Secure Transmission of Bio-sensor Images for Ubiquitous Healthcare

Anupam Kumar Bairagi, Md. Golam Robiul Alam, Choong Seon Hong*

Department of Computer Engineering, Kyung Hee University, Korea

Email: {anupam, robi, cshong}@khu.ac.kr

Abstract

Ensuring security and privacy in wireless body area networks (WBAN) are one of the challenging research issues in personalized healthcare. The image, signal, video, and textual information produced by the bio-sensors are vulnerable for unauthorized access and patients' privacy. In this paper, we propose an efficient steganography algorithm to hide patients' secret key into the sensor image to protect the sensor images from unauthorized access. We also hide the diagnostic imaging report into the sensor image to ensure patients' privacy in remote patient monitoring and telemedicine. We apply the proposed algorithm in M2A wireless endoscopy sensor images and found the superiority of our algorithm over the existing benchmark approaches in perspective of steganalysis.

1. Introduction

Protecting healthcare data generated by wearable and implantable bio-sensors in BAN is the demand in needs for future ubiquitous patient care technology. The biomedical sensors including micro-sensors and nano-sensors produced images of different affected organs and body parts and also transmits to the sink nodes for further diagnosis, surgery and treatments either locally or remotely. Sometimes the images are stored in a database along with patient's health report electronically that is called electronic health record (EHR) which can be used more conveniently. EHRs can improve the economic competence and performance of the health organizations [1]. Most of the cases, EHRs are kept separate and other stakeholders cannot use that records. To overcome the barrier, these images can be stored in the cloud storage and accessed when necessary by the proper authorities with the help of patient's key.

Privacy is the prime issue in case of medical information in subject to store and access to and from the cloud storage. To secure and ensure the unique identity of each image we embed the patients' secret key into the image through a lightweight data hiding algorithm. We also can hide the necessary diagnostic report into the sensor image to ensure the privacy of patients' without or with minimal changing of least-significant-bits of the sensor images. In this paper we propose an algorithm to hide patient's report into sensor image which could be stored in the cloud storage and information would be extracted from the image with the help of patient's key after accessing from the storage by consultant.

2. Background

Steganography is the method of hiding information within a cover so that it arises no suspicion to the intruders of containing valuable information. When medical information is stored in cloud, it requires good access control mechanism so that unauthorized access can be prohibited. A steganography-based access control model has proposed in [2] for shielding the secrecy of medical data but key management and distribution is the main drawback of the system. A Fresnlet based data hiding method have been proposed in [3] where medical image is concealed in another image. Here robustness is maintained by sacrificing imperceptibility. Depending on Quad and reduced difference expansion (RDE), a medical data hiding method has been proposed in [4] for recovering the original image after extracting data but it produce low quality stego-image. Considering the privacy of patient's information and difficulties with key exchange mechanism, we have used image steganography concept where sensor images are used for carrying medical information and a secret key by the help of the proposed embedding and extraction algorithm with good stego-image quality and robustness.

3. Proposed Method

The working model of the method is shown in the Fig. 1. Here the bio-sensor will capture the patient's image and send to the sink node. The node will conceal a patient key within the image and send to the hospital server. The doctor will make a report depending on the image and hide that report to the image using hiding algorithm and store it in cloud storage. This stego-image can be accessed by consultant or other telemedicine expert and can extract the report from image using extraction algorithm. Lastly he/she can reproduce the report that can again be concealed within the image and can be stored in cloud storage and simultaneously be updated in the hospital server .

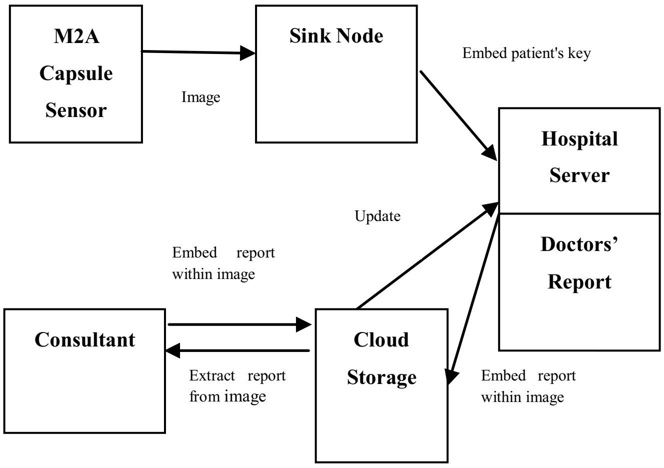


Figure 1 Proposed model

Algorithm 1: Data Hiding

```
initialize MI, MD by using medical image and message to be hidden
        BD by using binary form of the MD
        $P_k$ is the patient's key
        Row, Col, r, c mCounter
while r ≤ Row
    while c ≤ Col
        pos = 2+ (MI(r, c, 3) - LSB(MI(r, c, 3))+$P_k$) mod 7
        if MI(r, c, 1, pos) = BD(mCounter)
            mCounter = mcounter + 1
            LSB(MI(r, c, 1))=1
        else
            LSB(MI(r, c, 1))=0
        endif
        if MI(r, c, 2, pos) = BD(mCounter)
            mCounter = mcounter + 1
            LSB(MI(r, c, 2))=1
        else
            LSB(MI(r, c, 2))=0
        endif
        if MI(r, c, 3, pos) = BD(mCounter)
            mCounter = mcounter + 1
            LSB(MI(r, c, 3))=1
        else
            LSB(MI(r, c, 3))=0
        endif
        if mCounter ≤ Length(BD)
            c=c+1
        else
            exit from both of the loop
        endif
    End of loop
    c=1
    r=r+1
End of loop
```

Algorithm 2: Data Extracting

```
initialize MI by using stego-image
        $P_k$ is the patient's key
        BD, Row, Col, r, c, mC, mCounter, mL
while  r ≤ Row
    while  c ≤ Col
        pos = 2+ (MI(r, c, 3) - LSB(MI(r, c, 3))+$P_k$) mod 7
        if LSB(MI(r, c, 1))=1
            BD(mCounter)=MI(r, c, 1, pos)
            mCounter = mcounter + 1
        endif
        if LSB(MI(r, c, 2))=1
            BD(mCounter)=MI(r, c, 2, pos)
            mCounter = mcounter + 1
        endif
        if LSB(MI(r, c, 3))=1
            BD(mCounter)=MI(r, c, 3, pos)
            mCounter = mcounter + 1
        endif
        if mCounter≤mL
            c=c+1
        else
            exit from both of the loop
        endif
    End of loop
    c =1
    r=r+1
End of loop
while mC ≤mL/8
    ch=BD(8*mC-1:8*mC)
    mD(mC)=ch
    mC= mC+1
End of loop
```

4. Simulation and Evaluation

To assess the algorithm, MATLAB R2010a modules are defined independently for embedding and extraction of data. The experiment is performed on three M2A capsule endoscopy images (JPG) of size 789X800, 800X800, 789X800 collected from [5] using four different amounts (A=35.16, B=42.09, C=57.61, D=62.54 Kilobytes) of data. We have used Steganography Studio 1.0.2 tool for analyzing the images. The peak signal-to-noise ratio (PSNR) and normalized cross-correlation values of the experiment are shown in the Fig. 2 and Fig. 3 respectively.

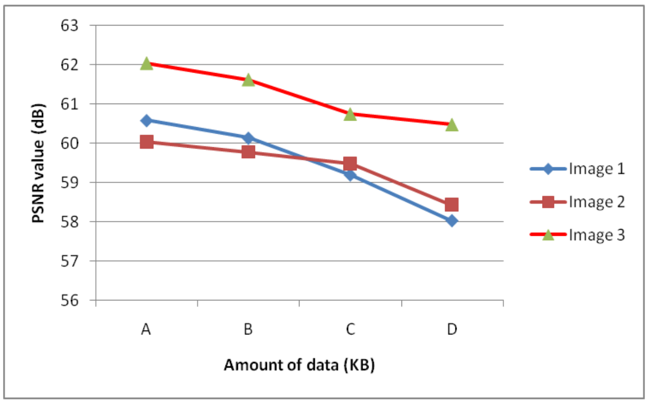


Figure 2 Results of PSNR on different images

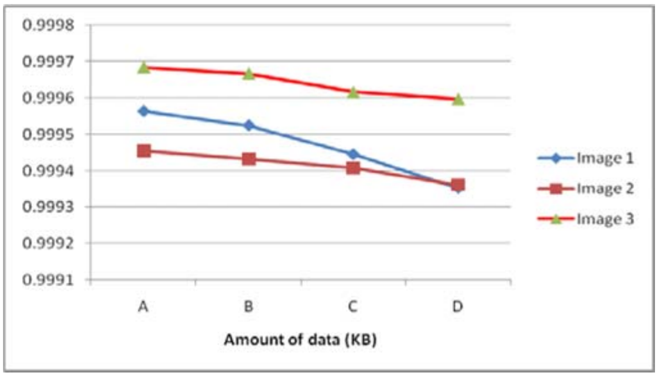


Figure 3 Experimental results of correlation

Fig. 2 depicts the increase of amount of data decrease the quality of stego-image. The lowest value of PSNR value is 58dB that represents good image quality. On the contrary the highest of that in the method [4] is below 40dB which indicates lower stego-image quality. A sample cover image and stego image is shown in the Fig. 4 which indicates no visual distortion between the images. Histogram of images is shown in Fig. 5 which indicates no significant difference between cover image and stego-image.

5. Conclusion

The proposed method has been assessed in terms of imperceptibility and correlation with varying hiding capacity. The experimental results show that the proposed method produces better quality images than the previous method. The system is robust as any of the combination will not produce any meaningful result without the knowledge of private key. The proposed approach can resist visual analysis, histogram analysis. In the future we will try to increase the capacity minimizing degradation of the quality of the stego-image.

Acknowledgement

This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2014-(H0301-14-1003). *Dr. CS Hong is the corresponding author.

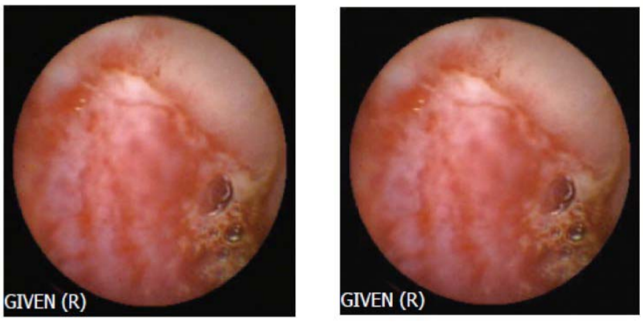
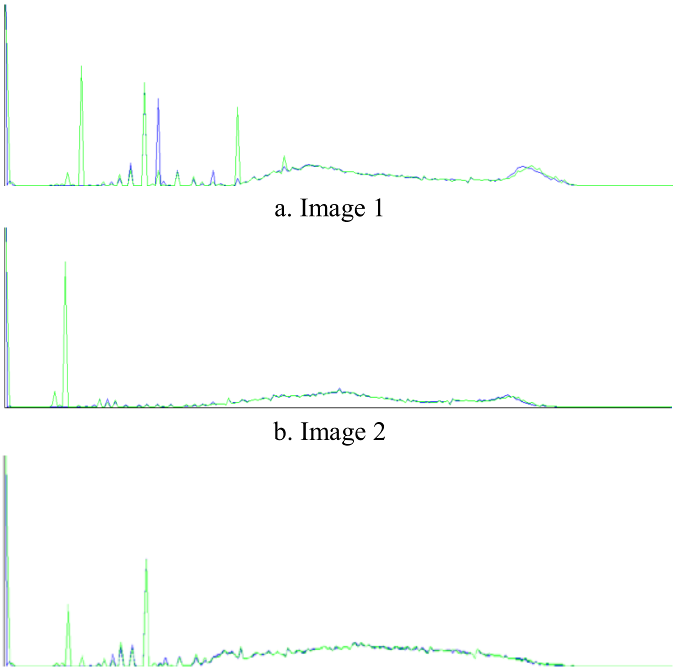


Figure 4 Comparison of cover and stego image



a. Image 1

b. Image 2

c. Image 3

Figure 5 Histogram of cover image and stego-image

References

[1] W. Millard, “Electronic Health Records: Promises and Realities: A 3-Part Series Part I: The digital Sea Change, Ready or Not.”, Annals of emergency medicine, vol. 56, no. 2, p. A17-A20, 2010

[2] V. Mai, I. Khalil, and A. Ibaida,"Steganography-based access control to medical data hidden in electrocardiogram”, 35th Annual International Conference of the IEEE E EMBS, Pp.1302-1305, Osaka, Japan, 3-7 July 2013

[3] M. Nazeer, and D. G. Kim,"A novel Fresnlet based robust data hiding algorithm for medical images", In Imaging Systems and Techniques (IST), IEEE International Conference on IEEE, pp. 213-216., 2012

[4] T. Ahmad, M. Holil, W. Wibisono, and R. M. Ijtihadi, “An Improved Quad and RDE-based Medical Data Hiding Method”, in Proceedings of the IEEE International conference on CYBERNETICSCOM , 2013

[5] O. Ersoy, B. Sivri, Serap Arslan, F. Batman and Y. Bayraktar, "How much helpful is the capsule endoscopy for the diagnosis of small bowel lesions?", World Journal of Gastroenterology, 2006 June 28; 12(24): 3906-39