Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 538 – 543

Procedia Computer Science

The Second International Symposium on Computer Vision and the Internet (VisionNet'15): Signal Processing, Image Processing and Pattern Recognition (SIPR'15)

A Cryptographic Technique for Security of Medical Images in Health Information Systems

Quist-Aphetsi Kester [a, b, c] *, Laurent Nana[b], Anca Christine Pascu[b], Sophie Gire[b],Jojo M. Eghan[c], Nii Narku Quaynor[c]

[a]*Faculty of Informatics, Ghana Technology University College, Accra, Ghana*
[b] *Lab-STICC (UMR CNRS 6285), European University of Brittany, University of Brest, France*
[c]*Department of Computer Science and Information Technology, University of Cape Coast, Cape Coast, Ghana*

Abstract

Medical image data is a central part of diagnostics in today's healthcare information systems. With the adoption of cloud computing approaches in the healthcare sector by most health institutions, medical image data are now stored remotely in third party servers. Privacy, safety and security needs to be guaranteed for such digital data by engaging encryption to ensure confidentiality and authentication methods to ensure authorship. Encryption and watermarking techniques of digital image data in this domain needed to be completely reversible. The engaged original plain image data in the cryptographic and watermarking methods should be fully recoverable due to the sensitivity of the data conveyed in medical images. In satisfying the recoverability and the authentication process in this paper, we proposed a fully recoverable encrypted and watermarked image technique for the security of medical images in health information systems. The approach was used to authenticate and secure the medical images in health information systems and our results showed to be very effective and reliable for fully recoverable images.

*Keywords:*health information systems; encryption; medical images;safety; privacy; authentication; recoverable

* Corresponding author. Tel.: +33-758-331-092; Tel: +233-209-822-141.
Kester.quist-aphetsi@univ-brest.fr / kquist@ieee.org

doi:10.1016/j.procs.2015.08.070

1. Introduction

Health information systems forms a critical parts of one's countries information technology infrastructure due to the sensitivity and nature of data processed over time with regards treatment history, medical records etc. The safety, privacy and security of health data stored over time can reflect on progress of patients, resistance and adoptability of human to drugs over time and genetic links to causes of diseases over time. Geographical profiling of such data can reflect a lot of information on progress of health, outbreaks, effectiveness healthcare delivery etc. In the health sector medical imaging has become a major part of most diagnostic procedures ranging from x-rays, ultra sound etc and it has dominated major part of a health infrastructure. Advancements in health information systems with emphasis on tele-medical procedures, remote health care services and health cloud storage infrastructures with medical imaging data as a key component in ensuring effective health delivery. The importance and urgency nature of health care services delivery has led to the creation of opportunities in the software development sector. This software application made it possible for health care service delivery to be done with more efficiency and timeliness. Effectiveness in the healthcare sector is crucial in the sense that the organization of medical records in health care facilities provides easy access to records in less time. This has become a major milestone in the heath care sector and has facilitated further advancement in medical technologies in the sector of surgical operations guided by sensors and artificial intelligence and has seen more and more advanced technological diagnostic tools for pre medical procedures that encompasses analysis and examination. A better approach to health care sector has seen a better engagement of imaging technologies as results of advances in research in signal processing and vision of internal body systems. This advancement has a greatly impacted positively on the health sector. Introductions of real-time information systems to the health sector for medical practitioners in real-time surgical operational procedures are revolutionizing how health care services are delivered around the globe. Artificial intelligence techniques such as machine learning, data mining and information retrieval approaches in health care etc has made it easier for causes and treatment of related diseases and adverse effect study of certain medications more effective. More comprehensive and understanding of outbreak of diseases through reports at hospitals geographical profiling has become easy as well. This brings to bear the relevance of Information systems as an integral part of cyber critical systems in today's cyber space. These health systems provide a lot of benefits and make it easy for a timely and effective provision of healthcare services.

With all the above mentioned benefits of health information systems as an integral part of progress in modern society, a compromised health information system can render catastrophic effect to both the host and the clients of such systems. The high increase cyber attacks on cyber critical infrastructure with the health sector was no exception as raised serious concerns about safety, security and privacy issues of information systems. Migration and integration of health information systems' data to third party services for management in a private, public or hybrid cloud can pose a lot of challenges to the privacy, safety and security of the storage of such data. Data security involving safety, privacy and protection are key issues in relations to medical issues in the case of patient and health practitioner relationship. In ensuring effective security, access control is a fundamental to securing information systems including health information systems. The external storage of data in the clouds computing environments engages access control as its fundamental security procedure. Data security engaging advanced cryptographic schemes is very important in safeguarding data in other to prevent it from being understood during a breach in the information system. Effective security approaches are needed in safeguarding the integrity and in securing medical image data in the cloud and for health information systems. Verification procedures through authentication approaches are needed in accessing medical data for confidentiality purposes. But these approaches of securing medical images have to less computational time, be reversible and have recoverability of data during the entire procedure of ensuring security within the system due to sensitivity nature of the image data and the importance of the information conveyed by the data in the image and hence a loss of data values in the process will pose a lot of problem. In providing effective solution to part of the challenges confronting health information systems involving data safety, privacy and security, we proposed an approach for medical images. We combined the techniques of cryptography and watermarked and achieved full recoverability and process reversibility. It also provided other security features such as tamper detection, authentication and confidentiality for the medical images. This makes contents stored in such Information infrastructure more secured. The paper has the following structure; section II Related works, section III is Methodology, section IV Results and analysis, and section V concluded the paper.

2. Literature Review

In the work of Usman, K. et al, they worked on medical image encryption based on pixel arrangement and random permutation for transmission security. Their procedure engaged a random permutation by pixels and achieved a high computation speed. and [1]. Abokhdair, N.O et al worked on integration of chaotic map and confusion technique for color medical image encryption, and a 2D lower triangular map was used for scrambling the addresses of image pixels. Their method was resistive to brute force attack [2]. Yicong Zhou et al in their work of , “a lossless encryption method for medical images using edge maps”, showed a new lossless approach, called EdgeCrypt, to encrypt medical images using the information contained within an edge map[3]. Below is the results obtained from their work.

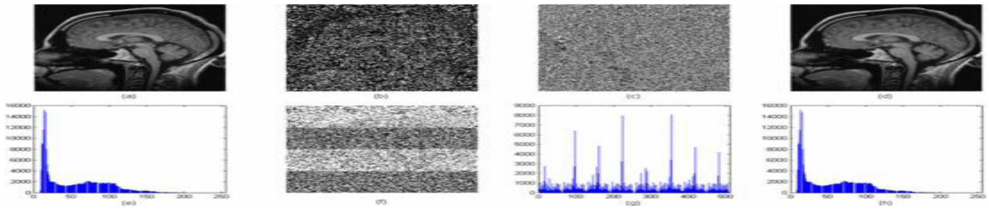


Fig. 1. The proposed system’s architecture.MRI image encryption. (a) The original MRI image; (b) The edge map obtained by Sobel edge detector with threshold 0.5; (c) The encrypted MRI image, (d) The reconstructed MRI image; (e) Histogram of the original MRI image; (f) The encrypted edge map, x_{0}=0.6 , r=3.65 ; (g) Histogram of the encrypted MRI image; (h) Histogram of the reconstructed MRI image.

Other works such as Transmission and storage of medical images with patient information" by R. Acharya U, P et al [4], "Chaos-Based Medical Image Encryption Using Symmetric Cryptography" by M. Ashtiyaniet [5] etc. Our approach is discussed in the following section.

3. Methodology

Medical images stored in the cloud, with third party service providers, and in health information systems contain information about patients. A compromised health information system or un authorized access to these data will violate the privacy of patients and wrong processing of a specific image for different patient will further affect the integrity of the medical institution. The safety, privacy and security of medical image are of paramount consideration in the health sector. Providing data integrity and authenticity of the medical images will ensure privacy, safety and security for medical data stored in medical information systems. In addressing these issues of unauthorized access, we propose an effective security information system with a fully recoverable and reversible technique for authentication and security of medical images in health information systems.

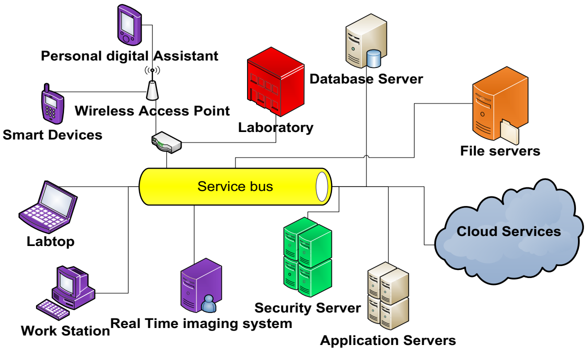


Fig. 2. The proposed system’s architecture.

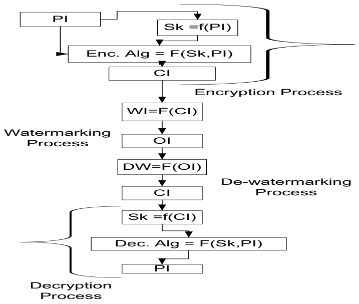


Fig.3. Summary of the process.

The encryption process is symmetric and uses client's authentication systems to grant access but uses patients' unique information in the encryption and watermarking of the medical images. With the proposed system, we ensured that, the security server has an application transaction service that provides effective confidentiality and authentication services for clients of the system before storage of the processed files in file servers or cloud systems. The security technique engaged is symmetric and the watermarking marking approach was in spatial domain and it provides authentication. With the proposed approach, disparate can easily access the medical images can communicate via the same service bus to access medical data such as x-ray image data, ultra sound scan documents etc. Any request made by an application residing in the same network infrastructure or external to it with regards to medical images will have services rendered to it via an abstraction level to that application. Data stored in file servers, in databases and in cloud can only be accessed and decrypted successfully through transaction activities involving the security server and this prevent exposure of sensitive medical data when the file servers are being comprised or there have been backdoor access to storage servers in the cloud.

3.1. The Encryption process

a) Import data from image and create an image graphics object by interpreting each element in a matrix.

b) Get the size of r as [c, p]

c) Get the Entropy of the plain Image

d) Get the mean of the plain Image

e) Compute the shared secret from the image

f) Engage SK for g) to q) using secret key value

g) Extract the red component as 'r'

h) Extract the green component as 'g'

i) Extract the blue component as 'b'

j) Let r =Transpose of r

k) Let g =Transpose of g

l) Let b =Transpose of b

m) Reshape r into (r, c, p)

n) Reshape g into (g, c, and p)

o) Reshape b into (b, c, and p)

p) Concatenate the arrays r, g, b into the same dimension of 'r' or 'g' or 'b' of the original image.

q) Finally the data will be converted into an image format to get the encrypted image.

The inverse of the algorithm will decrypt the encrypted image back into the plain image.

The secret key is obtained as follows:

$$Sk = [(c \ x \ p) + |(He \ x \ 10^3)| + |(\quad \bar{x} = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \quad)|] \bmod p$$

Where c, p are dimension of the image and He is the entropy value of the image and *x* bar is the arithmetic mean for all the pixels in the image.

3.2. The watremarking process

The spatial watermarking data was applied throughout the R channel of the ciphered image.

Let (:,:,1)=size of R be mxn[row, column] , size (R) = R (m x n),rij= r=CI (m, n, 1) and Embedding the data into CI

d=Aij, where d is the data to be embedded

x ∈Aij : [a, b]={x ∈ I: a ≤ x ≥ b}where a=0 and b=255

```
Let the size of d be [c1, p1] =size (d) and  $\lambda$=xi : x i$\in$ I: $0 \leq x \geq \infty$;
Let $\eta$=xi : x i$\in$ I: $0 \leq x \geq \infty$;
 for i=1:1:c1
      for j=1:1:p1
       r(i,j)=($A^2_{ij}$+ Aij+ r(i,j)) mod 256;
    end
end
```

The implantation of the approaches was done in MATLAB.

4. Online license transfer

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.Three sample of medical images were encrypted by the algorithm using MATLAB and the results are below. The RGB graphs from figure 5 to 9 were plotted using the first 10000 pixel values of both plain and ciphered images.

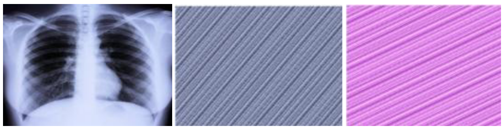
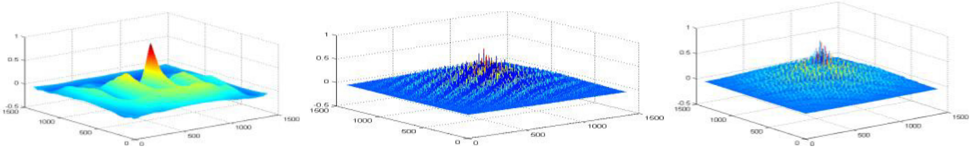


Fig. 4. X-ray Image of the ribs a) Plain image b) Ciphered Image c) Watermarked Image



a) Plain image b) Ciphered Image c) Watermarked Image

Fig.5. The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the X-ray Image

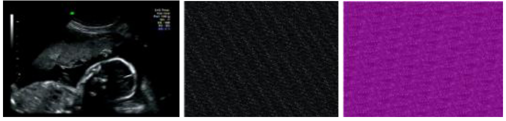
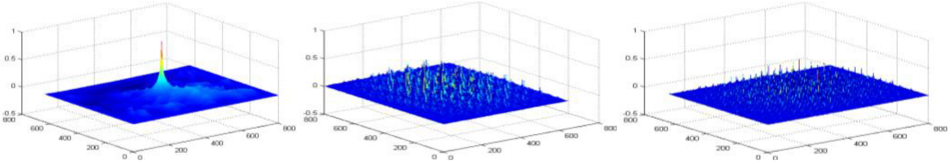


Fig.6. Ultrasound Image of the womb a) Plain image b) Ciphered Image c) Watermarked Image



a) Plain image b) Ciphered Image c) Watermarked Image

Fig.7. The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the Ultrasound Image

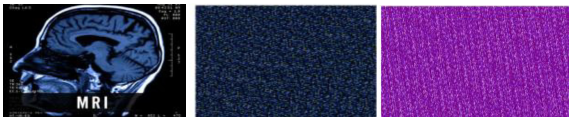


Fig.8..Magnetic Resonance Imaging of the brain a) Plain image b) Ciphered Image c) Watermarked Image

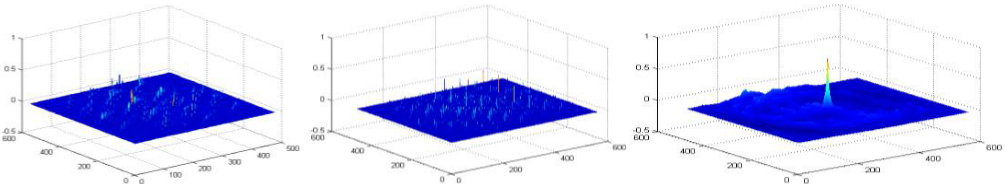


Fig.9.The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the MRI Image

TABLE 1: ANALYSIS OF PLAIN, CIPHERD, AND WATERMARKED IMAGE.

	Entropy(p)	*Arithmetic mean(m)*
XPI	7.1726	143.5284
XEI	7.1726	143.5284
XWI	5.6501	195.9501
UPI	3.7603	18.5810
UEI	3.7603	18.5810
UWI	4.5300	97.8801
MPI	4.6894	39.0415
MEI	4.6894	39.0415
MWI	4.9291	112.6501

From the table: PI=X-ray plain image; XEI=X-ray encrypted image; XWI=X-ray watermarked image; UPI=Ultrasound plain image; UEI= Ultrasound encrypted image; UWI= Ultrasound watermarked image; MPI=Magnetic Resonance Imaging Plain Image; MEI= Magnetic Resonance Imaging encrypted image; MWI=Magnetic Resonance Imaging watermarked image

5. Conclusion

At the end of the process, the technique engaged was very effective for all the images and there was no pixel expansion at the end of the process. The entropy and mean values for the images in were computed as shown in the table above. The total entropy and the mean of the plain images never changed for all the ciphered images and the plain images. That is the average total pixel values before encryption were the same as the average total pixel after encryption. But there was a change in pixel value during the watermarking process

Acknowledgements

This work was supported by Lab-STICC (UMR CNRS 6285) at UBO France, AWBC Canada, Ambassade de France-Institut Français-Ghana and the DCSIT-UCC, and also Dominique Sotteau (formerly directeur de recherche, Centre national de la recherche scientifique (CNRS) in France and head of international relations, Institut national de recherche en informatique et automatique, INRIA) and currently the Scientific counselor of AWBC.

References

1. Usman, K.; Juzoji, H.; Nakajima, I.; Soegidjoko, S.; Ramdhani, M.; Hori, T.; Igi, S., "Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security," e-Health Networking, Application and Services, 2007 9th International Conference on , vol., no., pp.244,247, 19-22 June 2007
2. Abokhdair, N.O.; Manaf, A.B.A.; Zamani, M., "Integration of chaotic map and confusion technique for color medical image encryption," Digital Content, Multimedia Technology and its Applications (IDC), 2010 6th International Conference on , vol., no., pp.20,23, 16-18 Aug. 2010
3. Yicong Zhou; Panetta, K.; Agaian, S., "A lossless encryption method for medical images using edge maps," Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE , vol., no., pp.3707,3710, 3-6 Sept. 2009
4. R. Acharya U, P. Subbanna Bhat, S. Kumar, L. C. Min, "Transmission and storage of medical images with patient information", Computers in Biology and Medicine, vol. 33, no.4, pp.303-310, 2003
5. M. Ashtiyani, P. M. Birgani, H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography", Information and Communication Technologies: From Theory to Applications 2008. ICTTA 2008. 3rd International Conference on, pp.1-5.