

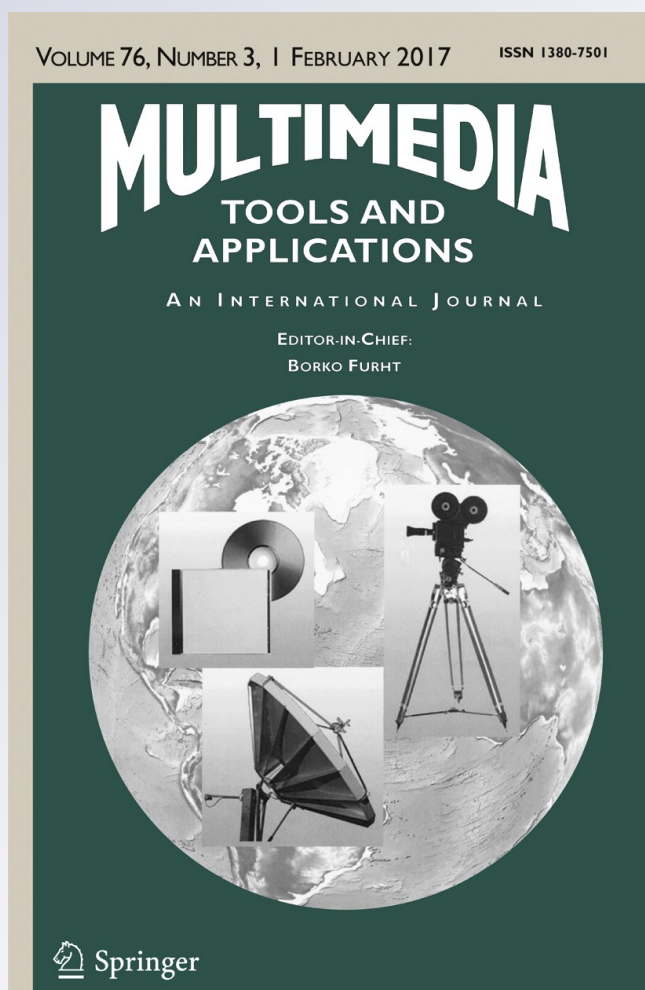
Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices

Muhammad Sajjad, Khan Muhammad, Sung Wook Baik, Seungmin Rho, Zahoor Jan, Sang-Soo Yeo & Irfan Mehmood

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501
Volume 76
Number 3

Multimed Tools Appl (2017)
76:3519-3536
DOI 10.1007/s11042-016-3811-6



Your article is protected by copyright and all rights are held exclusively by Springer Science +Business Media New York. This e-offprint is for personal use only and shall not be self-archived in electronic repositories. If you wish to self-archive your article, please use the accepted manuscript version for posting on your own website. You may further deposit the accepted manuscript version in any repository, provided it is only made publicly available 12 months after official publication or later and provided acknowledgement is given to the original source of publication and a link is inserted to the published article on Springer's website. The link must be accompanied by the following text: "The final publication is available at link.springer.com".

Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices

Muhammad Sajjad¹ · Khan Muhammad²  ·
Sung Wook Baik² · Seungmin Rho³ · Zahoor Jan¹ ·
Sang-Soo Yeo⁴ · Irfan Mehmood⁵

Received: 4 April 2016 / Revised: 12 July 2016 / Accepted: 27 July 2016 /

Published online: 16 August 2016

© Springer Science+Business Media New York 2016

Abstract In this paper, the problem of outsourcing the selective encryption of a medical image to cloud by resource-constrained devices such as smart phone is addressed, without revealing the cover image to cloud using steganography. In the proposed framework, the region of interest of the medical image is first detected using a visual saliency model. The detected important data is then embedded in a host image, producing a stego image which is outsourced to cloud for encryption. The cloud which has powerful resources, encrypts the image and sent back the encrypted marked image to the client. The client can then extract the selectively encrypted region of interest and can combine it with the region of non-interest to form a selectively encrypted image, which can be sent to medical specialists and healthcare centers. Experimental results and analysis validate the effectiveness of the proposed framework in terms of security, image quality, and computational complexity and verify its applicability in remote patient monitoring centers.

Keywords Medical image processing · Image steganography · Visual saliency models · Selective image encryption · Mobile-cloud computing · Information security · Resource-constrained devices

✉ Irfan Mehmood
irfan@sejong.ac.kr; irfan.mehmood@live.com

¹ Digital Image Processing Laboratory, Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan

² Intelligent Media Laboratory, Department of Digital Contents, College of Electronics and Information Engineering, Sejong University, Seoul, Republic of Korea

³ Department of Media Software, Sungkyul University, Anyang, Republic of Korea

⁴ Division of Convergence Computer & Media, Mokwon University, Daejeon, Republic of Korea

⁵ Department of Computer Science and Engineering, Sejong University, Seoul, Republic of Korea

1 Introduction

The recent advancements in sensor technologies have enabled e-health industry to remotely monitor the patients' conditions, thereby improving the patient healthcare. Using the sensor technology, various type of bio-signals and images are produced from the patient's body which are sent to healthcare centers for analysis and monitoring of ongoing medical diagnosis processes [37]. For instance, during the diagnostic process of gait analysis, the medical specialists are interested in measuring various gait parameters such as cadence, swing-stance ratio, step length, and stride width/length using wearable sensors, worn by patients. These parameters are then used in diagnosis of numerous diseases such as stroke, Huntington, Parkinson's disease, and Amyotrophic lateral sclerosis in healthcare centers [8]. Similarly, in case of wireless capsule endoscopy (WCE), a number of images of small bowel are produced by a wireless capsule swallowed by patient [9, 26]. The captured images are stored in an image recording unit which in collaboration with smart phones can be sent to medical center for diagnosis, facilitating them with tele-monitoring [27].

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 [52]. 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 smartphones cannot perform such encryptions due to their limited battery power and processing capability [25, 51]. 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 [37], X-ray images, and frames of diagnostic hysteroscopy videos [12]. In such circumstances, outsourcing the important medical data to cloud for selective encryption while maintaining its privacy and security is a challenging issue especially for resource-constrained devices such as smartphones. To tackle this problem, the authors in [51] 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. This leads to lower image quality and less security for attackers to extract the hidden data.

In this paper, we propose a domain-specific framework for encryption of images in resource-constrained circumstances. The major contributions of this work are summarized as follows:

- i. 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.

- ii. 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.
- iii. 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.

The rest of the paper is structured as follows: The problem is elaborated in Section 2. Section 3 describes the proposed mobile-cloud assisted framework. Experimental results and discussion are given in Section 4. The concluding remarks of the paper and future research directions are presented in Section 5.

2 The problem

In this sub-section, the problem solved by our proposed framework is elaborated. The scenario of the problem is described as follows: A resource-constrained device like smartphone intend to send a medical image to a medical specialist or healthcare center. Since, the medical data is sensitive, therefore, sending it without any encryption is vulnerable to many security risks. Therefore, it is important to encrypt the medical image prior to transmission to ensure its privacy. However, it is not possible for the resource-constrained device to apply high-level encryption on the medical data due to limited battery and processing capabilities. An illustration of the problem is given in Fig. 1.

To cope with this problem, two possible solutions can be considered as follows. 1) The processing and battery capabilities of smart devices can be increased, but it does not seem feasible

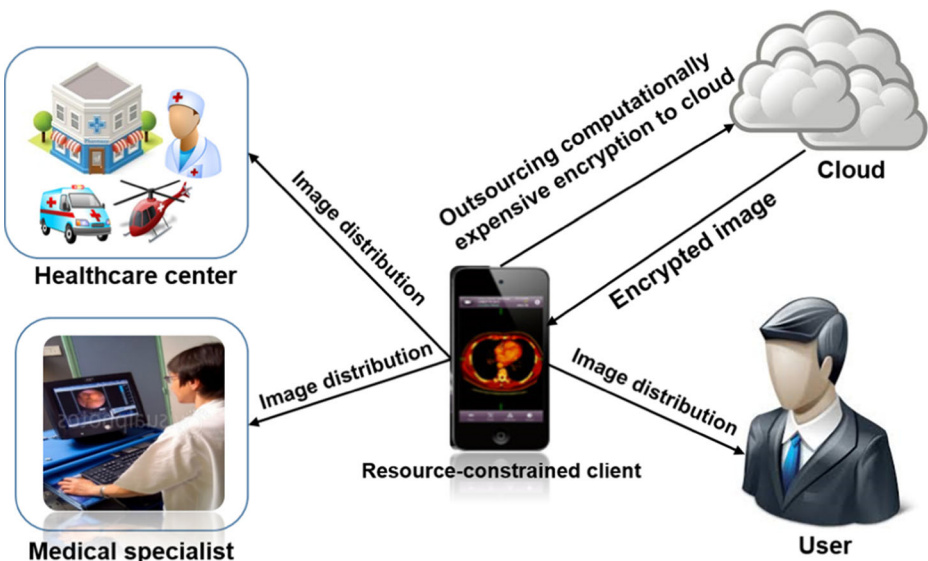


Fig. 1 Illustration of the problem

as the size of smart devices will increase, leading to portability problems. 2) The high-level encryption required for medical data can be outsourced to cloud, which seems the feasible solution for this problem. To ensure the security of medical contents during outsourcing, steganography can be used, making the medical data invisible to naked eye. Based on these motivations, we have proposed a mobile-cloud assisted framework to handle this problem.

3 The proposed framework

The proposed framework addresses the problem of sending a medical image securely from a resource-constrained device to a medical specialist, healthcare center or another concerned user. An illustration of the problem is given in Fig. 1. Our proposed framework solves the mentioned problem using mobile-cloud computing combined with steganography. The mechanism of the proposed framework is three-fold: 1) data preparation, 2) outsourcing encryption, and 3) data distribution. In data preparation stage, the salient object which is considered as an important region of interest (ROI) of the medical image is detected. The ROI is then embedded in a host image using an edge-directed data hiding method. In the second stage, the stego image is outsourced to cloud for selective encryption. The cloud is rich in terms of resources, therefore, high-level chaotic encryption is applied, producing a resultant marked image. Next, the encrypted stego image is forwarded to client. In the last stage, the client extracts the encrypted salient object from the received stego image and combines it with region-of-non-interest (RONI), producing an encrypted medical image. This finally encrypted image is then sent to healthcare centers, medical specialists or any other concerned user. A brief illustration of the symbols and terminologies used in the proposed system are depicted in Table 1. The systematic representation of the proposed system is given in Fig. 2. The main operations of the system are explained in the sub-sequent sections.

Table 1 Illustration of the symbols used in the proposed system

Symbol	Description
I_{Med}	The medical image which needs secure distribution
I_{ROI}	The region-of-interest (ROI) of I_{Med} after saliency detection
I_{RONI}	The region-of-non-interest (RONI) of I_{Med} after saliency detection
I_{MSBs}	The four most significant bit (MSB) planes of I_{ROI}
I_{LSBs}	The four least significant bit (LSB) planes of I_{ROI}
TLEA	Two-Level Encryption Algorithm
I_{EMSBs}	The encrypted MSBs returned by TLEA
K_{DHK}	The data hiding key used in embedding process
I_C	The cover image where I_{EMSBs} are embedded
I_S	The stego image produced after data hiding
Algo1, Algo2	Algo1 and Algo2 are two chaotic algorithms
K_{CEK}	The chaotic encryption key used in chaotic encryption at cloud
I_{ES}	The encrypted stego image returned by cloud to client
K_{EXK}	The extraction key used for ROI extraction from I_{ES}
I_{EMI}	The selectively encrypted medical image to be distributed.

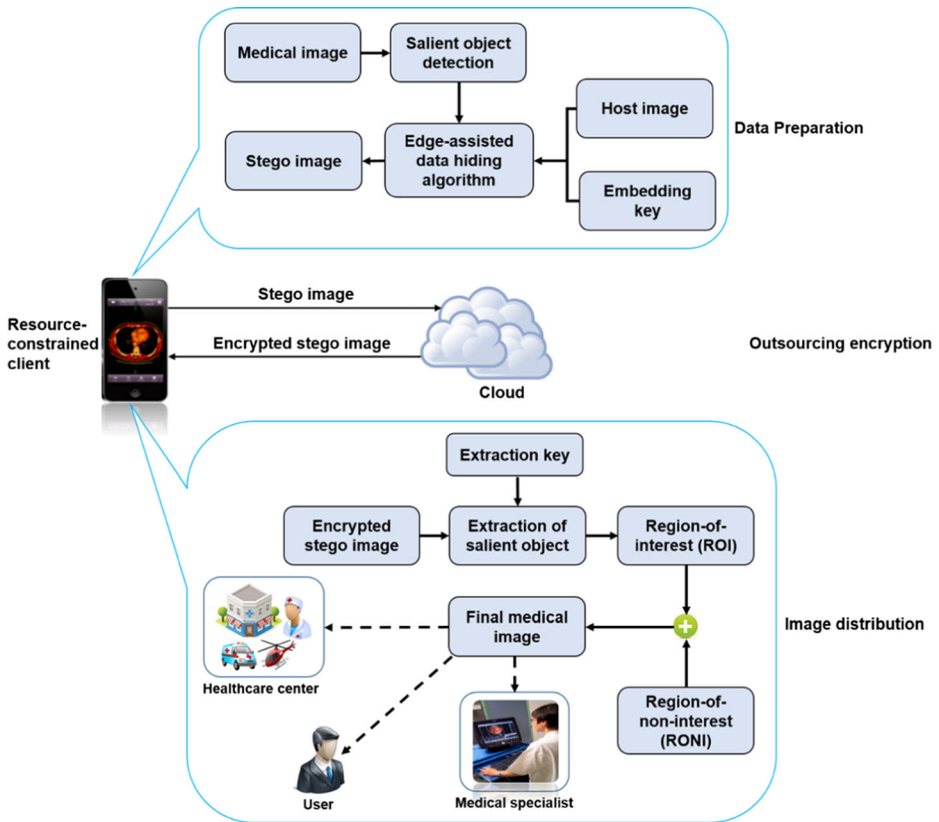


Fig. 2 Framework of the proposed system

3.1 Data preparation

The data preparation stage consists of three main operations including saliency detection of the input image, its light-weight encryption, and embedding of encrypted contents using edge-directed steganographic scheme. The end-result of this stage is a stego image, containing important contents of the medical image. To make clearer the understanding of the basic idea, consider a medical image I_{Med} which needs secure distribution. The first challenge is to find the most important data of I_{Med} . The simplest way to determine the important data is to consider the four MSBs of the input image [50], which is not the feasible solution. The reason is that in medical images, the ROI is more important from diagnostic point of view. Therefore, it is important to identify only the ROI of I_{Med} instead of blindly considering four MSBs. To determine the ROI of the medical image, saliency detection methods can be used [28]. In the proposed work, numerous saliency detections schemes [7, 13, 14] were evaluated. The method presented in [13] was found efficient and effective for salient object detection in medical images, therefore, it is incorporated in the proposed framework. An illustration of the salient object detection using the mentioned technique for a set of images is shown in Fig. 3.

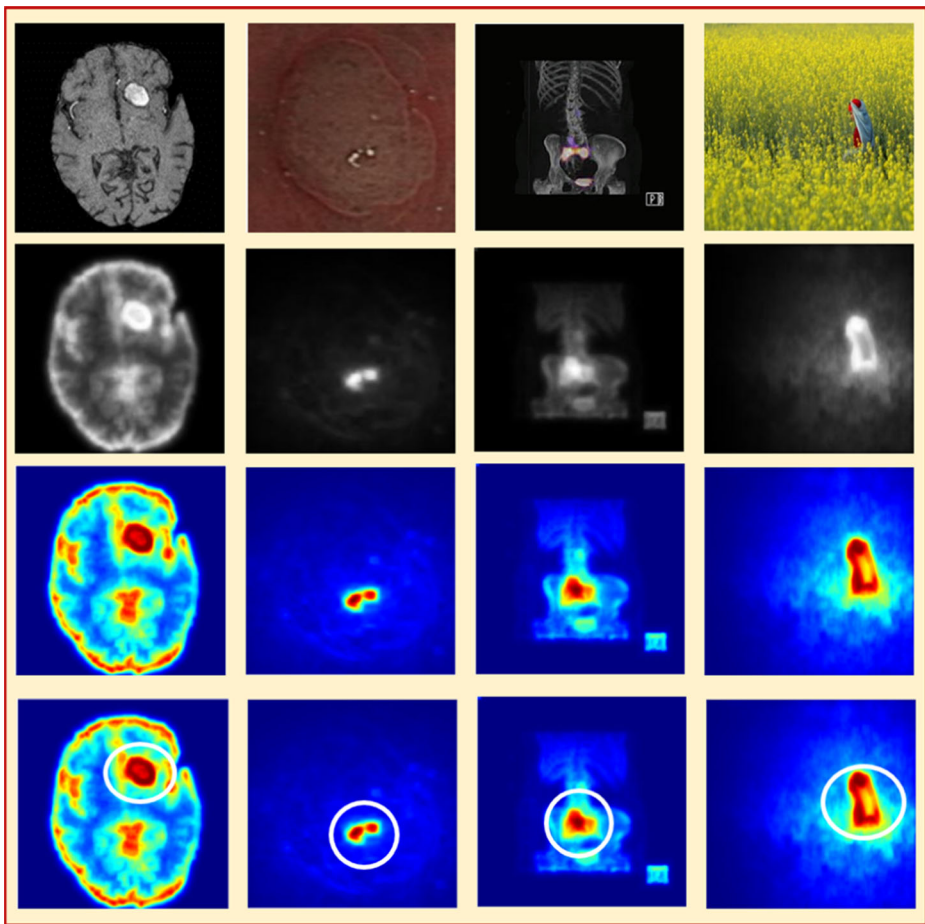


Fig. 3 Illustration of the salient object detection in both medical and natural images. First row (from left to right) shows the input images including MRI, hysteroscopy frame, nuclear, and a natural image (Although, the current work mainly focuses on medical images, yet a natural image is included in experiments with the intention that this framework can also be adopted for natural images). Second row represents the corresponding saliency map of each image. Third row illustrates the color coded saliency (i.e., ROI) of each image is enclosed in a circle with white border

The selected scheme [13] produces I_{ROI} and I_{RONI} as illustrated in Eq. 1. The MSBs and LSBs of the I_{ROI} are then separated as shown in Eq. 2.

$$[I_{ROI}, I_{RONI}] = SaliencyDetection(I_{Med}) \tag{1}$$

$$[I_{MSBs}, I_{LSBs}] = PlaneSeparator(I_{ROI}) \tag{2}$$

To ensure the security, I_{MSBs} are encrypted using our light-weight two-level encryption algorithm (TLEA) [38] as given in Eq. 3. The encrypted contents I_{EMSBs} needs to be hidden in a cover image using steganography. Steganography is the art of embedding a message within a host image without revealing its existence to others [33]. The ultimate goal is to maximize the payload, keeping the image quality intact in a cost effective manner [32]. Recently, researchers have presented numerous image steganographic methods emphasizing on image quality [29,

30, 48], payload [10, 49], reversibility [42], and security [4, 5, 18, 34, 35] such as LSB method [6, 22, 36], cyclic LSB methods [21, 31, 37], pixel indicator techniques [1, 16, 17, 40, 41], and pixel-value-differencing techniques [20]. These techniques utilize the host image pixels without considering pixel relationship during data hiding, thereby equally modifying all pixels which in turn affect the quality of the resultant images. To tackle this issue, an edge-assisted steganography is comparatively more feasible. Therefore, in the proposed framework, the encrypted contents I_{EMSBs} are embedded inside a host image I_C using an edge-directed steganographic method [2] based on data hiding key K_{DHK} as depicted in Eq. 4, producing a marked image I_S .

$$I_{EMSBs} = TLEA(I_{MSBs}) \tag{3}$$

$$I_S = EDDH(I_{EMSBs}, K_{DHK}, I_C) \tag{4}$$

3.2 Outsourcing encryption

It is comparatively difficult for a resource-constrained client to perform extensive powerful chaotic encryption due to limited resources. Therefore, the encryption workload is outsourced to cloud which is rich in processing, storage, and power resources. In the proposed work, the stego image I_S is outsourced to cloud for high-level chaotic encryption. Chaotic image encryption has dramatically drawn the attention of researchers these days for ensuring the security of image contents. It comprises of two main operations: permutation and masking [24, 47]. The former step indicates a multi-dimensional chaotic map, permuting the indices of image pixels. The later operation represents one-dimensional chaotic map, masking the gray-levels of the image. The generic concept of chaotic encryption is illustrated in Fig. 4.

It is worth mentioning that cloud do not know about the hidden data of stego image and therefore treats it as a plain image, proceeding it for high-level chaotic encryption. As mentioned in Fig. 4, the stego image I_S is outsourced to cloud where multi-dimensional chaotic map “*Algo1*” is applied on it, permuting its pixels. Another one-dimensional chaotic map “*Algo2*” is then applied on the result of previous step, masking the pixel values. The initial conditions and necessary parameters of *Algo1* and *Algo2* are supported by chaotic encryption key K_{CEK} . *Algo1* and *Algo2* are two chaotic encryption algorithms to be selected by the client based on his/her requirements. The whole process is illustrated in Eq. 5. The end result of this stage is an encrypted stego image which is returned to client by the cloud.

$$I_{ES} = ChaoticEncr(Algo_1, Algo_2, I_S, K_{CEK}) \tag{5}$$

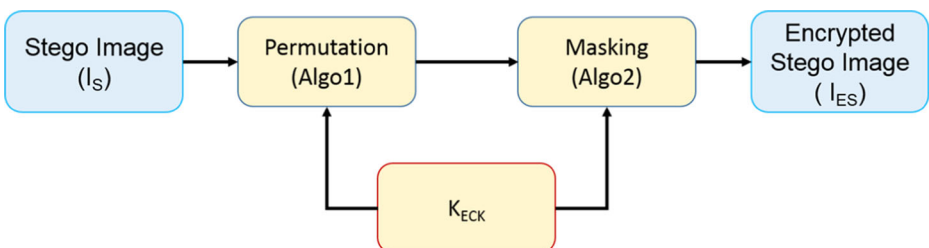


Fig. 4 Generic illustration of chaotic encryption

3.3 Image distribution

In this stage, the selectively encrypted medical image is distributed i.e. sent to healthcare centers, remote patient specialists, and any other concerned user or department. After getting I_{ES} from cloud, the client needs to extract the hidden encrypted contents. Therefore, an extraction algorithm is used to extract the required ROI embedded through steganography as illustrated in Eq. 6.

$$I_{EROI} = ROIExtract(I_{ES}, K_{EXK}) \quad (6)$$

$$I_{EMI} = RegionCombiner(I_{EROI}, I_{RONI}) \quad (7)$$

It should be noted that the extraction algorithm is the exact inverse of the embedding algorithm. To fully recover the hidden contents, an extraction key is used as indicated in Eq. 6. The encrypted ROI is then combined with RONI, forming a selectively encrypted image I_{EMI} as given in Eq. 7. The client can then distribute I_{EMI} in healthcare centers, remote patient monitoring specialists and other concerned users. Overall, the proposed system uses three different technologies: a saliency detection model for identifying important part of the input medical image, steganography for ensuring the privacy of important data during its outsourcing to cloud, and chaotic encryption of cloud for encryption of stego image.

4 Experimental results

This section explains in detail the experiments conducted for the performance evaluation of the proposed framework. The proposed system is tested from different perspectives such as its efficiency in saliency detection, reduction in payload size, and image quality of stego images. Two types of test images are considered for evaluation including medical and cover images. The medical images are taken from IRMA [19] and public image database [43]. For cover images, two other datasets USC-SIPI-ID and COREL are considered [33]. The medical dataset contains images of different modalities such as X-Ray, MRI, CT scan, frames of hysteroscopy videos, and Ultrasound. A set of medical and cover images from both the datasets are shown in Figs. 5 and 6. The size of images were adjusted to 256×256 and 512×512 pixels, depending on the requirement of experiments. For simulation purposes, MATLAB R2015a has been used. The detail of experiments is illustrated in the following sub-sections.

4.1 Payload analysis

In this sub-section, the proposed framework is evaluated from payload point of view. The incurred results for payload are compared with Xiang et al. [51] scheme and embedding of all planes of the ROI of medical images. As payload is the amount of data to be embedded in an image using steganography, therefore, image quality is inversely proportional to payload.

The relationship is described as follows: “the smaller the payload is, the better the image quality is and vice versa”. This clearly indicates that reducing the amount of secret data results in improvement of marked image quality. An analysis of the payload reduction by the proposed scheme is presented in Table 2. The results confirm that the proposed scheme

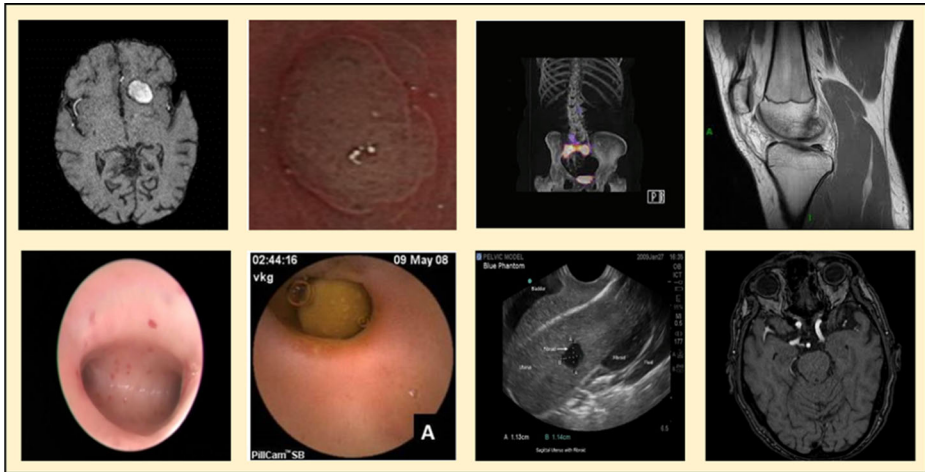


Fig. 5 Sample medical images from the considered medical dataset for performance evaluation. First row from left to right contains MRI, hysteroscopy frame, and two X-ray images. The second row shows a hysteroscopy frame, wireless capsule endoscopy frame, mammography image and MRI, respectively

successfully minimizes the amount of payload, thereby improving the quality of stego images compared to Xiang scheme.

4.2 Saliency detection analysis

In this section, we analyzed the performance of various saliency detection models for region of interest detection in medical images. We have considered three state-of-the-art saliency detection methods including: 1) saliency detection using information maximization (SIM) [7], 2) saliency using covariance features (SCF) [13], and 3) context-aware saliency detection (CASD) [14]. To evaluate the performance of each saliency detection scheme, five images from different modalities were selected. The saliency of each image was then calculated using the given three



Fig. 6 Set of cover images from the dataset for steganographic schemes evaluation

Table 2 Payload analysis of the Xiang scheme and the proposed method

Serial. no	Image modality	Image dimension	Dimension of ROI	Xiang scheme [51]	Proposed method	Decrease in payload (%)
				Payload size (bits)	Payload size (bits)	
1	MRI1	250 × 250	104 × 104	250,000	86,528	65.38
2	X-ray	250 × 247	150 × 150	247,000	180,000	27.12
3	Hyst-Frame	250 × 201	70 × 70	201,000	19,600	90.24
4	MRI2	250 × 250	153 × 153	250,000	187,272	25.09
5	Bird	179 × 250	75 × 95	179,000	57,000	68.15
Average				225,400	106,080	55.20

schemes and their execution time along with detected salient object was noted. An overview of the experimental results for various saliency detection models are given in Table 3.

We then analyzed the performance of all three methods using an evaluation criteria. Our evaluation criteria considers the execution time and correctness of ROI. According to the nominated criteria, we found SCF as the most feasible saliency detection model for the proposed framework due to its better trade-off between ROI detection and execution time as verified by the results in Table 3.

Table 3 Performance evaluation of CASD, SIM, and SCF using execution time and ROI detection

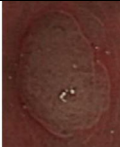


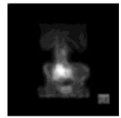
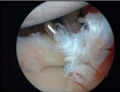
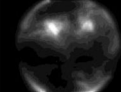
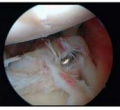
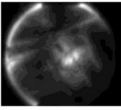

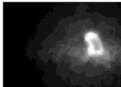
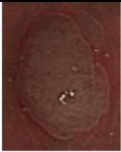



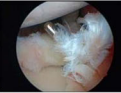
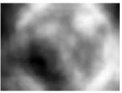
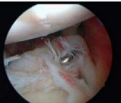
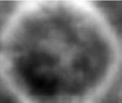


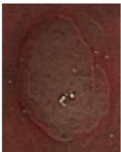
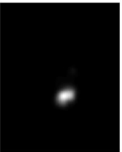

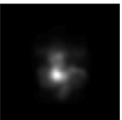

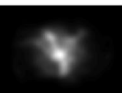

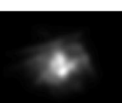


Method Name	Serial. No	Image Modality	Image Dimension	Input Image	Saliency Detection	Execution Time (sec)
CASD	1	Hysteroscopy Frame	250 × 201			40.27
	2	X-ray	250 × 247			131.17
	3	Othoscopic1	174 × 236			21.8726
	4	Othoscopic2	208 × 250			26.4578
	5	Bird	179 × 250			54.91
Average						54.9360

Table 3 (continued)

Method Name	Serial. No	Image Modality	Image Dimension	Input Image	Saliency Detection	Execution Time (sec)
SIM	1	Hysteroscopy Frame	250×201			0.416
	2	X-ray	250×247			0.4122
	3	Othoscopic1	174×236			0.4481
	4	Othoscopic2	208×250			0.8045
	5	Bird	179×250			2.5692
		Average				0.93
SCF	1	Hysteroscopy Frame	250×201			15.1535
	2	X-ray	250×247			15.2421
	3	Othoscopic1	174×236			15.8156
	4	Othoscopic2	208×250			15.2594
	5	Bird	179×250			14.9738
		Average				15.2888

4.3 Summary of overall analysis

In this sub-section, we compare the overall performance of the proposed framework with existing model. The authors in [51] have presented the first general-purpose model for outsourcing an image to cloud for selective encryption. Their model is interesting, however, it contains some problems. Firstly, authors have considered the four MSB planes of the input image directly as important data without any consideration of the image contents. Secondly, considering the four MSB planes as payload directly increases the size of secret information, which consequently affects the image quality. Finally, the steganographic scheme used for data hiding in their model, does not consider the pixel relationship during data embedding, leading to lower quality marked images. These problems make the existing model less suitable for sensitive security applications such as transmission of medical images to healthcare centers and specialists.

In our work, we focused on resolving the problems of this model and verified its applicability for medical domain for the first time. Our framework solves the above issues as follows: To ensure the security of sensitive medical data and save the resources of resource-constrained devices such as smartphone, we proposed a mobile-cloud assisted framework for selective encryption of medical images. We explored visual saliency models to detect the important region of medical images instead of blindly taking the four MSB planes of the image as important data. This mechanism has three advantages: i) reduction in the size of important data to be encrypted, ii) saving the resources of cloud, and iii) comparatively high stego image quality due to reduced payload. This can be verified from the results of Table 2. To improve the stego image quality, the four MSB or all planes of the detected salient object can be embedded in a host image using edge-directed steganographic method, depending upon the quality of cover image. The suggested steganographic scheme hides more bits in edgy pixels and less number of secret bits in smooth-area pixels, maintaining comparatively better image quality.

5 Conclusions

In this paper, a mobile-cloud assisted framework is proposed for selective encryption of medical images, facilitating resource-constrained clients such as smartphone. The framework uses the concept of steganography for keeping the existent of embedded data unrevealed to cloud, hence ensuring the security of sensitive medical data during its outsourcing for encryption. In the proposed method, firstly a saliency detection model is used to detect the region of interest from the given medical image. The detected ROI is then steganographically embedded within a cover image, resulting in a stego image which is outsourced to cloud for high-level encryption. Next, the cloud forwards the encrypted stego image to client where the encrypted important data is extracted and combined with region-of-non-interest, forming a selectively encrypted medical image. This resultant image can be then distributed among healthcare centers, remote specialists, and other concerned users. Through experiments, the following conclusions have been drawn:

1. Considering visual saliency models for detection of important region in medical images is comparatively more feasible instead of directly taking the four MSB planes as important data. This decreases the amount of secret contents that need to be embedded through steganography.
2. The quality of stego images can be improved due to decreased size of secret information because the size of secret data is inversely proportional to the quality of stego images.

In future work, we have intension to explore more saliency detection models to efficiently detect the ROI, thereby further reducing the amount of secret data. We will also focus on using sparse representation for effective data hiding and performance evaluation using numerous quality assessment metrics such as peak-signal-to-noise-ratio, normalized cross correlation, and quality index [53]. In addition, the current framework can be combined with video summarization schemes [3, 11] and other data hiding techniques [23, 44, 45] for secure wireless capsule endoscopy [39] and secure visual contents retrieval for personalized video libraries. Finally, we will explore different defense mechanisms [15, 46] against numerous attacks for our model.

Acknowledgments This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2013R1A1A2061978).

References

1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate Array on RGB indicator. *International Journal of Signal and Image Processing* 1: 196–204
2. Al-Dmour H, Al-Ani A (2016) A steganography embedding method based on edge identification and XOR coding. *Expert Syst Appl* 46:293–306
3. Almeida J, Leite NJ, Torres R d S (2012) Vison: Video summarization for online applications,. *Pattern Recogn Lett* 33:397–409
4. Al-Otaibi NA, Gutub AA (2014a) 2-Layer Security System for Hiding Sensitive Text Data on Personal Computers,. *Lecture Notes on Information Theory Vol 2*
5. Al-Otaibi NA, Gutub AA (2014b) Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority,. *Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014)*:250–256
6. Nouf Alotaibi, Adnan Gutub, and Esam Khan, stego-system for hiding text in images of personal computers, *The 12th Learning and Technology Conference*, 2015.
7. Bruce N, Tsotsos J (2005) Saliency based on information maximization,. *Adv Neural Inf Proces Syst*:155–162
8. Buke A, Gaoli F, Yongcai W, Lei S, Zhiqi Y (2015) “healthcare algorithms by wearable inertial sensors: a survey;” *Communications*. China 12:1–12
9. Chen Y, Lee J (2012) A review of machine-vision-based analysis of wireless capsule endoscopy video. *Diagnostic and therapeutic endoscopy*, vol 2012
10. Chih-Yang L, Chang C-C, Yu-Zheng W (2008) Reversible steganographic method with high payload for JPEG images. *IEICE Trans Inf Syst* 91:836–845
11. de Avila SEF, Lopes APB, da Luz A, de Albuquerque Araújo A (2011) VSUMM: a mechanism designed to produce static video summaries and a novel evaluation method. *Pattern Recogn Lett* 32:56–68
12. Ejaz N, Mehmood I, Baik SW (2013) MRT letter: visual attention driven framework for hysteroscopy video abstraction. *Microsc Res Tech* 76:559–563
13. Erdem E, Erdem A (2013) Visual saliency estimation by nonlinearly integrating features using region covariances. *J Vis* 13:11–11

14. Goferman S, Zelnik-Manor L, Tal A (2012) context-aware saliency detection, *Pattern Analysis and Machine Intelligence*. IEEE Transactions on 34:1915–1926
15. Gupta B, Joshi RC, Misra M (2009) Defending against distributed denial of service attacks: issues and challenges. *Information Security Journal: A Global Perspective* 18:224–247
16. Gutub AA-A (2010) Pixel indicator technique for RGB image steganography. *Journal of Emerging Technologies in Web Intelligence* 2:56–64
17. Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) “pixel indicator high capacity technique for RGB image based steganography,” in *WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications*
18. Gutub A, Al-Qahtani A, Tabakh A (2009) Triple-A: Secure RGB image steganography based on randomization, in *Computer Systems and Applications, AICCSA 2009. IEEE/ACS International Conference on*, 2009, pp. 400–403
19. https://ganymed.imib.rwth-aachen.de/irma/veroeffentlichungen_en.php.
20. Hussain M, Wahab AWA, Anuar NB, Salleh R, Noor RM (2015) Pixel value differencing steganography techniques: Analysis and open challenge,. *Consumer Electronics-Taiwan (ICCE-TW), 2015 I.E. International Conference on*:21–22
21. Khan F, Gutub AA-A, (2007) message concealment techniques using image based steganography, in *The 4th IEEE GCC Conference and Exhibition*
22. Li X, Yang B, Cheng D, Zeng T (2009) a generalization of LSB matching, *Signal Processing Letters*. IEEE 16:69–72
23. Lin C-C, Liu X-L, Yuan S-M (2015) Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping. *Inf Sci* 293:314–326
24. Liu Z, Zhang F, Wang J, Wang H, Huang J (2016) Authentication and recovery algorithm for speech signal based on digital watermarking. *Signal Processing* 123:157–166
25. Lv Z, Chirivella J, Gagliardo P (2016) Bigdata oriented multimedia mobile health applications. *J Med Syst* 40:1–10
26. Mehmood I, Sajjad M, Baik SW (2014a) Mobile-cloud assisted video summarization framework for efficient management of remote sensing data generated by wireless capsule sensors. *Sensors* 14: 17112–17145
27. Mehmood I, Sajjad M, Baik SW (2014b) Video summarization based tele-endoscopy: a service to efficiently manage visual data generated during wireless capsule endoscopy procedure. *J Med Syst* 38:1–9
28. Mehmood I, Sajjad M, Ejaz W, Baik SW (2015) Saliency-directed prioritization of visual data in wireless surveillance networks. *Information Fusion* 24:16–30
29. Mstafa RJ, Elleithy KM (2014) A highly secure video steganography using Hamming code (7, 4),. *Systems, Applications and Technology Conference (LISAT), 2014 I.E. Long Island*:1–6
30. Mstafa RJ, Elleithy KM (2015) A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. *Multimedia Tools and Applications*:1–23
31. Muhammad K, (2015) Steganography: A Secure way for Transmission in Wireless Sensor Networks, *arXiv preprint arXiv:1511.08865*,
32. Muhammad K, Ahmad J, Farman H, Zubair M (2014) A novel image steganographic approach for hiding text in color images using HSI color model. *Middle-East J Sci Res* 22:647–654
33. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2015a) A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimedia Tools and Applications*:1–27
34. Muhammad K, Ahmad J, Farman H, Jan Z, Sajjad M, Baik SW (2015b) A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption,. *KSII Transactions on Internet and Information Systems (TIIS)* 9:1938–1962
35. Muhammad K, Ahmad J, Sajjad M, Zubair M (2015c) Secure image steganography using cryptography and image transposition. *NED Univ J Res* 12:81–91
36. Muhammad K, Mehmood I, Lee MY, Ji SM, Baik SW (2015d) Ontology-based secure retrieval of semantically significant visual contents. *Journal of Korean Institute of Next Generation Computing* 11:87–96
37. 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
38. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2016b) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*:1–30

39. Muhammad K, Ahmad J, Sajjad M, Rho S, Baik SW (2016c) Evaluating the Suitability of Color Spaces for Image Steganography and Its Application in Wireless Capsule Endoscopy. *2016 International Conference on Platform Technology and Service (PlatCon)*:1–3
40. Parvez MT, Gutub A-A (2008) RGB intensity based variable-bits image steganography. *Asia-Pacific Services Computing Conference, APSCC'08*. IEEE 2008:1322–1327
41. Parvez MT, Gutub AA-A (2011) Vibrant color image steganography using channel differences and secret data distribution. *Kuwait J Sci Eng* 38:127–142
42. Qin C, Chang C-C, Huang Y-H, Liao L-T (2013) An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism. *IEEE Transactions on Circuits and Systems for Video Technology* 23: 1109–1118
43. Salvatore M, Margolies L, Kale M, Wisnivesky J, Kotkin S, Henschke CI, et al. (2014) Breast density: comparison of chest CT with mammography. *Radiology* 270:67–73
44. Singh AK, Kumar B, Dave M, Mohan A (2015a) Multiple watermarking on medical images using selective discrete wavelet transform coefficients. *Journal of Medical Imaging and Health Informatics* 5:607–614
45. Singh AK, Dave M, Mohan A (2015b) Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools and Applications*:1–21
46. Tewari A, Jain A, Gupta B (2016) Recent survey of various defense mechanisms against phishing attacks. *Journal of Information Privacy and Security* 12:3–13
47. Wang L, Song H, Liu P (2016) A novel hybrid color image encryption algorithm using two complex chaotic systems. *Opt Lasers Eng* 77:118–125
48. Wu H, Wang H (2013) Multibit color-mapping steganography using depth-first search. *Biometrics and Security Technologies (ISBAST), 2013 International Symposium on*:224–229
49. Wu H, Wang H, Zhao H, Yu X (2015) Multi-layer assignment steganography using graph-theoretic approach. *Multimedia Tools and Applications* 74:8171–8196
50. Xiang T, Wong K-w, Liao X (2007) Selective image encryption using a spatiotemporal chaotic system. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 17:023115
51. Xiang T, Hu J, Sun J (2015) Outsourcing chaotic selective image encryption to the cloud with steganography. *Digital Signal Processing* 43:28–37
52. 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
53. Yang J, Lin Y, Gao Z, Lv Z, Wei W, Song H (2015b) Quality index for stereoscopic images by separately evaluating adding and subtracting. *PLoS One* 10:e0145800



Muhammad Sajjad received his Master degree from Department of Computer Science, College of Signals, National University of Sciences and Technology, Rawalpindi, Pakistan. He received his PhD degree in Digital Contents from Sejong University, Seoul, Republic of Korea. He is now working as a research associate at Islamia College Peshawar, Pakistan. He is also the head of “Digital Image Processing Laboratory (DIP Lab)” at Islamia College Peshawar, Pakistan. His research interests include digital image super-resolution and reconstruction, sparse coding, video summarization and prioritization, image/video quality assessment, and image/video retrieval.



Khan Muhammad received his BCS degree in Computer Science from Islamia College, Peshawar, Pakistan in 2014 with research in information security. Currently, he is pursuing MS leading to PhD degree in digitals contents from Sejong University, Seoul, Republic of Korea. He is working as a researcher at Intelligent Media Laboratory (IM Lab) since 2015. His research interests include image and video processing, data hiding, image and video steganography, video summarization, diagnostic hysteroscopy, and wireless capsule endoscopy.



Sung Wook Baik received the B.S degree in computer science from Seoul National University, Seoul, Korea, in 1987, the M.S. degree in computer science from Northern Illinois University, Dekalb, in 1992, and the Ph.D. degree in information technology engineering from George Mason University, Fairfax, VA, in 1999. He worked at Datamat Systems Research Inc. as a senior scientist of the Intelligent Systems Group from 1997 to 2002. In 2002, he joined the faculty of the College of Electronics and Information Engineering, Sejong University, Seoul, South Korea, where he is currently a Full Professor and Dean of Digital Contents. He is also the head of Intelligent Media Laboratory (IM Lab) at Sejong University. His research interests include computer vision, multimedia, pattern recognition, machine learning, data mining, virtual reality, and computer games.



Seungmin Rho is a faculty of Department of Media Software at Sungkyul University in Korea. In 2012, he was an assistant professor at Division of Information and Communication in Baekseok University. In 2009–2011, he had been working as a Research Professor at School of Electrical Engineering in Korea University. In 2008–2009, he was a Postdoctoral Research Fellow at the Computer Music Lab of the School of Computer Science in Carnegie Mellon University. He gained his B.S degree in Computer Science from Ajou University. He received his MS and PhD degrees in Information and Communication Technology from the Graduate School of Information and Communication at Ajou University, South Korea. He visited Multimedia Systems and Networking Lab in University of Texas at Dallas from Dec. 2003 to March 2004. Before he joined the Computer Sciences Department of Ajou University, he spent two years in industry. His current research interests include database, big data analysis, music retrieval, multimedia systems, machine learning, knowledge management as well as computational intelligence.



Dr. Zahoor Jan is currently holding the rank of an associate professor in computer science at Islamia College Peshawar, Pakistan. He received his MS and PhD degree from FAST University Islamabad in 2007 and 2011 respectively. He is also the chairman of Department of Computer Science at Islamia College Peshawar, Pakistan. His areas of Interests include image processing, machine learning, computer vision, artificial intelligence and medical image processing, biologically inspired ideas like genetic algorithms and artificial neural networks, and their soft-computing applications, biometrics, solving image/video restoration problems using combination of classifiers using genetic programming, optimization of shaping functions in digital watermarking and image fusion.



Sang-Soo Yeo received his master's degree and PhD degree in Computer Science & Engineering from Chung-Ang University, Seoul, Korea. He was a visiting scholar at Kyushu University, Japan. He worked for BTWorks, Inc. as a General Manager, and at the same time was an adjunct professor at Hannam University. He is currently a professor at the Division of Computer Engineering, Mokwon University, Korea. He is President of the Institution of Creative Research Professionals (ICRP), and Vice President of ICT Platform Society (ICTPS). His research interests include security, ubiquitous computing, multimedia service, ubiquitous computing, embedded system, and bioinformatics.



Irfan Mehmood received his BS degree in Computer Science from National University of Computer and Emerging Sciences, Pakistan. He completed Ph.D. degree from Sejong University, Seoul, Korea. Dr. Irfan is Assistant Professor in College of Electronics and Information Engineering at Sejong University, Seoul, South Korea. His research interests include video and medical image processing, big data analysis, and visual information summarization. He is the corresponding author of this paper.