Squint Pixel Steganography: 
A Novel Approach to Detect Digital Crimes 
and Recovery of Medical Images

Rupa Ch., V. R. Siddhartha Engineering College, Vijayawada, India

ABSTRACT
Technology is playing a major role in the rapid growth of Techno media in relation to information security. Tampers are a major handicap while transferring medical images. In order to circumvent these issues used Steganography to hide the information inside a cover medium with different carrier formats. In this paper, the author proposes a novel squint pixel based medical image steganography technique to avoid distortion by an attacker. In this method, Original medical image itself acts as a carrier image. A Medical image segmented into two sets of pixels, Region of interest (ROI) and squint pixels of region of non-interest (RONI). The authentic data and information of ROI of a medical image embedded in penultimate and least significant bits (PLSB) of squint pixels of RONI. Results of experiments on various medical images show that the proposed method produces high quality stego medical images with high accuracy and recovery of ROI data without loss.

KEYWORDS
PLSB, ROI, RONI, Squint Pixel, Steganography

1. INTRODUCTION
Telemedicine has made specialized medical care accessible even to remote and areas. It uses telecommunication and information technology that has helped in reducing the distant barriers as well as communication gap between patients and the medical staff.

Currently, advanced diagnostic methods support distributed client server approach. It allows transmission of medical data from one site to another with confidential interactions. It has held among the communication parities such as patients and medical staff. Maintenance of data integrity is of paramount importance while the Medical images have transferred. This also extends to the protection of medical data from unauthorized users. This one referred as maintaining confidentiality of medical images. Steganography is used to handle the above two concerns.

The steganographic techniques are classified into six categories depending on the cover medium for hiding data in an image, spatial domain, frequency domain, spread spectrum, statistical method, distortion technique and cover method (Abbas, Joan, Keven, & Paul, 2010; Ajit, & Karla, 2013). Based on an application, any one of the file from either text or audio or video or image or protocol can be able to choose as a cover medium. In text
steganography (Bailey, & Curran, 2006, Hardikkumar, 2012), data is embedded into text. In audio steganography (Bailey, & Curran, 2006, Hardikkumar, 2012), the data is embedded into audio files like MP3. In video steganography, the data has embedded into video files. In image steganography, the data embedded into image files like .png, .jpeg. In protocol steganography, data has embedded into network protocol such as TCP/IP. In addition, Image steganography has been applied on medical images (Al-Dmour, & Al-ani, 2016) while transmitting the data for diagnosis.

The key properties of the proposed data hiding system are the embedding capacity, robustness and imperceptibility of an image. Most of the medical images contain two parts called region of interest (ROI) and region of non-interest (RONI). ROI is important as this the particular portion identified by the physician as part of the diagnosis. As such, extreme care has taken while transmitting ROI in order to prevent tampering by unauthorized users, which in turn would affect the diagnosis. In an image, the part other than ROI considered as RONI, which uses to protect ROI data as sensitive information. In this paper, we propose a novel squint pixel based penultimate and least significant bit (PLSB) steganographic technique (Rupa, 2013) with Modified Message Digest (MMD) hash function (13, 14) to achieve the following objectives.

1. To circumvent the two files mechanism such as original file and cover medium in steganographic process to transmit sensitive data (ROI).
2. To Recover original ROI with lossless.
3. To avoid distortion in ROI of steganographic image by not embedding any data inside of ROI.
4. To hide original ROI into RONI with squint pixel technique rather than sequential manner.
5. To facilitate the increase in hiding capacity by using penultimate and least significant bits (PLSB) under imperceptibility property.
6. To incorporate Modified Message digest authentication method to verify whether the data is tampered or not.

The paper deals with the related work in steganography in section 2. In section 3, detailed description on the proposed method and the results discussions were in section 4.

2. RELATED WORK

Till now many security techniques were developed in order to protect the ROI data of medical images from tampering. Most of the techniques focused on how to identify tampered areas inside ROI and how to recover original ROI when any tamper identified. Moreover, maximum hiding techniques use sequential pixels over block based with some simple mathematical calculations approaches. Pouria (Pouria, Mohammed, & Emad, 2004) proposed a method, where the data has embedded into the mean value of number of pixels. If a n-bit data is to be embedded into the image it should have n –blocks and mean value of the ith block should be modified uniformly. Decision table generation is required to embed and to extract the data. The Major drawbacks of this method are as follows. (1) If decision table logic will tamper then it will not be possible to recover the original data. (2) This method does not use any authentication data to cross check whether the image has tampered or not. (3) Imperceptibility property fails if the mean value shows last bit to embed the data.
Development of an Intelligent Patrol Routing System Using GIS and Computer Simulations
www.igi-global.com/chapter/development-intelligent-patrol-routing-system/5271?camid=4v1a