Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Encryption of Medical Images using Steganography for Mobile-cloud- A Survey

Jasmine Kaur
M.Tech Scholar, Department of Computer Science
Punjabi University, Patiala, Punjab, India

Abstract: The resource constrained devices are used for outsourcing the medical images to cloud for selective encryption by using steganography. The visual saliency model is used to detect region of interest from medical images. In the host image the important detected data is embedded. Stego image is produced for encryption by outsourcing to cloud. The image is encrypted by powerful resources of cloud and then sent to client. The selected encrypted region of interest is extracted by client and combined it with non region of interest and then the selectively encrypted image is formed and can be sent to health care centers and medical specialists. The image quality, security and computational complexity are analyzed validate effectiveness. The applicability of monitoring centers in remote patient is verified.

Keywords: Mobile cloud-computing, Image steganography, Selective image encryption, Resource-constrained devices

I. INTRODUCTION

In recent years, smart mobile devices, such as smart phones and tablets, have increasingly become the computing platform of choice. The presence sensors like cameras, GPS systems, microphones, compasses, and motion sensors, make them distinctive from desktop. Video chatting, photo sharing, and location-based services are widely used rely on these sensors. These applications mainly rely on cloud. Smart mobile devices are still resource-constrained in many ways, e.g., battery, storage, network, etc. To significantly expand their capability, cloud technology (driven by leading IT companies equipped with millions of compute-cores and unlimited storage space) has certainly presented a great opportunity to augment the capabilities of mobile devices. Along with these trends, this dissertation focuses on mobile systems and applications that rely on both sensors and cloud infrastructure, which we term "cloud-enabled mobile sensing systems and applications". As we mentioned, many useful cloud-enabled mobile sensing applications already exist that collect, process, and share sensor data.Since smart mobile devices are acquiring more capabilities and can be easily carried everywhere, what people desire to do with their smart mobile devices is also evolving. Users of smart mobile devices are eager to have faster applications with more features and a longer battery life in order to make their lives more efficient and become better connected to one another. However, when processing and sharing sensor data on mobile devices, many unsolved problems currently exist. For instance, it is often hard to efficiently collect, process, or share sensor data. This inefficiency can be caused by high data-rate sensors, such as cameras, due to their data-intensive workloads, the use of smart phone crowds because of human involvement, or the aggressive use of low-quality networks. Thus, without relevant solutions, we will lose opportunities to enable novel applications and quickly be confined within resource limits of mobile devices. Moreover, sharing sensor data with our friends and acquaintances, through the use of social networking websites and other cloud-based services, often reveals users' personal contexts in unexpected ways.

II. NEED OF SECURITY AND PRIVACY OF MEDICAL DATA

The captured medical data is very sensitive and transmission of such data over the public network 'Internet' is vulnerable to many security issues. To address this problem, a number of chaotic encryption algorithms have been presented, encrypting the entire plain text or image. However, in case of real-time and resource-constrained security applications like WCE, such traditional encryption schemes are not feasible due to their huge computational complexity [1]. To solve this limitation up to some extent, the concept of selective encryption is presented, where only the important data is encrypted, thereby reducing the amount of image data to be encrypted. Although, this solution is effective for various applications, but still numerous resource-constrained devices like smart phones cannot perform such encryptions due to their limited battery power and processing capability [3][4]. In this scenario, the computationally expensive encryption operations can be outsourced to cloud, which has powerful resources in terms of processing, storage, and energy. The main problem with outsourcing the secret data for encryption to the cloud is ensuring the privacy of outsourced data. The level of this sensitivity increases when it is related to medical data such as video frames of WCE [2], X-ray images, and frames of diagnostic hysteroscopy videos [5]. Therefore outsourcing of the important medical data to cloud for selective encryption is a challenging issue especially for resource-constrained devices while maintaining its privacy and security such as smart phones. To tackle this problem, the authors in [4] presented a general-purpose framework for outsourcing an image to cloud for selective encryption while maintaining its security using steganography. Their approach has three main problems:

1) The four MSB planes of the input image are directly taken as important data without mentioning any strong evidence,
2) Considering the four MSB planes as payload directly affects the image quality due to larger size of secret data, and
3) The payload is embedded using a steganographic method in a raster scanning order without considering the relationship between image pixels.

After this [6] worked on similar problem a proposed a framework through mobile cloud server whose major contributions are as below

1) A mobile-cloud assisted framework is proposed for selective encryption of medical images, ensuring the security of sensitive medical data as well as saving the resources of resource-constrained devices.

2) A visual saliency model is used to detect the salient region of interest from medical images instead of blindly using the four MSB planes of the image. This mechanism has three advantages including reduction in the size of important data to be encrypted, saving the resources of cloud, and comparatively high stego image quality due to reduced payload.

3) Depending upon the quality of cover image, the four MSB or all planes of the detected salient object are embedded in a host image using edge-directed steganographic method. The suggested method maintains the image quality by hiding more bits in edgy pixels and less number of secret bits in smooth-area pixels.

We have decided to explore this method further and have chosen steganography of medical images as our research topic. Before going further one needs to understand the topic of image stegnography.

III. MOBILE STEGANOGRAPHY TECHNIQUES

Steganography tries to fool the human eye by making it believe that something is not there when, in fact, it is "Steganography" takes cryptography a step further by hiding an encrypted message so that no one suspects it exists. While steganography and cryptology have for a principal goal to hide messages in a specific channel, mobile steganography goal is to hide information in a file, image or other media in a such a manner no one will suspect the very existence of the hidden data. Moreover, it is able to share those hidden data with a third party outside of an organization in some cases. Whereas in cryptography, the information is scrambled so it is impossible to understand it, unless the proper key is applied [7].

The steganography technique can also be useful in some other areas such as the protection of organizational sensitive data, copyright protection, and preventing e-document forging. The most prominent technique uses are the following.

A. Least Significant Bit (LSB) Steganography in images

The most common technique in mobile devices steganography is the Least Significant Bit (LSB). According to Hosmer, the LSB is "The hiding of data within a digital carrier by slightly altering an insignificant characteristic of the carrier that does not appear to change the standard rendering of the data" [10]. The digital image used in mobile devices steganography are, "...two dimensional arrays of varying intensity levels. For a grayscale image, 8 bits per pixel are used whereas in a color image following RGB model; there are 24 bits/pixel, 8 bits assigned to each color components" [8]. Least Significant Bit (LSB) incorporation is a common method of embedding data in a cover image. The LSB technique replaces the last bit with the message bit. For example, let's assume that a carrier has a 2560x 1440 pixels size image, and has the capacity to store 11,059,200 bits or 1,382,400 bytes' total amount of hidden data capacity. The grid for 3 pixels of a 24-bit image carrier is represented in binary as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011) Let's now assume that we want to hide data which has a capacity of 96 bits. The binary representation of the data that needs to be hidden is 01100000, Which is embedded into the least significant bits of the carrier image, the binary representation of the payload. The resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101101 01100011)

As we can see above, the number was embedded into the first eight bytes of the grid; it should be stressed that only 3 bits needed to be changed which on average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [8]. These changes generally will not be noticeable in an anthropomorphic sense. Thus the message is successfully hidden. The LSB can be implemented easily, which is one advantage of the technique.

There is also an abundance of free applications of the steganographic technique for mobile device available to be downloaded online. However, due to its low robustness and lack of tamper resistance of the LSB, it is highly sensitive to any image action such as cutting, filters, resizing, contrasting, and more. The fact that LSB steganography cannot withstand almost any modification that will cause the hidden message to get lost has caused some to turn their attention to another technique, such as audio.

B. Audio Steganography

Mobile audio steganography cornerstone is being able to add a file or data on a recording without significantly altering the sound itself. Today, mobile devices are capable of using a programs such as Skype, Whatsapp, ChatOn, and Tango (for example). These programs, in most cases, utilize traditional methods of security, therefore are more vulnerable to audio steganography techniques, such as the alteration of sound files in a way to add hidden information. The Internet provides numerous audio applications such as voice query, and voice activated websites. [9] Asserted that there are three prominent embedding data methods in audio. These methods include hiding data in frequency/wavelet domains, in the temporal sphere, and in coded domain.

C. Video Steganography

Video is usually a mix of both sound and image, and therefore audio, and image steganography should be able to be used on mobile video to the incorporate hidden message. So video on mobile devices can be utilized as carrier. While mobile devices can produce videos, there is not much writing or application using video steganography on mobiles devices, because "processing and post-production phases are operations best accomplished on desktops" [10].

A video bit stream consists of variable length codes (VLC) representing different segments of the video. Typically, the video stream is offered in compressed kind, so steganography algorithms need to be decompressed to fit in compressed bit-stream. When the required specificity of steganography algorithms is met, the payload must be hidden within the compressed domain. Watermarking algorithms by

video compression using multiple software is a technique that video steganography can use [11].

D. Text Steganography

Mobile devices can be used to create text. This text can be modified to hide data, by misspellings, font resizes, and spaces/line skipping patterns. Some tools can detect such alterations. Also, a text can contain a secret code that can vary from the distribution of word lengths to the frequencies of vowels and consonants. Finally, the hidden put within the structural flavor of the message, this can be found for instance in e-mails or chats [10]. Text steganography provides a wide range of options for those seeking to hide data; such options include generating a random character, format change of an existing text, altering words within a text, and generating readable texts. The difficulty of text steganography is the absence of redundancy information that exists within image, audio or a video file. Therefore, information can be hidden by introducing changes in the structure of the document without making a noticeable alteration of the output. Any change in a text is easy to spot, which is different from an image or an audio file, where subtle changes can be made. The text file has no need of ample storage space; it is a faster and easier way to communicate [12]

IV. RELATED WORK

In this section we have covered a brief survey of existing literature which used different steganographic techniques.

Samer Atawneh et al. [13] presented a new efficient embedding algorithm in the wavelet domain of digital images based on the diamond encoding (DE) scheme. The proposed algorithm first converts the secret image into a sequence of base-5 digits. After that, the cover image is transformed into the DWT domain and segmented into 2 × 1 coefficient pairs. The DE scheme is used then to change at most one coefficient of each coefficient pair to embed the base-5 digits. Experimental results depict that the proposed algorithm is more efficient in embedding compared to other methods in terms of embedding payload and image quality.

Hedieh Sajedi et al. [14] proposed a method in which the blocks of secret image are compared with blocks of a set of cover images and the image with most similar blocks to those of the secret image is selected as the best candidate to carry the secret image. Using appropriate features for comparing image blocks, guaranties higher quality of stego images and consequently, allows for higher embedding capacity, less delectability and, enhanced security. Based on this idea, in this paper, an adaptive cover selection steganography method is proposed that uses statistical features of image blocks and their neighborhood. Using the block neighborhood information, they prevent appearing virtual edges in the sides and corners of the replaced blocks.

Yi-zhen Chen et al. [15**]** introduced an improved adaptive steganography algorithm SVBA algorithm, which fully analyzes the area statistical properties and adopts HVS features. SVBA algorithm first divides the image into 8*8 blocks and analyzes the mean, variance and entropy value of gray by block, then sets a sensitivity vector for each block with considering HVS features and adjusts the steganography schema dynamically according to the block sensitivity vectors. Simulation experiment results on Matlab7.0 show this algorithm has a balanced performance on efficiency, capacity, imperceptibility and robustness.

Ratnakirti Roy et al [16**]** proposed an object based image steganography technique that utilizes image entropy to segment smooth and textured areas in a cover image and then embed data with a variable data rate high efficiency embedding scheme.

Hyunho Kang et al [17] developed a method for block-based tamper detection steganography that can verify not only forgery but also a cutting attack on a stego image. Moreover, a stego image has better quality and more capacity than some previous steganography works. For verifying the integrity of the secret information, both the previous block and the most significant bits (MSBs) of the current block were used. The number of insertion bits per pixel is determined according to the variance of adjacent pixels. Secret information embedding and extraction are performed by using a block unit in the spatial domain of an image.

Sabyasachi Kamila et al [18] proposed a new method for color image steganography in frequency domain where Discrete Wavelet Transform (DWT) of the cover image is used to differentiate high frequency and low frequency information of each pixel of the image. Proposed method hides secret bits in three higher frequency components making sure that the embedding impact on the cover image is minimum and not centralized in sensitivity domain

Hamad A. Al-Korbi et al. [19] aimed at proposing a high capacity and efficient steganography technique, where binary images, color images, and large text files can be all concealed within a single cover image at the same time using Haar Wavelet transform. A high capacity of about 99% has been achieved using the proposed algorithm, with low mean square error (MSE) and high power signal-tonoise ratio (PSNR). This algorithm is developed with the aid of MATLAB environment. The obtained results from the proposed algorithm have been promising in terms of efficiency, performance, and capacity.

M. Tulasidasu et al. [20] presented a best approach for Least Significant Bit focused around picture Steganography that upgrades the current LSB substitution systems to enhance the security level of concealed data. All current strategies for Steganography concentrate on implanting technique with less concern to the pre-processing, for example, encryption of secret picture. In the proposed work shrouded data is stored into distinctive position of LSB of picture utilizing block division procedure relying upon the secret key. Therefore it is hard to concentrate the concealed data knowing the recovery systems. Peak signal to noise ratio (PSNR) is used to measure the quality of stego pictures. The estimation of PSNR gives better come about in light of the fact that our proposed strategy changes little number of bits of the picture.

Jin-Suk Kang et al. [21] proposed a new method of the adaptive steganography using complexity on bit planes of color image. Applying fixing threshold and variable length, if we insert information into all bit planes, all bit planes showed different image quality. Therefore, we investigated the complexity on bit plane and data, similarity insert information into bit planes. As a result, the proposed method increased the insertion capacity and improved the image quality as compared to fixing threshold and variable length method.

Ali Kanso et al. [22] suggest a new steganographic spatial domain algorithm based on a single chaotic map. Unlike most existing steganographic algorithms, the proposed algorithm uses one chaotic map to determine the pixel position of the host color image, the channel (red, green or blue) and the bit position of the targeted value in which a sensitive information bit can be hidden. Furthermore, this algorithm can be regarded as a variable-sized embedding algorithm.

Constantine Manikopoulos et al. [23] proposed the steganography detection system (SDS), and applied to the detection of block DCT-based steganography in gray-scale images, segmented into 8x8 blocks. The differences in the coefficients of the block DCT transforms of the watermarked and unwater marked images from the original are treated as features. SDS utilizes statistical preprocessing over an observation region of each image that generates feature vectors over the regions. These vectors are then fed into a simple neural network classifier.

REFERENCES

[1] Yang J-J, Li J, Mulder J, Wang Y, Chen S, Wu H, et al. (2015a) Emerging information technologies for enhanced healthcare. Comput Ind 69:3–11

[2] Muhammad K, Sajjad M, Baik SW (2016a) Dual-level security based Cyclic18 steganographic method and its application for secure transmission of Keyframes during wireless capsule endoscopy. J Med Syst 40:1–16

[3] Lv Z, Chirivella J, Gagliardo P (2016) Bigdata oriented multimedia mobile health applications. J Med Syst 40:1–10

[4] Xiang T, Hu J, Sun J (2015) Outsourcing chaotic selective image encryption to the cloud with steganography. Digital Signal Processing 43:28–37

[5] Ejaz N, Mehmood I, Baik SW (2013) MRT letter: visual attention driven framework for hysteroscopy video abstraction. Microsc Res Tech 76:559–563

[6] Muhammad Sajjad; Khan Muhammad;Sung Wook Baik; Seungmin Rho; Zahoor Jan; Sang-Soo Yeo;Irfan Mehmood," Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices." published in Multimedia Tools and Applications (2016), pp 1–18

[7] Badgaiyan, C., Dewangan , A., Pandey , B., Yeulkar, K., & Sinha , a. (2012). A NEW STEGANOGRAPHIC TECHNIQUE: IMAGE HIDING IN MOBILE APPLICATION. International Journal of Advanced Computer and Mathematical Sciences .

[8] Sinha, B. (2013). Comparison of PNG & JPEG Format for LSB Steganography . Retrieved from International Journal of Science and Research (IJSR)

[9] F. Djebbar, B. Ayad, H. Hamam, K. Abed-Meriam, A view on latest audio steganography techniques, in: Proceedings of the International Conference on Innovations in Information Technology, 2011, pp. 409-414.

[10] Caviglione, L., & Mazurczyk , W. (2014, August 27). Steganography in Modern Smartphones and Mitigation Techniques. Retrieved from arxiv

[11] Holey, P., Thakare, A., & Vyawahare, H. (2014). A Secure Data Hiding in Video: A Review.International Journal of Current Engineering and Technology.

[12] Agarwal, M. (2013). TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013, 92

[13] Samer Atawneh; Ammar Almomani ; Hussein Al Bazar;Putra Sumari ; Brij Gupta,"Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain." published in Multimed Tools Application (2016). doi:10.1007/s11042-016-3930-0

[14] Hedieh Sajedi, Mansour Jamzad, "Cover Selection Steganography Method Based on Similarity of Image Blocks", Published in: Computer and Information Technology Workshops, 2008. CIT Workshops 2008, IEEE 8th International Conference on date of Conference: 8-11 July 2008

[15] Yi-zhen Chen, Zhi Han,Shu-ping Li,Chun-hui Lu,Xiao-Hui Yao, "An Adaptive Steganography Algorithm Based on Block Sensitivity Vectors Using HVS Features", published in: Image and Signal Processing (CISP), 2010 3rd International Congress on date of Conference: 16-18 Oct. 2010

[16] Ratnakirti Roy, Suvamoy Changder, "Image Steganography with Block Entropy based Segmentation and Variable Rate Embedding", published in: Business and Information Management (ICBIM), 2014 2nd International Conference on date of Conference: 9-11 Jan. 2014

[17] Hyunho Kang, Keiichi Iwamura, "Image Protection System with Steganography and Authentication", published in: Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on Date of Conference: 27-29 Aug. 2014

[18] Sabyasachi Kamila, Ratnakirti Roy, Suvamoy Changder, "A DWT based Steganography Scheme with Image Block Partitioning", published in: Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on date of Conference: 19-20 Feb. 2015

[19] Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee, Waleed Al-Nuaimy, "High-Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data", published in: Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on date of Conference: 3-5 Nov. 2015

[20] M. Tulasidasu, B.lakshmi sirisha, K. Rasool Reddy, "Steganography Based Secret Image Sharing Using Block Division Technique", published in: Computational Intelligence and Communication Networks (CICN), 2015 International Conference on date of Conference: 12-14 Dec. 2015

[21] Jin-Suk Kang, Yonghee You 1, Mee Young Sung 1, "Steganography using Block-based Adaptive Threshold", published in: Computer and information sciences, 2007. iscis 2007. 22nd international symposium on date of Conference: 7-9 Nov. 2007

[22] Ali Kanso, Hala S. Own, "Steganographic algorithm based on a chaotic map", published in Commun Nonlinear Sci Numer Simulat 17 (2012) 3287–3302.

[23] Constantine Manikopoulos, Yun-Qing Shi, Sui Song, Zheng Zhang, Zhicheng Ni, Dekun Zou, "Detection of block DCT-based Steganography in gray-scale images", published in Multimedia Signal Processing, 2002 IEEE Workshop on Date of Conference: 9-11 Dec. 2002