
Garima Mehta, Amity University, Noida, India
Malay Kishore Dutta, Amity University, Noida, India
Pyung Soo Kim, Korea Polytechnic University, Siheung, South Korea

ABSTRACT

Tele-ophthalmology has gained a lot of popularity as it involves retinal fundus images which can be analyzed for identification of severe diseases like diabetic retinopathy and glaucoma. With this increasing popularity, requirement for medical data confidentiality and privacy has also increased during transmission or storage. To meet this challenge, this paper propose an efficient and lossless cryptosystem based upon chaotic theory for encryption of medical fundus images. In the proposed encryption scheme a strategic combination of scrambling and substitution architecture is proposed which complements each other. The proposed scheme of encryption for fundus images is challenging as these images are 3-D color image and cannot be compressed as compression may not be able to retain all relevant medical information. For performance analysis, the proposed algorithm has been evaluated for perceptual and cryptographic security. The experimental results indicate that the proposed method is lossless and resistant against attacks making the proposed scheme suitable for real time applications.

KEYWORDS
Arnold Cat Map, Chaotic System, Encryption, Piece Wise Linear Chaotic Map, Telemedicine, Tele-ophthalmology

1. INTRODUCTION

In today’s growing health care sector, telemedicine, the art of transfer of medical data over telecommunication channels (Montagnat, 2004; Nayak, 2009; Nayak,2004) for specialized medical expertise and improved patient care is gaining a lot of popularity. Telemedicine offer either offline/online consultation with medical professionals for routine or specialized consultation on current medical health of the patient. Telemedicine may be applied to various types of medical data like MRI, Eco graphic images, X-Ray images, CT scan or retinal images etc. stored in electronic format in the medical databases (Norcen, 2003). These medical databases are specially designed for acquisition and storage of medical image data acquired from the patients worldwide to reduce the wastage of resources or duplicate examinations, analysis and medical health checkups.

One of the budding branches of telemedicine is tele-ophthalmology (Ng, 2009) which enables ophthalmologists to take ocular images to quantify microcirculation for diagnosing diseases like Diabetic Retinopathy and Glaucoma (Helen, 1999). The benefit of using tele-ophthalmology is to diagnose and monitor ophthalmic diseases for the patients living in distant areas. For security and data confidentiality in tele-ophthalmology applications there is a need to create a secure communication...
channel through which retinal images can be transferred. Hence to reduce the security risks, encryption may be introduced in area of tele-ophthalmology. Another reason for encryption of medical data is to provide the medical data confidentiality and accessible to authorized users only (Formazin, 2008). The choice of encryption method employed is very important since conventional cryptography mechanisms like RSA and AES are not suitable for encryption of medical data (Fu, 2013) due to its relatively large size and highly complexity. Further this method doesn’t support real time applications because of computational complexities. To solve these issues different encryption algorithms were developed.

As telemedicine is emerging as powerful technology advancement in the field of health care, the transmission of bulky medical images over the networks has also increased. As transmission networks are vulnerable to security breaches, the need of securing digital medical images is becoming an important concern. Encryption seems to provide an effective way around to prevent the loss of identity of medical images as it maintains confidentiality and integrity of the medical images. Existing work related to encryption of medical data has been done over CT images, X-Ray images, echo-graphic images, mammographic images in chaotic domain (Ashtiyani, 2008; Abokhdair, 2010; Fu, 2013). All these kind of medical images are usually 2-dimensional images whereas retinal images considered in this work are three dimensional color depth images. Moreover, for these retinal images dimensional reduction or compression may not be possible as well as loss of information during encryption and decryption process is undesirable since any loss of information may lead to false diagnosis. Thereby there is a need to develop a lossless and efficient encryption scheme to secure these colored retinal images.

The major contribution is to propose a chaotic based block wise, lossless and efficient cryptosystem that provides a potential solution for securing colored fundus images for transmission via telecommunication channels or storage in the distributed medical infrastructure networks. In the proposed cryptosystem coalition of rearrangement and replacement is done using arnold cat map and piece wise linear chaotic map respectively to achieve the desired level of confidentiality. Arnold cat map is used to scramble the original image into unintelligible format to increase the security, while piecewise linear chaotic map is used for substitution as it has good dynamical and statistical properties which are required for an efficient encryption scheme. This combination which complements each other also increases the key space to enhance the ability to withstand brute force attacks.

Another challenge in this work is unlike existing work of encrypting medical images like CT scan, MRI images, Echo-Graphic images, X-Ray which are gray scale 2-D images, this work is an attempt to encrypt 3 dimensional color fundus images. These images are depth images and have voluminous data this paper propose a strategic efficient and lossless encryption algorithm to encrypt these 3 dimensional fundus images in a block wise manner as compared to full medical image encryption because of its large size which makes it suitable for real time applications in tele-ophthalmology.

The paper is organized as follows. The need for encryption of medical data security and choice of encryption method is described in section 2 whereas section 3 shows the proposed encryption algorithm. Experimental results and security analysis of proposed algorithm are shown in section 4. Finally, the paper is compared with existing research work and hence conclusion is presented.

2. NEED FOR ENCRYPTION OF MEDICAL DATA

In most of the existing work (Ashtiyani, 2008; Abokhdair, 2010; Lavanya, 2012) encryption has been done on medical images like MRI, CT Scan, X-Ray, echo-graphic, mammographic for data confidentiality and patient credentials security and to prevent data modifications. In this paper, encryption of ophthalmological images has been reported. Fundus photography is becoming popular
Systematic Literature Review on Empirical Results and Practical Implementations of Healthcare Recommender Systems: Lessons Learned and a Novel Proposal
[www.igi-global.com/article/systematic-literature-review-on-empirical-results-and-practical-implementations-of-healthcare-recommender-systems/149244?camid=4v1a](www.igi-global.com/article/systematic-literature-review-on-empirical-results-and-practical-implementations-of-healthcare-recommender-systems/149244?camid=4v1a)

User Needs and Limitations of Existing Mobility Devices: A User Perspective
[www.igi-global.com/article/user-needs-and-limitations-of-existing-mobility-devices/211948?camid=4v1a](www.igi-global.com/article/user-needs-and-limitations-of-existing-mobility-devices/211948?camid=4v1a)