Application Of LSB In Medical Images

Archana Gupta

Department of Computer, Research Scholar, Singhania University, Pacheri Bari, Disstt. Jhunjhunu, Rajasthan, India.
Email: archana.ag51@gmail.com

ABSTRACT: To easily access of medical information,maintain electronic record and high fidelity and also avoid misinterpreted tele-diagnosis we are adopt a steganographic technique of Least Significant Bit for embed the string in the digital medical image.While uses of medical image offer distinct opportunities of improving healthcare access,delivery and standards,security protection of the images.Experimenal results show that proposed schemes provide us large data hiding capacities along with very high PSNR values as compare to exiting data hiding technique.Critically ill or injured patients can be treated locally by effective and secured communication between remote hospital and distance specialist.

Keywords : LSB,Bit,Pixel,Images,String.

1 INTRODUCTION

east significant bit insertion is a common, simple approach to embedding information in a cover image.The Least Significant Bit in other word the 8-bit of some or all of the bytes inside an image is changed to a bit of the secret message.Least Significant Bit steganography has been used; he has no way of knowing which pixels to target without the secret key. LSB makes use of BMP and GIF images, since they use lossless compression when using a 24-bit image, a bit of each of the red,green and blue colour component can be used,since they are each represented by a byte.In other words, one can store three bits in each pixels. A GIF image cannot have a bit depth greater than 8, thus the maximum number of colours that a GIF can store is 256.GIF images are indexed images where the colours used in the images are stored in a palette, sometimes reffered to as a colour lookup table.Each pixel is represented as a single byte and the pixel data is an index to the colour palette.The colours of the palette are typically ordered from the most used colour to the least used colours to reduce lookup time. GIF images is that should one change the LSB of a pixel,it can result in a completely different colour since the index to the colour palette is changed.If adjacent palette entries are similar, there might be little or no noticeable change, but should the adjacent palette entries be very dissimilar, the change would be evident.One possible solution is to sort the palette so that the colour differences between consecutive colours are minimized.Another solution is to add new colours which are visually similar to the existing colours in the palette.This requires the original image to have less unique colours than the maximum number of colours.In a 8 bit grayscale GIF image,there are 256 different shades of grey.The changes between the colours are very gradual, making it harder to detect. The quality of image with reference to the original image can be measured with Mean Square Error to indicate that minimum MSE acceptable degradation ,Peak Signal to Noise Ratio around 50db is acceptable limit.Normalized correlation coefficient used to measure the authenticity and Structural Similarity Index Measure the similarity between two images. Human eye cannot notice the changes in the LSB change of the image.With this concept images are used to hide the secret information.Randomly selecting the pixels in the image and replacing the ASCII values of the text are highly unbreakable algorithm of steganography to make the image steganography robust. Image is the collection of pixels or set of pixels. The smallest component of a digital image is called pixel.Each pixel has own coordinates.Number of row and column gives the dimension of the image. The number of bits in a colour scheme called bit depth,refers to the number of bits used for each pixel.The smallest bit depth in current colour schemes is 8, meaning that there are bits used to describe the colour of each pixel.Monochrome and grayscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey.Digital colour images are typically stored in 24 bit files and use the RGB colour model,also know as true colour.All colour variations for the pixels of a 24 bit .Images are derived from three primary colour:R,G,B and each primary colour is represented by 8bits. Thus in one given pixel,there can be 256different quantities of RGB,adding upto more than 16 million combinations,resulting in more than 16 million colours.Not surprisingly the larger amount of colours that can be displayed. So, that's why we used digital images because different shades of colour is presented and in which the area of greater data diversity when we select the pixel and replace it with message bit no one can easily detect it because different shades of colour undercover the original shades.

2 Review

In which (2013) Ramaiya , et al., using steganography technique like LSB 2-bit,DES 64-bit,16 round,S-Box 6-bit as input and 4 bit output , 4*16 definition tables, 0-15 decimal values.The general conclusion that arises from the result is that high level of security is provided and variation in two LSB of each pixel will not affect the cover image quality.But small modification to an S-Box could significantly waken DES. In which (2013) Samidha and Agrawal using steganography technique like LSB Raster Scan, Random Scan ,Layout Management , Spatial Domain.The general conclusion that arises from the result is that pixels can be used to hide data.Technique can be extended at any place in image using any dimension of any shape. In which (2012) Mare, et. al., using steganopgraphy technique like LSB: 9LSBs RGB images,payload adaptation.the general conclusion that arises from the result is that stronger steganographic model.Size of jump table for extraction is reduces and leaves more space for secret data but jump table cannot be store in nosy areas. In which(2012) Pevny, et. al., using steganography technique like Linear least –square regression,Support vector regression, Quantitative steganalysis,LSB.The general conclusion that arises from the result is that able to construct quantitative steganalyzers for stego systems for which no quantitative attacks exited but not provide high accuracy. In which (2012) Sanchez,et. at., using steganography technique like LSB MLA: GA and PR algorithm.The general conclusion that arises from the result is that sending the message and receiving the original message are treated equally but need to improve the

safety of sending the X matrix.

In which(2012) Selvi,et. al., using steganography technique like LSB: LSBM and LSBMR,edge detection.The general conclusion that arises from the result is that recovered sent message through noisy channels like binary symmetric channel. In which (2012) Zheng , et. at., using steganography technique like LSB :Replacement and Matching , Software identification,Steganography detection.The general conclusion that arises from the result is that variety of steganography software can reliably identify based on LSB steganography algorithm but difficult to find more steganography software's with fewer templates and difficult to transform a better form of intermediate code.

3 Proposed Method/Technique

In order to achieve an adaptive algorithm we consider the following features of the embedding function:

1. Pixel Selection for embedding the data.
2. The bit representation of the Message.
3. Modification of the Cover.

To select the area of greater data diversity, analyze the region and proposed the algorithm. There is no particular algorithm for LSB technique,as it depends on how many LSB's you want to use for storing the secret message and the relative size of the secret message compared to cover image. LSB based steganographic techniques either change the pixel value by +1 or -1 or leave them unchanged.This is dependent both on nature of hidden bits and the least significant bit of the corresponding pixel values. The basic idea of LSB insertion is to embed information in the LSB of the image pixels.A digital image consists of a matrix of colour and intensity values.In a typical gray scale image,8 bit/pixel are used.In a typical full colour image,there are 24 bit/pixel , 8bits assigned to each colour component.The simplest steganographic techniques embed the bits of the message directly into the LSB plane of the cover image in a deterministic sequence.In this technique the amplitude of change is small so modification can not easily detect.LSB embedding also allows high perceptual transparency.

4 Conclusion

Good imperceptibility and sufficient data capacity are two properties which should be possed by all the steganography technique.In which LSB insertion, least significant bit of every byte is altered to form the bit string representing the embed ded file. Altering the LSB will only cause minor changes in colors.

Acknowledgment

My express thanks and gratitude to all departments personal and sponsors who give me a opportunity to present and express my paper on this level.I wish to place on my record my deep sense of gratitude to all reference papers authors for them valuable help through their papers,books and websites. etc.

References

[1] S.Mahato, D.K.Yadav and D. A.Khan," A modified approach to text steganography using hypertext markup language," Advanced computing and Communication technologies (ACCT), 2013 3rd International Conference on 6-7 April 2013, page(s): 40-44.

[2] M..K..Ramaiya ,N.Hemrajani,"and A.K. Saxena, "Improvisation of security aspect in steganography applying DES ," Communication systems and network technologies (CSNT), 2013 International Conference on 6-8,April 2013,page(s): 431-436.

[3] Dr. D. Samidha and D. Agrawal,"Random image steganography is spatial domain,"Emerging trends in VLSI, embedded system,nano electronics and telecommunication system(ICEVENT), 2013 International Conference on 7-9Jan 2013,page(s): 1-3.

[4] S.F. Mare,M.Vladutiu and L.Prodan ,"High capacity steganographic algorithm based on payload adaptation and optimization,'Applied computational intelligence and informatics (SACI) ,2012 7th International Symposium on 24-26 May 2012,page(s) : 87-92.

[5] T.Pevny,J. Fridrich and A.D. Ker,"From blind to quantitative steganalysis,"Information forensics and security,IEEE transcations on (Vol:7,Issues:2) April 2012,page(s):445-454.

[6] A.Sanchez , A.conci,E.Zeljkovic,N.Behlilovic and V.Karahodzic ,'A new approach to relatively short message steganography,"Telecommunications(BIHTEL),2012, IX International Symposium on 25-27 Oct.2012,page(s):1-4.

[7] G.K.Selvi,L.Mariadhasan and K.L.Shunmuganathan,"Steganography using edge adaptive image ,:Computing , Electronics and Electrical Techonologies (ICCEET), 2012 International Conference on 10-12 Oct. . 2012,page(s): 1023-1027.

[8] Y.Zheng , F.Liu,X.Luo and C.Yang ,"A method based on feature matching to identify steganography software,"Multimedia information networking and security (MINES) , 2012 4th International Conference on 2-4 Nov. 2012,page(s): 99-994.