Spatial Cryptographic and Watermarking Technique for Authentication and Security of Medical Images in a Cloud Based Health Information Systems

Quist-Aphetsi Kester[1,2,3,4(✉)]

[1] Ghana Technology University, Accra, Ghana
[2] Lab-STICC (UMR CNRS 6285), University of Brest, Brest, France
kester.quist-aphetsi@univ-brest.fr, kquist@ieee.org
[3] Satellite Communications and Navigation Systems Department, CRITAC, Accra, Ghana
[4] Directorate of Information Assurance and Intelligence Research, CRITAC, Accra, Ghana

Abstract. Cloud computing has provided tremendous opportunities for a lot of organizations in cutting operating cost, making data available to distributed units, provision of easy interoperability etc. 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. And medical images form dominant part of the sensitive patient data. Hence privacy and security needs to be guaranteed for such images stored in the cloud. Most of the access security and encryption approaches are left for the cloud owners to manage and these poses a lot of insecurity if the system is compromised. In our wok, we proposed a hybrid spatial cryptographic and watermarking technique for authentication and security of medical images before storage in the cloud. Due to the sensitive nature of medical images, we were able to achieve full recoverability of the plain image after decryption and dewatermarking without pixel loss. Our results showed to be very effective and reliable for fully recoverable images.

Keywords: Cloud computing · Medical images · Health information systems · Security · Cryptography

1 Introduction

Health information systems are an integral and important part of our modern societal information technology infrastructure [1, 2]. The effective and accurate exchange of information within and between healthcare organizations helps in easy access, collection, use, and exchange of information between healthcare facilities [3]. Such information can be triggers of an outbreak, knowledge of on rare cases etc. [4]. Medical record histories of patients are very critical in understanding behavior and traits of diseases over time [5, 6]. And medical imaging has revolutionalized the way healthcare

T.F. Bissyande and O. Sie (Eds.): AFRICOMM 2016, LNICST 208, pp. 281–291, 2018.
https://doi.org/10.1007/978-3-319-66742-3_27

delivery is made across countries. Medical records are very sensitive documents in healthcare delivery and hence good care is needed to be taken to protect it [7]. Information systems adopted security approaches in securing these images. The easy of healthcare delivery and real-time and easy access to healthcare records of patience has pushed modern healthcare practices to adopt cloud storage approaches [8]. This approach then draws in a third party service provider to render services such as warehousing, interoperability, applications as a service etc. Most data stored in the cloud can leak due to malicious activities over the internet. Back door access to stored image files can compromise the privacy and confidentiality of the data stored and hence security approaches are needed in securing these medical data. Also authentication of images by mapping them using watermark approaches to patient records is also very necessary.

2 Review

The increased patient mobility in time across geographical area, combined with the fact that different health care treatments are frequently offered by different health care units, have resulted in the development of web-based electronic health care records. These have also pushed a lot of medical information systems to adopt cloud computing approaches. Although such systems facilitate access to the entire medical history of the patient, it is not straight forward to design and implement security mechanisms for ensuring the confidentiality and integrity of the data or/and the privacy of the patient, without limiting the communication of information between health care professionals and sacrificing system flexibility. In solving the above situation, Dimitris Gritzalis et al. proposed a security architecture for interconnecting health information systems and which was explained in their work [9]. The cloud architecture provides limited security control on the data for its users and a typical example of the cloud architecture is shown below which is typical of modern health information system in the cloud (Fig. 1).

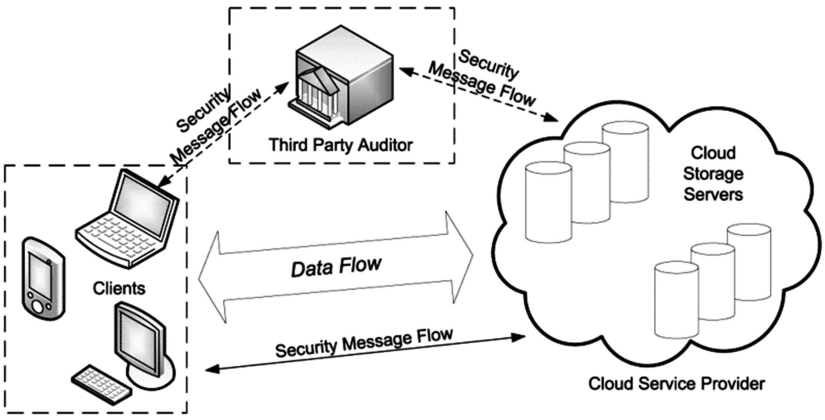


Fig. 1. Data cloud data storage architecture

The above diagram represented three different network entities that can be identified as follows: Client: an entity which uses cloud services and can either individual consumers or organizations; Cloud Storage Server (CSS): an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data; and the Third Party Auditor: an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request [10]. With the architecture above, client benefits from a lot of services advantages such as saving cost in the setup of physical information technology infrastructure setup cost, computational cost with dependency on power source for cooling centers and servers, migration of facilities during relocations and setting up other distributed access units, overhead cost for system maintenance and staff training etc. [11]. But in high hopes of these loses control or have limited oversight on user data security, system integrity, data access etc. [12]. In providing security for medical images, Abokhdair et al. in their work of Integration of chaotic map and confusion technique for color medical image encryption, proposed algorithm based on combination of scrambling and confusion processes. 2D lower triangular map used for scrambling the addresses of image pixels, and the proposed propeller algorithm was used to confuse the gray values of image pixels. Their method also was resistive to brute force attack [13]. Yicong Zhou et al. in their work, "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. Their algorithm can also be applied to grayscale images or color images [14]. There have been other works such as Transmission and storage of medical images with patient information" by Acharya et al. [15], "Chaos-Based Medical Image Encryption Using Symmetric Cryptography" by M. Ashtiyaniet [16] etc. Our proposed approach to security is discussed in the following section.

3 Methodology

With our proposed approach based on the architecture in Fig. 2 by introduced a third party security service that renders a real-time session service of encryption and decryption of data between the cloud storage, streaming and other system services and the client. The third party executes the proposed a hybrid spatial cryptographic and watermarking technique for authentication and security of medical images before storage in the cloud. This means it provides services in addition to the primary security protocols between clients and the cloud as diagram below provides the detailed of the architecture behind the system. This ensures that the data stored in the cloud is secure and can only be accessed via that service as a security through a third party or via a service bus.

The pixel values of the images to be encrypted were visually encrypted using n-share of the visual cryptographic technique engaged based on pixel displacement in the RGB channels of the image. The watermarking process was based on a unique patient credential and was applied in this work to only the R-channel of the image.

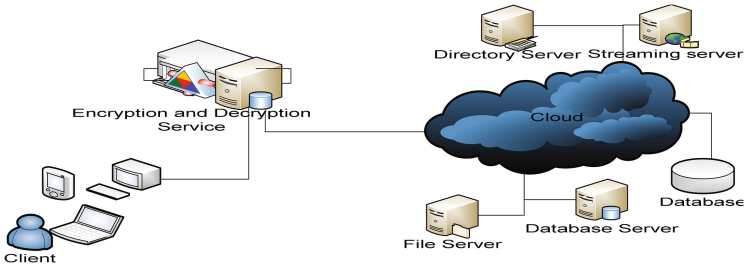


Fig. 2. Proposed process architecture

3.1 The Image Encryption Process

Step 1. Start
Step 2. Extraction of data from a plain image,
Let I = an image = f (R, G, B)
I is a color image of m × n × 3 arrays

$$\begin{pmatrix} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ r_{n1} & g_{n2} & b_{n3} \end{pmatrix} \tag{1}$$

(R, G, B) = m x n
Where R, G, B ∈ I
(R o G) i j = (R) ij. (G) ij
Where r_11 = first value of R
r= [ri1] (i=1, 2… m)
x ∈ r_i1 : [a, b]= {x ∈ I: a ≤x ≥b}
a=0 and b=255
R= r= I (m, n, 1)
Where g_12 = first value of G
g= [gi2] (i=1, 2... m)
x ∈ g : [a, b]= {x ∈ I: a ≤x ≥b}
a=0 and b=255
G= g= I (m, n, 1)
And b_13 = first value of B
g= [bi3] (i=1, 2... m)
x ∈ b_i1 : [a, b]= {x ∈ I: a ≤x ≥b}
a=0 and b=255
B=b= I (m, n, 1
Such that R= r= I (m, n, 1)

Step 3. Extraction of the red component as 'r'
Let size of R be m x n [row, column] = size (R) = R (m × n)

$$\text{rij} = \text{r} = \text{I}(\text{m}, \text{n}, 1) = \begin{pmatrix} R \\ r_{i1} \\ \vdots \\ \vdots \\ \vdots \\ r_{in} \end{pmatrix} \tag{2}$$

Step 4. Extraction of the green component as 'g'
Let size of G be m × n [row, column] = size (G)

$$\text{gij} = \text{g} = \text{I}(\text{m}, \text{n}, 1) = \begin{pmatrix} G \\ g_{i2} \\ \vdots \\ \vdots \\ \vdots \\ g_{n2} \end{pmatrix} \tag{3}$$

Step 5. Extraction of the blue component as 'b'
Let size of B be m × n [row, column] = size (B) = B (m × n)

$$\text{bij} = \text{b} = \text{I}(\text{m}, \text{n}, 1) = \begin{pmatrix} B \\ b_{i3} \\ \vdots \\ \vdots \\ \vdots \\ b_{n3} \end{pmatrix} \tag{4}$$

Step 6. Getting the size of r as [c, p]
Let size of R be [row, column] = size (r) = r (c × p)
Step7. Engagement of SSK which is the symmetric secret key generated. The key is then engaged to iterate the step 8 to 14.
Step 8. Let r = Transpose of rij

$$\text{r} = \begin{pmatrix} R & & & & \\ r_{i1} & \cdots & \cdots & \cdots & r_{n1} \end{pmatrix} \tag{5}$$

Step 9. Let g = Transpose of gij

$$\mathrm{g} = \begin{pmatrix} G & & & & \\ g_{i3} & \dots & \dots & \dots & g_{n3} \end{pmatrix} \tag{6}$$

Step 10. Let b = Transpose of bij

$$\mathrm{b} = \begin{pmatrix} B & & & & \\ b_{i2} & \dots & \dots & \dots & b_{n2} \end{pmatrix} \tag{7}$$

Step 11. Reshaping of r into (r, c, p)

$$\mathrm{r} = \text{ reshape } (\mathrm{r},\ \mathrm{c},\ \mathrm{p}) = \begin{pmatrix} R \\ r_{i1} \\ \vdots \\ \vdots \\ \vdots \\ r_{in} \end{pmatrix} \tag{8}$$

Step 12. Reshaping of g into (g, c, p)

$$\mathrm{g} = \text{ reshape } (\mathrm{g},\ \mathrm{c},\ \mathrm{p}) = \begin{pmatrix} G \\ g_{i2} \\ \vdots \\ \vdots \\ \vdots \\ g_{n2} \end{pmatrix} \tag{9}$$

Step 13. Reshaping of b into (b, c, p)

$$\mathrm{b} = \text{ reshape } (\mathrm{b},\ \mathrm{c},\ \mathrm{p}) = \begin{pmatrix} B \\ b_{i3} \\ \vdots \\ \vdots \\ \vdots \\ b_{n3} \end{pmatrix} \tag{10}$$

Step 14. Concatenation of the arrays r, g, b into the same dimension of ‘r’ or ‘g’ or ‘b’ of the original image

$$= \begin{pmatrix} R & G & B \\ r_{i1} & g_{i2} & b_{i3} \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ r_{n1} & g_{n2} & b_{n3} \end{pmatrix} \tag{11}$$

Step 15. Finally the data will be converted into an image format to get the encrypted image.

3.2 The Watermarking Process

Let the host signal be defined by A as below. The following approach was used to embed the data into the image, A. For a given Image A, we have

$$A = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & \cdot & \cdot & \cdot & x_{1n} \\ x_{21} & x_{22} & \cdot & \cdot & \cdot & \cdot & \cdot & x_{2n} \\ x_{31} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_{3n} \\ x_{41} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & x_{4n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{m1} & \cdot x_{m2} & x_{m3} & x_{m4} & \cdot & \cdot & \cdot & x_{mn} \end{bmatrix} \tag{12}$$

For a given message E to be embedded in A where E < A, we have,

$$E = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdot & \cdot & \cdot & x_{1n} \\ x_{21} & x_{22} & \cdot & \cdot & \cdot & \cdot & x_{2n} \\ x_{31} & \cdot & \cdot & \cdot & \cdot & \cdot & x_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{m1} & \cdot x_{m2} & x_{m3} & \cdot & \cdot & \cdot & x_{mn} \end{bmatrix} \tag{13}$$

Where we obtain the channels of the image as R, G, B $\in$ A
$(R \text{ o } G)_{ij} = (R)_{ij}.(G)_{ij}$ and x $\in$ [i, j, m, n] and $\{x \in I: 1 \leq x \leq +\infty\}$
For x $\in$ [R, G, B]: [a, b] = $\{x \in I: a \leq x \geq b\}$ where a = 0 and b = 255

$$\begin{aligned} R = r &= A(m, n, 1) \\ G = g &= A(m, n, 1) \\ B = b &= A(m, n, 1) \end{aligned} \tag{14}$$

[c, p] = s(R); is the size of R as [c, p]
Let s(R) = size of R be [row, column] = size (R) = R (c $\times$ p)

Embedding E the data into A will be
d = Eij, where d is the elements of the data to be embedded
Let the size of d be [c1, p1] = size (d)

```
for i=1:1:c1
            for j=1:1:p1
           if(c1<c)
                  R(i,j)= ((i,j)+Eij)mod256
                  G(i,j)= G(i,j)
                  B(i,j)= G(i,j)
              else
                   R(i,j)=R(i,j)
                   G(i,j)=G(i,j)
                   B(i,j)=B(i,j)
             end
            end
end
```

4 Results and Analysis

The image below of dimension 640 × 480 pixels obtained from a UAV, vertical and horizon resolution of 72 dpi and bit depth of 24 was operated on by the proposed process and the following results were obtained from it.

The graph of the normalized cross-correlation of the matrices of the image.

The normalized cross-correlation of the matrices of is

$$\gamma(u,v) = \frac{\sum_{x,y}\left[f(x,y) - \overline{f}_{u,v}\right]\left[t(x-u,\, y-v) - \overline{t}\right]}{\left\{\sum_{x,y}\left[f(x,y) - \overline{f}_{u,v}\right]^2 \sum_{x,y}\left[t(x-u,\, y-v) - \overline{t}\right]^2\right\}^{0.5}} \tag{15}$$

f is the mean of the template, $\overline{t}$ is the mean of in the region under the template. $\overline{f}_{u,v}$ is the mean of *f(u, v)* in the region under the template.

From the Table 1,

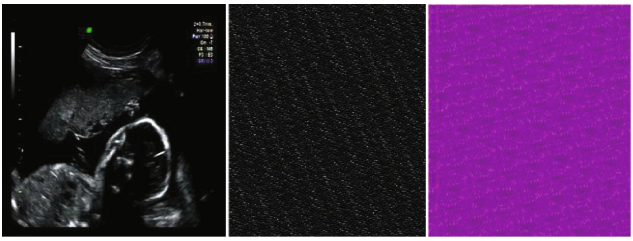
UPI = Ultrasound plain image
UEI = Ultrasound encrypted image
UWI = Ultrasound watermarked image

Table 1. Extracted features from the process.

Heading level	Entropy	Arithmetic mean
UPI	3.7603	18.5810
UEI	3.7603	18.5810
UWI	4.5355	97.8913
DWI	3.7603	18.5810
RPI	3.7603	18.5810

URI = Ultrasound recovered image
DWI = Ultrasound dewatermarked image

The results in Fig. 3 show how the ciphered image was encrypted and then watermarked. The graph of the normalized cross-correlation of the matrices of the plain, ciphered and watermarked image of the Ultrasound Image are shown in Figs. 4, 5 and 6 respectively. It can be observed from the graphs that, the distribution of pixel values are evenly distributed with arithmetic mean value of 18.5810 for the plain and ciphered image due to lossless encryption approach engaged.



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

Fig. 3. Ultrasound Image of the womb

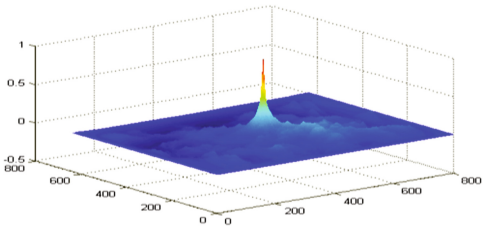


Fig. 4. The graph of the normalized cross-correlation of the matrices of the plain image of the Ultrasound Image

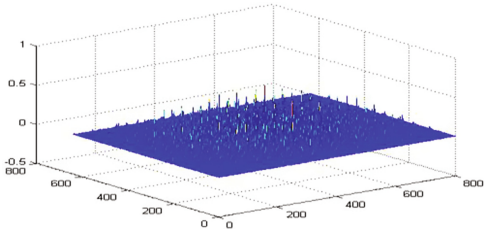


Fig. 5. The graph of the normalized cross-correlation of the matrices of the ciphered image of the Ultrasound Image

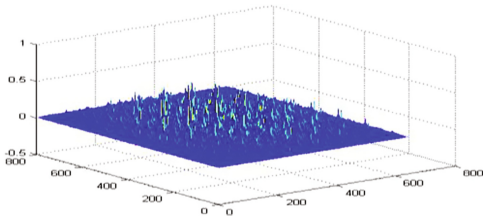


Fig. 6. The graph of the normalized cross-correlation of the matrices of the watermarked image of the Ultrasound Image

5 Conclusion

We were able to obtain a full recoverable image at the end of the process due to the fact that our proposed method can reconstruct the pixel back in the image which is very important for medical images since they contain vital information about the patient. And our proposed work was resistive against statistical and brute force attacks. 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 before encryption was the same as the average total pixel after encryption. But there was a change in pixel value during the watermarking process due to pixel expansion process. Because we engaged image features and patient identification in the ciphering process, each image is uniquely encrypted; making it safer for the images and also it is easy to authenticate the image with the patient's records as well. The approach ensures that the confidentiality of patient image data is guaranteed.

References

1. Abdelhak, M., Grostick, S., Hanken, M.A.: Health Information: Management of A Strategic Resource. Elsevier Health Sciences (2015)
2. Leventhal, J.C., Cummins, J.A., Schwartz, P.H., Martin, D.K., Tierney, W.M.: Designing a system for patients controlling providers' access to their electronic health records: organizational and technical challenges. J. Gen. Intern. Med. **30**(1), 17–24 (2015)
3. Witting, K.: Health information exchange: Integrating the Healthcare Enterprise (IHE). In: Hannah, K.J., Hussey, P., Kennedy, M.A., Ball, M.J. (eds.) Introduction to Nursing Informatics. HI, pp. 79–96. Springer, London (2015). doi:10.1007/978-1-4471-2999-8_6
4. Stuss, D.T., Amiri, S., Rossor, M., Johnson, R., Khachaturian, Z.: How we can work together on research and health big data: strategies to ensure value and success. In: Dementia Research and Care Can Big Data Help?: Can Big Data Help?, p. 61 (2015)
5. Ludwick, D.A., Doucette, J.: Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. Int. J. Med. Inform. **78**(1), 22–31 (2009)
6. Eysenbach, G.: Recent advances: consumer health informatics. BMJ. Br. Med. J. **320**(7251), 1713 (2000)
7. Anderson, R.J.: Security in clinical information systems. Br. Med. Assoc., London (1996)

8. Mouratidis, H., Giorgini, P., Manson, G.: Integrating security and systems engineering: towards the modelling of secure information systems. In: Eder, J., Missikoff, M. (eds.) CAiSE 2003. LNCS, vol. 2681, pp. 63–78. Springer, Heidelberg (2003). doi:10.1007/3-540-45017-3_7
9. Gritzalis, D., Lambrinoudakis, C.: A security architecture for interconnecting health information systems. Int. J. Med. Inform. **73**(3), 305–309 (2004)
10. Wang, Q., Wang, C., Ren, K., Lou, W., Li, J.: Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst. **22**(5), 847–859 (2011)
11. Liu, H.: Big data drives Cloud adoption in enterprise. IEEE Internet Comput. **17**(4), 68–71 (2013)
12. Tari, Z.: Security and privacy in Cloud computing. IEEE Cloud Comput. **1**(1), 54–57 (2014)
13. Abokhdair, N.O., Manaf, A.B.A., Zamani, M.: Integration of chaotic map and confusion technique for color medical image encryption. In: 2010 6th International Conference on Digital Content, Multimedia Technology and its Applications (IDC), pp. 20–23, 16–18 August 2010
14. Zhou, Y., Panetta, K., Agaian, S.: A lossless encryption method for medical images using edge maps. In: Engineering in Medicine and Biology Society, 2009, EMBC 2009, Annual International Conference of the IEEE, pp. 3707–3710, 3–6 September 2009
15. Acharya, U.R., Bhat, P.S., Kumar, S., Min, L.C.: Transmission and storage of medical images with patient information. Comput. Biol. Med. **33**(4), 303–310 (2003)
16. Ashtiyani, M., Birgani, P.M., Hosseini, H.M.: Chaos-based medical image encryption using symmetric cryptography. In: 3rd International Conference on Information and Communication Technologies: From Theory to Applications 2008, ICTTA 2008, pp. 1–5 (2008)