Reversible Anonymization of DICOM Images using Cryptography and Digital Watermarking

Youssef ZAZ*
Department of Computer Sciences
Faculty of Sciences, Abdelmalek Essaadi University
Tetuan, Morocco

Lhoussain ELFADIL
FPO
Ibn Zohr University
Ouarzazate, Morocco

***Abstract*—Digital Imaging and Communications in Medicine (DICOM) is a standard for handling, storing, printing, and transmitting information in medical images. The DICOM file contains the image data and a number of attributes such as identified patient data (name, age, insurance ID card,…), and non-identified patient data (doctor's interpretation, image type,…). Medical images serve not only for examination, but can also be used for research and education purposes. For research they are used to prevent illegal use of information; before authorizing researchers to use these images, the medical staff deletes all the data which would reveal the patient identity to prevent patient privacy. This manipulation is called anonymization. In this paper, we propose a reversible anonymization of DICOM images. Identifying patient data with image digest, computed by the well-known SHA-256 hash function, are encrypted using the proposed probabilistic public key crypto-system. After compressing the Least Significant Bit (LSB) bitplan of the image using Hofmann coding algorithm, the encrypted data is inserted into a liberated zone of the LSB bitplan of the image. The proposed method allows researchers to use anonymous DICOM images and keep to authorized staff -if necessary- the possibility to return to the original image with all related patient data.**

Keywords-DICOM images; watermaking; Hofmann coding; reversible anonymization, public key cryptosystem.

I. INTRODUCTION

DICOM images contain different kind of information, intermixing identifying patient data (I-Data) and non-identifying patient data (M-data) in a single file. To use these images by scientific researchers or for teaching purposes, hospitals proceed to the image anonymization by deleting all I-Data to ensure the patient privacy. Several software and web based applications were proposed to ensure this anonymization, as proposed by [5], [4] and [6].

For research purposes, sometimes the return to some I-Data in order to explain typical phenomenon is inescapable, but, the images are already anonymized and there is no way to use those information. To deal with this problem, [2] proposed to substitute I-Data by a unique anonymous token. In case that later an authenticated user needs full access to an image, the token can be used for re-linking separated I-Data and M-Data. [7] proposes to extract and save identifying data in another database and non-identifying data is stored in the archive.

When data is requested, the proposed system resolves the correlating and gathers the person-identifying information from the separate database. Another web-based separation is proposed in [8]. All above methods circumvent the main objective of DICOM images, which is to keep the image and the related data in the same file. To ensure the anonymization with keeping I-Data in the same file, the watermarking techniques are unavoidable. [3] proposed embedding the digest computed by SHA-256, in the Region of Non-Interest (RONI) of the image LSB bitplan. This method presents some difficulties to determine the RONI.

In this paper, we propose a reversible anonymization of DICOM images based on cryptography and watermarking. After liberating a space in LSB bitplan of the host image by compressing the original LSB bitplan using the Hoffmann coding, the I-Data and the image digest computed by SHA digital signature algorithm, are encrypted using the proposed public key crypto-system and inserted in liberated zone.

This paper is organized as follows: Section 2 gives a brief review of DICOM standard. Section 3 explains the security requirement for medical data storage. Section 4 exposes the proposed public key crypto-system. Section 5 exposes the global algorithm of reversible anonymization, and the last section concludes the paper.

II. DICOM IMAGES

Introduced in 1993, DICOM (Digital Imaging and Communications in Medicine) a technology standard that is used virtually in Hospitals, clinics, imaging centers and specialists. Its structure is designed to ensure the interoperability of systems used to produce, store, display, send, …, and retrieve medical images and derived structured documents as well as to manage related workflow.

DICOM is required by all Electronic Health Records Systems that include imaging information as an integral part of the patient record.

DICOM is used in radiology, cardiology, radiotherapy, oncology, ophthalmology, dentistry, and so on.

For more description about DICOM, see the official web site [13].

III. SECURITY REQUIREMENTS FOR MEDICAL DATA STORAGE

To preserve patient privacy, all medical data are considered as sensitive. To read the content of an image, a user should be authorized. To prevent data infiltration, the anonymization prevents the exposure of identified patient data to unauthorized users. Many techniques are available to ensure the storage of medical data:

A. File access control

Under operating systems, the administrator defines access restrictions (read, write and execute) to file owner, the stuff members, and public users.

B. Data access control

Medical databases are stored in local servers and can be consulted remotely for tele-diagnostic for example. Access or denial to medical data should be adequately granted.

C. File encryption and signature

To reduce considerably the risk of disclosure, the use of crypto-system is a great solution. Encrypt medical data before transmission upon open networks, like Internet, ensures the confidentiality of patient identity. Adding digital signature ensure the data integrity also.

D. File anonymization

The identified patient data or de-identified patient data - information that does not identify the individual and for which there is no reasonable basis to believe the individual can be identified from it - must be kept confidential. Several software and web based applications can ensure the DICOM anonymization by deleting certain attributes like (Name, Address, Social card ID,…) .

IV. PROPOSED PUBLIC KEY CRYPTOSYSTEM

A. Overview

Formally, PKE = three efficient (probabilistic) algorithms:

KeyGen( ):

Outputs: public key pk and secret key sk

Enc(pk , m):

Outputs: a ciphertext c

Dec(sk , c):

Outputs: a message m

And always, we assume that the communication is exchanged in insecure channel, and then always, we assume that there are pirates (adversaries).

The scheme is called semantically secure if the probability $probability("A"wins) - \frac{1}{2}$ is negligible for every efficient adversary $"A"$.

Our proposed scheme is based on third order linear sequences.

In [10], P. Smith and M. J. J. Lennon proposed using Lucas sequences cryptosystems, and they proved that the computation cost by using Lucas sequences is half reduced instead of using exponentiation in the standard RSA. Moreover, from [12], the security of Lucas sequences is polynomial-time equivalent to the generalized discrete logarithm problem. In [11], Gong and L. Harn introduced cryptosystems based on third order linear sequences, and they show that the computation cost of the proposed scheme is reduced by $\frac{2}{3}$ instead of using exponentiation in the standard RSA. All these given variants have a weak point on semantic security. In this paper, a probabilistic variant is given, together with the security analysis. Moreover, as the crucial property of Lucas sequences is that cryptosystem are not formulated in terms of exponentiation, this would make them unsusceptible to various well known attacks that threaten the security of more traditional exponentiation based cryptosystems like RSA.

B. Mathematical foundation

Remind that for two integers a , b and a polynomial $f(X) = X^3 - aX^2 + bX - 1$, a third order linear characteristic sequence generated by (a,b) is denoted by $s(a,b)$ and defined by the following recurrence:

$$s_{k+3}(a,b) = as_{k+2}(a,b) - bs_{k+1}(a,b) + s_k(a,b) \qquad (1)$$

(a,b) is called the generator of $s(a,b)$ and k is its exponent.

It is well known that if α_1, α_2 and α_3 are the complex roots of $f(X)$. Then there exist three rational numbers (a_1, a_2, a_3) such that for every integer k .

$$s_k(\ a, b) = a_1\alpha_1^{\ k} + a_2\alpha_2^{\ k} + a_3\alpha_3^{\ k} \qquad (2)$$

Note that the tuple (a_1, a_2, a_3) depends only on the choice of $s_0(a,b)$, $s_1(a,b)$, $s_{-1}(a,b)$ and conversely. If $s_0(a,b), s_1(a,b)$ and $s_{-1}(a,b)$ are integers, then a_1, a_2, a_3 are integers too.

Through the paper, let p is an odd prime integer, $s(a,b)$ is a third order linear sequence such that $s_0(a,b), s_1(a,b)$, $s_{-1}(a,b)$ are integers and $a_1 \equiv a_2 \equiv a_3 \equiv 1 (\text{mod } p)$.

Then $s_{-1}(a,b) \equiv b (\text{mod } p)$, $s_0(a,b) \equiv 3 (\text{mod } p)$, $s_1(a,b) \equiv a (\text{mod } p)$ and for every k , $s_k(a,b)$ is an integer. Since $\overline{f(X)}$ is irreducible in $F_p[X]$, then $f(X)$ is irreducible in $Q[X]$ too. In that case, let $K = Q[\alpha_1]$, Z_K its ring of integers, $N_{K/Q}$ and $T_{K/Q}$ the norm and trace of K . Then for every integer k , $s_k(a,b) \equiv T_{K/Q}(\alpha_1^{\ k}) \bmod p$. Since $\alpha_1^{\ p} (\text{mod } p)$ and

$\alpha_1^{p^2} \pmod p$ are the conjugate of $\alpha_1 \pmod p$, we have: $N_{K/Q}(\alpha_1) \equiv \alpha_1^{p^2+p+1} \equiv 1 \pmod p$.

Thus, $T = p^2 + p + 1$ is a period of $s(a,b)$ modulo p.

The following cryptographic properties are well known modulo p (see [GH 99]). We give theme modulo p^2 without proof.

To simplify, for every integer k, let us denote $s_k := s_k(a,b) \pmod{p^2}$.

If $s_0(a,b) \equiv 3 \pmod{p^2}$, $s_1(a,b) \equiv a \pmod{p^2}$ and

$s_{-1}(a,b) \equiv b \pmod{p^2}$. Then for every integer k,

if $f_k(X) \equiv X^3 - s_k X^2 + s_{-k} X - 1 \pmod{p^2}$,

then $f_k(X) \equiv (X - \alpha_1^k)(X - \alpha_2^k)(X - \alpha_3^k) \pmod{p^2}$.

In particular, for every integers k and e,

$$s_e(s_k(a,b), s_{-k}(a,b)) \equiv (s_{ek}, s_{-ek}) \pmod{p^2}. \quad (3)$$

C. Infrastructure

The algorithms of the proposed public key schemes are based on the result given in Proposition.1, given in this paragraph.

Let $n = pq$ be an RSA, (a,b) two integers such that $f(X) = X^3 - aX^2 + bX - 1$ is irreducible modulo p (resp. modulo q), $s(a,b)$ the third order linear sequence modulo n^2 generated by (a,b) such that $s_{-1}(a,b) \equiv b \pmod{n^2}$, $s_0(a,b) \equiv 3 \pmod{n^2}$,

$s_1(a,b) \equiv a \pmod{n^2}$.

Let

$$T = LCM(p^2 + p + 1, q^2 + q + 1) \quad (4)$$

be the least common multiple of $p^2 + p + 1$ and $q^2 + q + 1$.

Let $\Gamma := \{(x,y) \in Z^2, s_T(x,y) \equiv 3 \pmod n\}$

and $L : \Gamma^2 \to \frac{Z}{nZ}$ defined by

$$\mathrm{L}(x,y) = \frac{s_T(x,y) - 3}{n} \pmod n.$$

Since for every $(x,y) \in \Gamma$, $s_T(x,y) \equiv 3 \pmod n$, L is well defined and we have the following proposition:

Proposition.1

If $L(a,b)$ is invertible modulo n, then for every integer k,

$$\frac{L(s_k(a,b), s_{-k}(a,b))}{L(a,b)} \equiv k \pmod n \quad (5)$$

Proof.

For every $i := 1,2,3$,

let $\Gamma^i := \{x \in Z[\alpha_i],\ x \equiv 1 \pmod{n\, Z[\alpha_i]}\}$

and $L_i : \Gamma^i \to \frac{Z[\alpha_i]}{nZ[\alpha_i]}$ defined by $\mathrm{L}_i(x) = \frac{x-1}{n} \pmod n$.

Then for every $(x,y) \in \Gamma^{i^2}$,

$$\mathrm{L}_i(xy) \equiv \frac{xy-1}{n} \equiv \frac{x(y-1)+x-1}{n} \equiv x\frac{(y-1)}{n} + \frac{x-1}{n} \pmod n.$$

Since $x \in \Gamma^i$, we have $\mathrm{L}_i(xy) \equiv \frac{(y-1)}{n} + \frac{x-1}{n} \pmod n$

and then $\mathrm{L}_i(xy) = \mathrm{L}_i(x) + \mathrm{L}_i(y)$.

Let $\mathrm{T} = k_p(p^2 + p + 1)$. Since for every $i := 1,2,3$,

$$\alpha_i^T \equiv (\alpha_i^{p^2+p+1})^{k_q} \equiv (N_{K/Q}(\alpha_i))^{k_q} \equiv 1 \pmod p \quad \text{(resp. } \alpha_i^T \equiv 1 \pmod q\text{)},$$

it follows that $\alpha_i^T \equiv 1 \pmod n$. Thus for every $i := 1,2,3$, $\alpha_i^T \in \Gamma^i$ and for every integer k, $L_i(k\alpha_i^T) \equiv kL_i(\alpha_i^T) \pmod n$. So, $s_{kT}(a,b) - 3 \equiv (\alpha_1^{kT} - 1) + (\alpha_2^{kT} - 1) + (\alpha_3^{kT} - 1) \pmod n$ and

$$L(\mathrm{s_k}(a,b), \mathrm{s_{-k}}(a,b)) \equiv \frac{\mathrm{s_k}(a,b) - 3}{n} \equiv \sum_{i=1}^{3} \frac{\alpha_i^{kT} - 1}{n} \equiv k \sum_{i=1}^{3} L^i(\alpha_i^T) \pmod n$$

Finally, $\mathrm{L}(\mathrm{s_k}(a,b), \mathrm{s_{-k}}(a,b)) \equiv kL(a,b) \pmod n$, and if $L(a,b) \pmod n$ is invertible,

then $\frac{\mathrm{L}(\mathrm{s_k}(a,b), \mathrm{s_{-k}}(a,b))}{L(a,b)} \equiv k \pmod n$.

The solely problem that remains to establish our proposed scheme, is to describe a method How to choose a couple (a,b) such that $L(a,b) \pmod n$ is invertible: if $L(a,b) \pmod n$ is not invertible, we describe a method which allows us to choose a couple (a,b) of integers that $L(a,b) \pmod n$ is invertible.

If $\frac{s_T(a,b) - 3}{n} \pmod n$, then we will keep $s_{-1}(a,b) \equiv b \pmod{n^2}$, $s_0(a,b) \equiv 3 \pmod{n^2}$ and $s_1(a,b) \equiv a \pmod{n^2}$. Else, i.e., if p or q divides $\frac{s_T(a,b) - 3}{n}$, then let $E := \{n, q, p\}$ and $y = \frac{n}{x} \in E$ the largest element of E dividing $\frac{s_T(a,b) - 3}{n}$. (If $x \neq 1$, then x does not divide $\frac{s_T(a,b) - 3}{n}$). Let $A := a + nx$, and consider $s_{(A,b)}$ the characteristic sequence generated by (A,b) modulo n^2:

$s_{-1}(A,b) \equiv b \pmod{n^2}$, $s_0(A,b) \equiv 3 \pmod{n^2}$

and $s_1(A,b) \equiv A \pmod{n^2}$.

Let β_1, β_2 and β_3 be the complex roots of $f(X) = X^3 - AX^2 + bX - 1$. Since $\overline{f(X)} \equiv \overline{g(X)} \pmod{p}$ (resp. $\overline{f(X)} \equiv \overline{g(X)} \pmod{q}$), then up to a permutation for every $i := 1,2,3$, there exists an integral complex t_i such that $\beta_i = \alpha_i + nt_i$. Thus, for every integer k,

$$s_k(A,b) = \sum_{i=1}^{3} \beta_i^{\,k} = \sum_{i=1}^{3} (\alpha_i + nt_i)^k = s_k(a,b) + nk(t_1 + t_2 + t_3) + n^2 u_k \quad ,$$

where u_k is an integral complex. For $k = 1$, we have $t_1 + t_2 + t_3 \equiv x \pmod{n}$.

Since $\frac{s_T(A,b) - 3}{n} \equiv \frac{s_T(a,b) - 3}{n} + x \pmod{n}$, $x \in \{1, p, q\}$ and if $x \neq 1$, then x does not divide $\frac{s_T(a,b) - 3}{n}$,

then $\frac{s_T(A,b) - 3}{n}$ is invertible.

Finally, without loss of generality, up to replace a by $a + nx$, we can assume that $\frac{s_T(a,b) - 3}{n} \pmod{n}$ is invertible.

Now we are ready to establish our proposed schemes.

D. The deterministic version

Algorithm of encryption and decryption:

1- Public parameters: $pk = (n, a, b)$.

2- Private parameters: $sk = (p, q)$.

3- Encryption: For a message $0 \leq m \leq n-1$, Bob calculates the block ciphertext (c_1, c_2) such that $c_1 = s_m(a,b) \pmod{n^2}$ and $c_2 = s_{-m}(a,b) \pmod{n^2}$.

4- Decryption: For a given block ciphertext(c_1, c_2), Alice can decrypt, by calculating $\frac{L(c_1, c_2)}{L(a,b)} \pmod{n}$.

Indeed, since (c_1, c_2) is a ciphertext, let $0 \leq m \leq n-1$ such

$c_1 = s_m(a,b) \pmod{n^2}$ and $c_2 = s_{-m}(a,b) \pmod{n^2}$. Therefore by using (3), we have

$s_T(c_1, c_2) \equiv s_T(s_m(a,b), s_{-m}(a,b)) \equiv (s_{Tm}(a,b), s_{-Tm}(a,b)) \equiv \pmod{n^2}$.

Moreover as $L(a,b)$ is invertible, using (5) of proposition.1, we have this equality:

$$\frac{L(c_1, c_2)}{L(a,b)} \equiv \frac{L(s_m(a,b), s_{-m}(a,b))}{L(a,b)} \equiv m \pmod{n}.$$

E. The probabilistic version

Algorithm of encryption and decryption:

1- Public parameters: $pk = (n, a, b)$.

2- Private parameters: $sk = (p, q)$.

3- Encryption: For a message $0 \leq m \leq n-1$, Bob chooses a random integer r and calculates the block ciphertext (c_1, c_2) such that

$c_1 = s_{m+rn}(a,b) \pmod{n^2}$ and

$c_2 = s_{-(m+rn)}(a,b) \pmod{n^2}$.

4- Decryption: For a given block ciphertext (c_1, c_2), Alice can decrypt, by calculating $\frac{L(c_1, c_2)}{L(a,b)} \pmod{n}$.

First, for the same plaintext 0, if $r \neq s$, then for $c_r = s_{rn}(a,b) \pmod{n^2}$, $c_s = s_{sn}(a,b) \pmod{n^2}$,

we have $c_r \neq c_s \pmod{n^2}$. Thus, as r is randomly chosen, then this scheme is probabilistic.

On the other hand, as in the proof of the last scheme, let $0 \leq m \leq n-1$ such $c_1 = s_{m+rn}(a,b) \pmod{n^2}$

and $c_2 = s_{-(m+rn)}(a,b) \pmod{n^2}$. By using (5) of Proposition.1, we have this equality :

$$\frac{L(c_1, c_2)}{L(a,b)} \equiv m + rn \equiv m \pmod{n}.$$

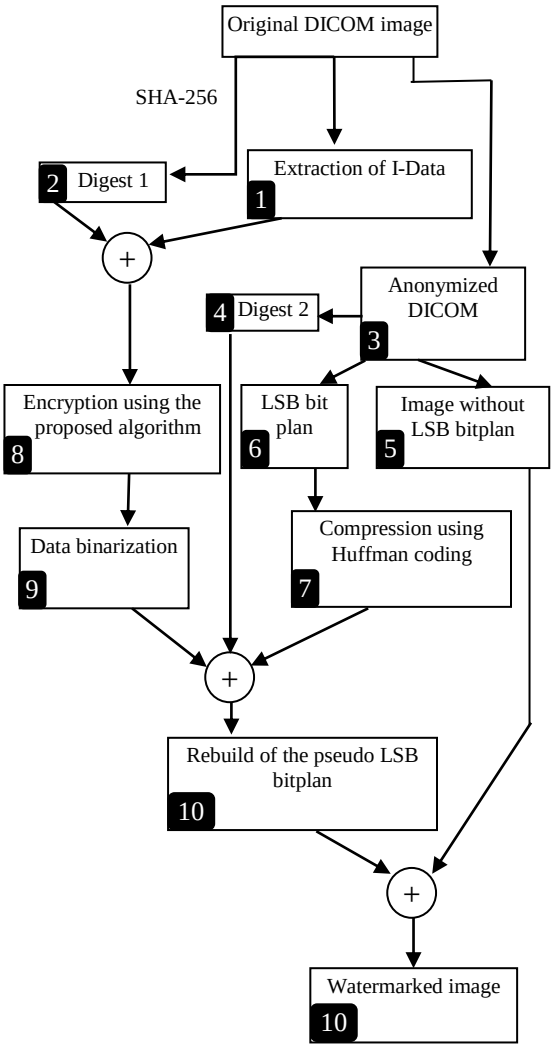
V. New DICOM Reversible Anonymization Mechanism

In order the keep the possibility to return to I-Data by using the secret key, we proposed to hide these data inside the image by watermarking it. To respect data integrity, the LSB bitplan of the image is compressed using Hoffmann coding and the liberated zone is used to embed I-Data. (See [9] for explanations about LSB bitplan compression). The I-Data and the digest1, computed from the original DICOM image using the well-known SHA-256 hash function, are encrypted using the proposed cryptosystem (see paragraph IV). The encrypted data is converted to binary form and inserted in the liberated zone of the image LSB bitplan.

The proposed method ensures that the anonymized DICOM images treated by our method are authentic, and when the return to the patient's identity is paramount, an authorized user (who has the secret key) can reveal the patient identified data to have more information about the patient and explain certain cases.

The algorithm is schematized below:

Emission side:



1– Extraction of identified patient data (I-Data) from the original DICOM image.

2– Computation of the original image digest, using SHA-256 hash function (digest 1).

3- Anonymization of the original DICOM.

4– Computation of the anonymized image digest, to be used by researchers to ensure the originality of the image (digest 2).

5– Extraction of the image without LSB bitplan.

6– Extraction of the LSB bitplan.

7– Compression of the LSB bitplan using Hofmann coding algorithm (used in [9]).

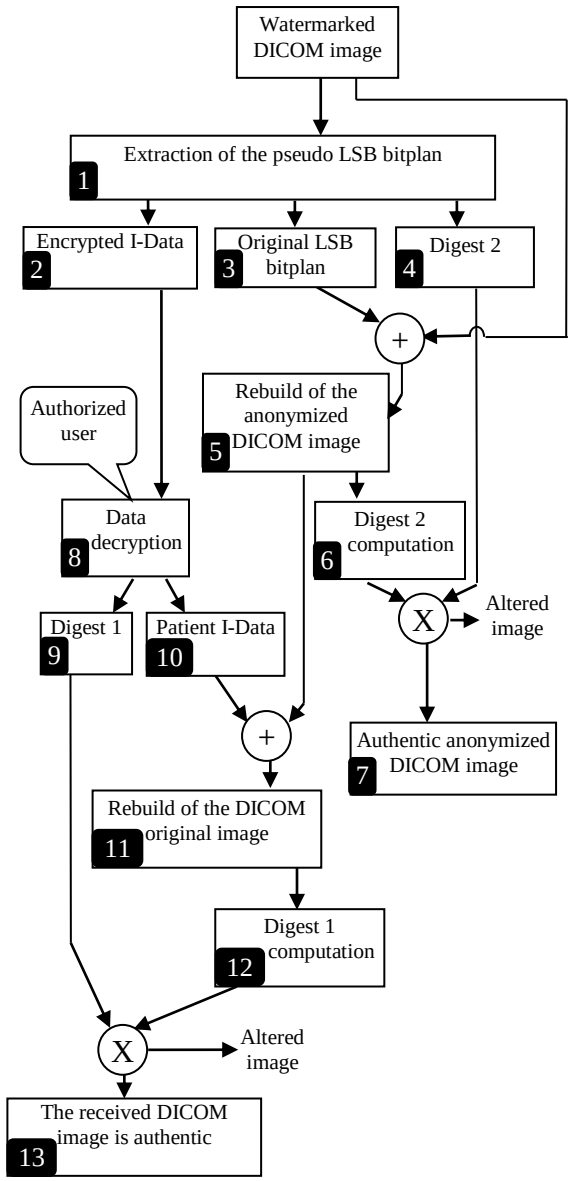
8– Encryption of I-Data and Digest 1 using the proposed crypto-system (see the algorithm in paragraph (IV - E).

9– Conversion of the encrypted data to binary format.

10– Rebuild of the pseudo LSB bitplan composed by: original LSB and binarized data (I-Data and digest 1)

11– Rebuild of the watermarked image to be used by researchers. The new image contains hidden patient I-Data patient.

Reception side:



Extraction of the LSB bitplan from the watermarked image.

2- Extraction of the encrypted data.

3– Extraction of the compressed LSB bit plan, to be decompressed using Hofmann decoding algorithm.

4- Extraction of Digest 1.

5- Rebuild of the anonymized image using the extracted LSB bitplan.

6- Computation of the digest from the rebuilt image. (digest 2).

7- Verification of the authenticity of the anonymized image by comparing the saved and the computed digests.

8- Authorized user, having secret key, can decrypt Data using the proposed decryption algorithm (see paragraph IV-E).

9– Extraction of the saved digest (digest 1).

10 – Extraction of the patient I-Data.

11 –Rebuild of the original DICOM image by combining anonymized image and I-Data.

12 – Computation of Digest 2.

13- Verification of the DICOM image originality, by comparing the saved and the computed digests.

VI. CONCLUSION

In this paper, we proposed a mechanism to perform a reversible anonymization to DICOM images. The identity patient data and image digest are encrypted using a new public key crypto-system and then watermarked in liberated zone of the image LSB bitplan obtained by compressing the original LSB. The proposed algorithm efficiently ensures the data confidentiality (encryption and watermarking), the reversibility (original data may be re-obtained), the authenticity (only the authorized user can access to identified patient data) and the timeliness by using a new scheme of public key crypto-system.

REFERENCES

[1] S. Hidenobu, N. Mami, S. Shinsuke, K. Mitsuru, K. Yoshiki, N. Noboru, N. Hiromu. Anonymization System to Protect the Personal Data in Secondary Use of DICOM Images. Institute of Electronics, Information and Communication Engineers, Vol.105, NO.579, pp. 71-74 (2006).

[2] M. Onken, J. Riesmeier, M. Engel, A. Yabanci, B. Zabel, S. Després. Reversible Anonymization of DICOM Images Using Automatically Generated Policies. Medical Informatics in a United and Healthy Europe. pp 861-865 (2009).

[3] J. M. Zain and M. Clarke. Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images. International Journal of Computer Science and Network Security, Vol.7, No.9, pp 19-28 (2007).

[4] Peyton H. Bland, Gary E. Laderach, and Charles R. Meyer. A Web-based Interface for Communication of Data between the Clinical and Research Environments without Revealing Identifying Information. Academic Radiology Journal, Vol 14, Issue 6, pp 757-764 (2007).

[5] A P Toms B Kasmai, S Williams, and P Wilson. Building an anonymized catalogued radiology museum in PACS: a feasibility study. British Journal of Radiology 79, pp 666-671 (2006).

[6] M. G. Ruiz, A. G. Chaves, C. R. Ibañez, J. M. Gutierrez Mazo, et al.. . mantisGRID: A Grid Platform for DICOM Medical Images Management in Colombia and Latin America. Springer - Journal of Digital Imaging. Vol 24, Number 2, pp 271-283 (2010).

[7] D. Abouakil, J. Heurix, and T. Neubauer. Data Models for the Pseudonymization of DICOM Data. The 44th Hawaii International Conference on System Sciences. pp 1-11 (2011).

[8] P. H. Blanda, G. E. Laderach, and C. R. Meyer. Implementation and use of a web-based interface for confidential communication of data between the clinical and research environments. Proceedings of the Society of Photo-Optical Instrumentation Engineers. PMC. pp. 1-16 (2009).

[9] Y. Zaz and L. Elfadil. Enhanced EPR Data Protection using Cryptography and Digital Watermarking. The 2nd International Conference on Multimedia Computing and Systems (IEEE Xplorer). Ouarzazate, Morocco (2011).

[10] P. Smith and M. J. J. Lennon, LUC : A new public key system. Ninth IFIP Int. Symp. on Computer Security, pp. 103-117 (1993).

[11] G. Gong and L. Harn. Public-Key Cryptosystems Based on Cubic Finite Field Extensions. In IEEE Trans. Inform. Theory, vol. 45, pp. 2601-2605 (1999).

[12] Chi-Sung Laih, Fu-Kuan Tu, and Wen-Chun Tai. On the security of the Lucas function, Information Processing Letters 53, pp 243-247 (1995).

[13] Official DICOM web site http://medical.nema.org/

AUTHORS PROFILE

Youssef Zaz is an assistant professor in University of Abdelmalek Essaadi (Morocco). He currently teaches and conducts research in computer related and image processing. He is also interested in the e-commerce and GNSS. Before joining Abdelmalek Essaadi in Sptember 2011, he was in Ibn Zohr University (Morocco) from 2006 to 2011. He worked as IT project Manager with National Department of Post Telecommunication and IT from 2000 to 2006. His main scientific interests lay in the fields of image watermarking and pattern recognition. Dr Youssef has authored numerous scientific publications and communications in international conferences. He is a chairman of the IEEE conference (International Conference on Multimedia Computing and Systems). He is also a reviewer for several international conferences.

Lhoussain El Fadil is currently assistant professor of mathematics in the Polydisciplinary Faculty of Ouarzazat (FPO), Ibn Zohr University (Morocco). In 2004, he was awarded his PhD from Department of Mathematics and Computer Sciences in FST of Fez (Morocco). He was a post doc for one year in CRM of Barceleno (2008) and a fellow for one year in NTNU (Norway) (2009). He has authored several research papers in algebra, number theory and cryptography.