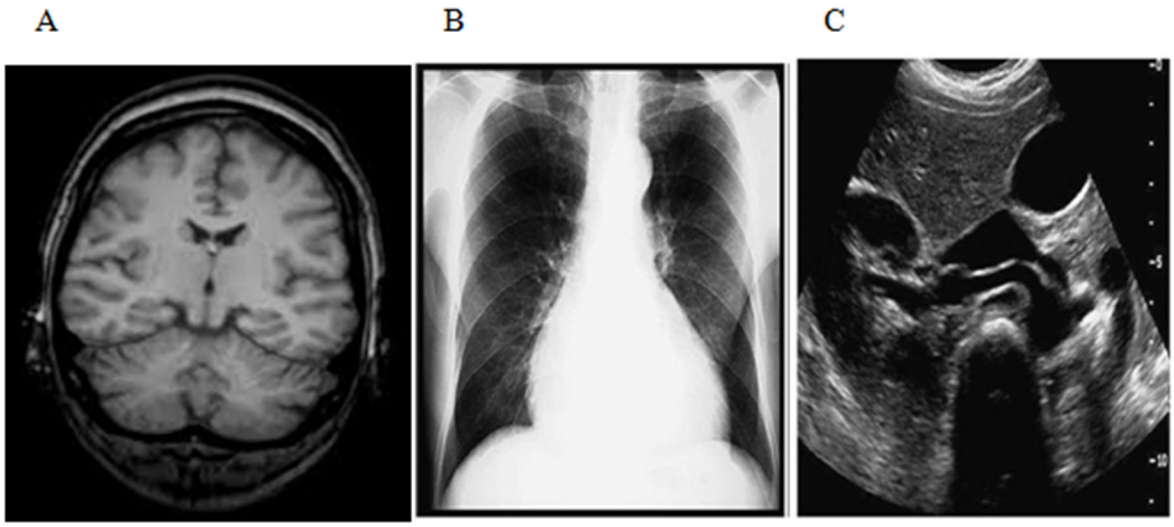

Figure 7. Tested medical images. (A) Brain, (B) Lungs and (C) Kidney.

4.1 Computational Complexity in Generating Key

The number of ways in which a graph can be colored with given color is termed as chromatic polynomial. In proposed method bipartite graph is used as it has more Chromatic Polynomial (CP) it is not easy to crack.

Case 1: 1 root vertex (R_1), n leaf nodes, and C colors then R1 can be color in C ways and n leaf nodes can be color in (C-1) ways, so CP = $[C\times(C-1)^n]$ ways.

Case 2: 2 root vertices (R_1,R_2), n leaf nodes and Ccolors then there are two methods to color.

- Both root vertices with same color then it will follow what we discussed in case 1 that is root (R_1 and R_2) can be color in C ways and n leaf nodes can be color in (C-1) ways. So CP when root assigned with same color = $[C\times(C-1)^n]$ ways.
- Both root vertices with different color then R_1 can be color in C ways, R_2 in (C-1) ways and leaf nodes can be color in (C-2) ways. So CP = $[C\times(C-1)^n]+[C\times(C-1)\times(C-2)^n]$ ways.

4.2 Quality Measure of Image after Embedding

To check the medical cover image whether any change has occurred after embedding of patient information. In NROI region n number of bits can be embed but in this paper only important information about the patient is embedded and tested. Parameters like PSNR and MSE are tested for 450-1250 bits to make sure that there is negligible change in the cover image after embedding of patient information.

4.2.1 Peak Signal to Noise Ratio (PSNR)

The quality of receivedstego image is checked with PSNR value. Generally if the PSNR value of stego image more than 30 db then the quality is considered to be good. In this paper with proposed method all PSNR value are greater than 70 db. Figure 8 shows the calculated PSNR between cover image and restored image after extraction for different medical images.

4.2.2 Mean Square Error (MSE)

It shows the cumulative square mean error between the stegoimage and cover image. The proposed algorithm givesstego image for which MSE value calculated and observed that there are negligible differences which liebetween 0 to 0.018. Table 2 shows the test result of PSNR and MSE.

5. Comparison of Proposed Method with Previous Arts

The proposed method is compared with existing steganography algorithms from literature survey shown in Table 3. Previous methods like Thiyagarajan and Aghila[11], Bouslimi[6], Walton[5], Hajjaji et al.[7] are compared with proposed algorithm. The parameters like computational complexity, reversible steganography, quality of stego image and fully dynamic key are discussed and tested.

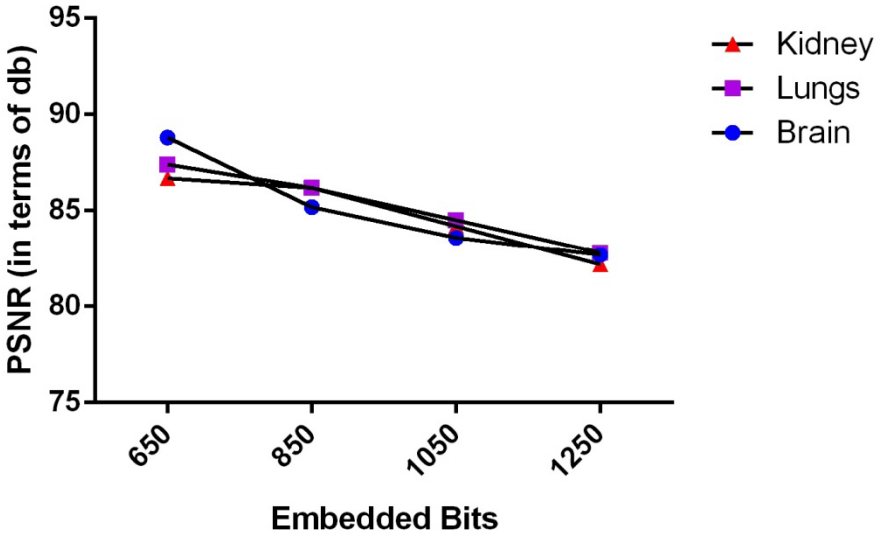

Figure 8. PSNR value of restored image with respect to cover image.

Table 2. PSNR and MSE value for tested medical images

Medical Image	Number of Bits Embedded	PSNR (db)	MSE
Brain	450-650 650-850	80.46 78.62	0.002 0.004
Lungs	850-1050 1050-1250	74.36 72.96	0.008 0.01
Kidney	450-650 650-850	76.72 75.82	0.015 0.018

Table 3. Comparison of proposed method with other steganography methods

Parameters	Algorithm				
	Thiyagarajan and Aghila	Bouslimi et al.	Walton	Hajjaji et al.	Proposed Method
Domain	Spatial	Spatial	Spatial	Spatial	Spatial
Fully/Partial Dynamic Key	Partial	No	No	No	Fully
Reversible Algorithm	Yes	No	No	No	Yes
Following same Pattern	No	Yes	Yes	Yes	No
Transmission Error Tested	Yes	Yes	Yes	Yes	Yes

In this paper the proposed algorithm is dealing with pixels so it comes under spatial domain steganography. The uniqueness of proposed algorithm is that it does not follow any pattern or sequence to embed the data and the key is dynamic generated by graph coloring. On the other hand no need to transfer the key to receiver side. After extraction of information, cover image is restored withoutany error which ensures the reversibility of the algorithm.

6. Conclusion

Reversible steganography technique is proposed by using the fully dynamic key generated with the help of pixels and graph coloring. This proposed method recovers the cover image losslessly after extraction of patient information. Various parameters like computational complexity of key generation by unauthorized person and the change in quality after embedding the information show better result as compared with other methods. Future enhancement of this method is to test with pathology and other types of medical images and increase the level of security by encrypting medial image.

7. References

1. McEvoy FJ, Svalastoga E. Security of patient and study data associated with DICOM images when transferred using compact disc media. Journal of Digital Imaging. 2009; 22(1):65–70.
2. Petitcolas FA, Anderson RJ, Kuhn MG. Information hiding - A survey. Proceedings of the IEEE. 1999; 87(7):1062–78.
3. Wong PW. A public key watermark for image verification and authentication. IEEE Proceedings of International Conference on Image Processing (ICIP'98); 1998.
4. Wolfgang RB, Delp EJ. A watermark for digital images. IEEE Proceedings of International Conference on Image Processing; 1996.
5. Walton S. Image authentication for a slippery new age. Dr Dobb's Journal-Software Tools for the Professional Programmer. 1995; 20(4):18–27.
6. Bouslimi D, Coatrieux G, Cozic M, Roux C. A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Transactions on Information Technology in Biomedicine. 2012; 16(5):891–9.
7. Hajjaji M A, Mtibaa A, Bourennane E-B. A watermarking of medical image: Method based "LSB". International Journal of Computer Science Issues. 2011.
8. Fridrich J, editor Image watermarking for tamper detection. IEEE Proceedings of International Conference on Image Processing (ICIP'98); 1998.
9. Fridrich J, Goljan M, Baldoza AC. New fragile authentication watermark for images. IEEE Proceedings of International Conference on Image Processing; 2000.
10. Lim Y, Xu C, Feng DD. Web based image authentication using invisible fragile watermark. Proceedings of the Pan-Sydney Area Workshop on Visual Information Processing; 2001. p. 11.
11. Thiyagarajan P, Aghila G. Reversible dynamic secure steganography for medical image using graph coloring. Health Policy and Technology. 2013; 2(3):151–61.
12. Ramalingam M, Isa NAM. A steganography approach over video images to improve security. Indian Journal of Science and Technology. 2015; 8(1):79–86.
13. Srinivasan B, Arunkumar S, Rajesh K. A novel approach for color image, steganography using nubasi and randomized, secret sharing algorithm. Indian Journal of Science and Technology. 2015; 8(S7):228–35.
14. Ramalingam M, Isa NAM. Video steganography based on integer Haar Wavelet Transforms for secured data transfer. Indian Journal of Science and Technology. 2014; 7(7):897–904.
15. Shahadi HI, Jidin R, Way WH. Lossless audio steganography based on lifting wavelet transform and dynamic Stego Key. Indian Journal of Science and Technology. 2014; 7(3):323–34.
16. Nadernejad E, Sharifzadeh S, Hassanpour H. Edge detection techniques: Evaluations and comparison. Applied Mathematical Sciences. 2008; 2(31):1507–20.
17. Kota C M, Aissi C. Implementation of the RSA algorithm and its cryptanalysis. ASEE Gulf-Southwest Annual Conference on Session-IVB4; Lafayette: The University of Louisiana; 2002 Mar.