Application Of Steganography In Medical Images

Archana Gupta

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

ABSTRACT: Medical records of patients are extremely sensitive information ,needing uncompromising security during both storage and transmission.In addition , these records often have to be traceable to patient medical data such as X-ray or Scan (CAT,MRI etc.) images.While numerous security tools that hide the information and prevent unauthorized access to the data exits,the possibility of hiding the very existence of these records,using image steanography , in discussed in this paper.An improved version of a high capacity data hiding scheme, called least significant bits(LSB).This paper present securing the transmission of medical images.The presented algorithm will be applied to images. Confidential information are commonly stored in digital media and transmitted via internet due to the rapid growth of internet.If the information in images is altered then this may lead to wrong assumptions.Certain medical applications require information exchange over an insecure network where a small piece of medical information is modified intentionally for certain illegal purpose which may lead to wrong diagnosis.Therefore protection of integrity ,reliability and confidentiality of the secret medical data in images are the important issues.To protect the secret medical information steganography techniques can be used where the secret medical data is altered,even if the attackers get to know the data it was not be of any use without knowing algorithm.

Keywords: Data Hiding, Data Embedding,Steganography,Cryptography.

1 INTRODUCTION

steganography is the art and science of invisible communication..It is play an important role in information security.It deals with embedding information in a given media without making any visible changes to it.It is a technology that hides a message within a object. For this security purpose we proposed watermarking technique for authentication of medical image.Medical image watermarking means embedding the patient information in the medical image.Watermarking increase the storage compatibility and avoid storing of multiple information etc.. In image steganography the information is hidden exclusively in images.Three different aspects in information hiding system contend with each other: Capacity, Security and Robustness.

Capacity: the amount of information that can be hidden in the cover medium.

Security: refer to eavesdropper inability to detect hidden information.

Robustness: to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Steganography algorithms to be robust against either malicious or unintentional changes to the images. The most powerful steganographic algorithms thus posses the ability to embed information in any type of file.This also solves the problem of not always being able to find a suitable images at the right moment,in the right format to use as a cover image. Adaptive steanography with a high embedding capacity and low distortion is an attractive topic in the area of information hiding. Digital steanography is the art of invisibility hiding data within data.It conceals the fact that message exits by hiding the actual message. In this secret data can be hidden inside the image, text, sound clip which can be represented in binary. Cryptography differ from steganography in the senses that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the exitence of an message secret.Cryptography is a visible communication. The process of embedding information into another object/signal can be termed as watermarking.It is used to provide copyright protection and also robustness against various attacks.It is a procedure of embedding data into a multimedia element like image, audio, video. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal. Invisible watermarks do not change the signals to a perceptually great extent i.e. there are only minor variations in the output signal. A digital watermark is an unnoticeable signal added to digital data known as cover work.Data to be inserted as watermark can be of text and image type,it is hidden in such a way that intruder can not detect it properly.

2.1 Review Stage

In which (2013) Alam and Ishan using steganography techniques likes SDS,ATMED,ATMAV ,MED.And other technical details like colour quantinization 256 colours ,240 blocks,RGB components-3bit R,2-bit G,3-bit B componethe accuracy of the transmitted data,safe, secure image data transformation and to authenticate the sender SDS is efficiently incorporated.But PSNR ration performance is not very much good and not effective for standard dataset. In which (2013) Geeth, et al., using steganography techniques like LSB 262,144-bits,Edge Detection Method,Multiple Edge Detection :Gaussian filter,2-dimensional convolution filter,Multiple Error Replacement ,Variable Embedding Ratio.The general conclusion arises from the result is that good visual qualities and higest embedding capacity with high security. In which (2013) Jose and Abraham use Steganography technique like Image Encryption, Chaotic Sequence, Pseudorandom number.The general conclusion that arises from the result is that providing higher data hiding capacity. In which (2013) Kadam,et,al., using steganography techniques like AES:128-bit key,32-bit words,128-bit cipher key,LSB Experimental design:like Intel core i3 at 2.27GHz,4GB RAM nt.The general conclusion that arises from the result is that prevent transformation of secret file from third party access,Increased data security level and keys of description process is protected from the heckers.But memory required for implementation should be small as possible. In which (2012) Manoharan using steganography technique like LSB, RS analysis,Low colour images.The general conclusion that arises from the result is that effective in all cases such as random embedding with LSB replacement and random embedding for sequential for LSB matching but technique only applies to synthetic images with a small number of distinct colours such as logos and flags and it is not effective for big sizes images. In which (2012) Mare et. al., using steganography technique like LSB : 9 LSBs 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) Penvy,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) Zhou, et. al., using steganography technique like LSB, AES: 128-bit.The general conclusion that arises from the result is that provide significant benefits upon sequential distribution and more secure method but much costly. In which (2011) Mandal and Ghatak using steganography technique like LSB (2,2) Visual cryptography , SITMSVC. The general conclusion that arises from the result is that original and regenerated images are same as the evaluated pixel values is position wise same as the original pixel values of the original cover image but degrades the quality of the images.

2.2 Technique for data hiding

DCT: Discrete Cosine Transform Technique

DCT coefficients are used for JPEG compression.Steganography would not be possible to use with JPEG images, since they use lossy compression which result in parts of the image data being altered.One of the major characteristics of steganography is the fact that information is hidden in the redundant bits of the object and since redundant bits are left out when using JPEG it was feared that hidden message would be destroyed.During transformation phase of the compression algorithm,rounding error occur in the coefficient data that are not noticeable.However, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs.

Spread Spectrum Technique

In this technique, hidden data is spread throughout the cover-image making it harder to detect.It is a system for error control coding and image processing to hide information in images. Spread spectrum communication can be defined as the process of spreading the band with of a narrowband signal across a wide band of frequencies.This can be accomplished by adjusting the narrowband waveform with a wideband waveform,such as white noise .After spreading , the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect.In Spread Spectrum image Steganography the message is embedded in noise and then combine with cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image;the embedded image is not perceptible to human eye oe by computer analysis without access to the original image.

Least Significant Bit :

Least significant bit insertiommon , 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 3-bits in each pixels. A GIF image cannot have a bit depth greater than , 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 typical ordered from the most used colour to the least used colours to reduce lookup time. For using GIF image extra care should be taken.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.

2.3 Proposed Method

In our proposed work methodology is exploratory type i.e. gather all type of information about these technique and perform analysis and implement it or implementation and then purpose a mathematical formulation of those result. In our proposed work we will try to find the suitable methods of steganography that can be applied to perform steganography in images.Here we analyzing one by one and purposing an algorithm that will provide the efficient technique after applying various attacks on stego objects and testing the result using PSNR value of the stego object. Compression plays a very important role in choosing which steganographic algorithm to use.Lossy compression techniques result in smaller images file sizes, but it increases the possibilities that the embedded message may be partly lost due to the fact that excess image data will be removed.Lossless compression through, keep the original digital image intact without the chance of lost although is does not compress the image to such a small file size. We are using digital image, so every work is done on pixel of the images.But the formats that are more suitable are those with a high degree of redundancy.Redundancy can be defined as the bits of an object that provide accuracy for greater than necessary for object’s use and display.The redundant bits of an object are those that can be altered without the alteration being detected easily. The number of bits in a color scheme called the bit depth refer to the number of bits used for each pixel.

4 Conclusion

It is necessary to achieve high embedding capacity and visual quality. The important factors that needs to be considered while designing a steganographic system are embedding capacity means number of secret bits that can be embedded per pixel.Visual quality of stego image (i.e image distortion) security and amount of data (compression) shared. So , compression , redundant bit and bit depth make digital image format more stronger than other format .And these factor help in achieving high embedding capacity and visual quality. The basic model of steganography uses a cover object, the secret messge and a steganography algorithm/technique.The outcome of the process is the stego object which is the object that has the secret message hidden inside.This stego object is sent to the receiver where receiver will get the secret data out from the stego image by applying decoding algorithm.

Acknowledgment

We thank everyone who gave support and ideas in brining out

this paper.

REFERENCES

[1] F.I.Alam and M.M.Islam,"An investigation into image hiding steganography with digital signature framework,"Informatics, Electronics and Vision (ICIEV), 2013 international conference on 17-1 May 2013, page(s): 1-6.

[2] C.R. Geeth, S.Basavaraju and Dr. C.Puttamadappa,"Variable load image steganography using multiple edge dectection and minimum error replacement method,"Information and Communication Technologies (ICT), 2013 IEEE conference on 11-12 April 2013, page(s):53-58.

[3] Data Hiding under Fingerprint image modified fast Haar Wavelet based transformation June 2013.

[4] R.Jose and G. Abraham,"A separable reversible data hiding in encrypted image with improved performance,Emerging research areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy (AICERA/ICMICR) 2013 Annual International Conference on 4-6 June 2013,page(s):1-5.

[5] P.Kadam, A. Kandhare , M. Patil,"Separable reversible encrypted data hiding is encrypted image using AES algorithm and lossy technique,"Pattern recognition ,Informatics and medical engineering (PRIME) 2013 International Conference on 21-22 Feb. 2013, page(s): 312-316.

[6] S. Manoharan,"Steganalysis of synthetic low-color images,"Information theory and its applications (ISITA) 2012 International symposium on 28-31 Oct. 2012, page(s): 784-78.

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

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

[9] F.Zhou, R. Yang, Z.Zheng and J.He, "Steganography in multimedia messaging service of mobile intelligent terminal,"Image and Signal processing (CISP), 2012 5TH International Conference on 16-18 Oct. 2012, page(s): 1340-1343.

[10] J.K.Mandal and S. Ghatak,"Secrect Image/Message Transmission through meaningful shares using (2,2) visual cryptography (SITMSVC),"Recent trends in information technology(ICRTIT),2011 International Conference on 3-5 June 2011,page(s): 263-268.