e-Health – For Continuity of Care
C. Lovis et al. (Eds.)
© 2014 European Federation for Medical Informatics and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
doi:10.3233/978-1-61499-432-9-745

Secure Teleassistance towards endless medical litigations: Identification of liabilities through a protocol using Joint Watermarking-Encryption Evidences

D. BOUSLIMI[a], G. COATRIEUX [a,1], C. QUANTIN[d-e], F.A. ALLAËRT[b], M. COZIC[c], Ch. ROUX[a]
[a]*Institut Mines-Telecom;Telecom Bretagne; Latim Inserm UMR1101, Brest, France.*
[b]*Health Claim Medical Chair ESC Dijon France.*
[c]*MEDECOM, Plougastel Daoulas 29470, France.*
[d]*CHRU Dijon, Service de Biostatistique et d'Informatique Médicale, Dijon, France.*
[e]*Inserm, U866, Univ de Bourgogne, Dijon, France.*

Abstract. Teleassistance is defined by the help provided through a telemedicine network by a medical practitioner to one other medical practitioner faced to a difficult case. One of the main limiting factors of its development is the fear of the practitioners to be involved in a litigation. In such a situation, the main issue is to determine as quick and as certain as possible if the damage is in relation with the tort of negligence and the liabilities of each involved physician. After a brief summary of the legal context, we present a protocol combining joint watermarking-encryption and a third party to enforce exchange traceability and therefore to bring valuable electronic evidence in case of teleassistance litigations.

Keywords. teleassistance, proof of data exchange, watermarking, encryption.

Introduction: teleassistance legal framework and medical litigations

The development of teleassistance began more than 20 years ago and has since demonstrated its efficiency [1]. Even though, technology strongly increased the quality and speed of image transmission, telemedicine only got a legal recognition in France in 2009 and its legal framework being defined in 2010 [2-3]. In this context, when a patient suffers of a prejudice related to a diagnostic error, it is necessary to determine the respective liabilities of the practitioners involved in the diagnostic/therapeutic process. Professional negligence will be argued if one of the practitioners involved in the teleassistance has had a negligent attitude, i.e. falling short of what might have been expected from him regarding his field of competence. To assess this possible lack of professionalism, and, thus, possible legal liability of one or both involved practitioners (joint liability), several questions will arise to allow the judge to reach a conclusion: Who made the request? What was requested? When? For whom? What documents were provided/requested? Who answered? What? When? Regarding which documents?

[1] Corresponding Author. Tel./Fax::+3-322-900-1508/1098; e-mail: gouenou.goatrieux@telecom-bretagne.eu.

In order to discover the process that originated the error and to give it a value of legal evidence [2-4], all the elements involved in the transaction must be stored; elements which can be identified according to the following needs [4]:

- ***N1***- Whole transmitted data have to be saved with the identity of all practitioners, the name of the patient, the date and the time of the transaction.
- ***N2-*** The date, time and substance of the answer of the referent practitioner must be strongly linked to the documents he received before sending it.
- ***N3-*** Save the substance of the answer of the referent with the identifiers of the physician, the specialist, the date and the time of the transaction.
- ***N4-*** Both practitioners must be identified in such a way they cannot repudiate their respective messages;
- ***N5-*** all elements involved in the transaction must be stored, with no means of modification, and rendered unreadable from an unauthorized access.

In this paper, in order to provide an appropriate response to these security needs, we propose a new secure tele-assistance protocol. This one takes advantage of Joint Watermarking-Encryption (JWE), a recent mechanism for digital content (e.g. images, medical report) protection which simultaneously offers confidentiality, integrity, authenticity and traceability functionalities [5-6]. The remainder of this paper is organized as follows. In section 1, we give a brief overview of JWE technique before presenting our protocol in section 2, and analyzing its security in section 3.

1. An overview of joint Watermarking-Encryption

Recently introduced in [5-6], a JWE algorithm conducts data encryption and data watermarking in a single operation process (see Fig.1). If encryption ensures data confidentiality, watermarking on its side can be used so as to verify data integrity and authenticity. We recall that watermarking [8] relies on two processes: embedding and reading. At the embedding stage, the message is inserted by modifying the host document (e.g. image, text) in an “imperceptible” way. “Imperceptible” means that the watermarked document can be used instead of the original document without interferences. Applied to an image; embedding consists in slightly modifying its pixel gray level values so as to insert the message in it. Image pixels are modified or modulated so that they can be interpreted/demodulated by the reader to gain access to the message. As depicted in Fig. 1, for digital images, the originality of JWE is that it allows the user to insert two messages, Ms and Me, which can be read/extracted in the encrypted and spatial domains, i.e. in the encrypted and decrypted image, respectively. The watermarking extraction functions fs and fe give access to Ms in the spatial domain and to Me in the encrypted image, respectively. Ms and Me can be security attributes (e.g. digital signature, unique identification number) that allow one user to verify the image integrity and authenticity even if this one is encrypted. If we consider the JWE function W_{emb}, the joint watermarked-encrypted version I_{we} of an image I is given as:

$$I_{we} = W_{emb}(I, M_s, M_e, K_e, K_{ws}, K_{we}) \qquad (1)$$

where K_e, K_{ws} and K_{we} are the encryption key and the watermarking keys in the spatial and encrypted domains, respectively. Embedded messages M_s and M_e can be extracted from I_{we} and its decrypted version I_{wd}, respectively as follows:

$$M_e = f_e(I_{we}, K_{we}); \; M_s = f_S(I_{wd}, K_{ws}) \qquad (2)$$

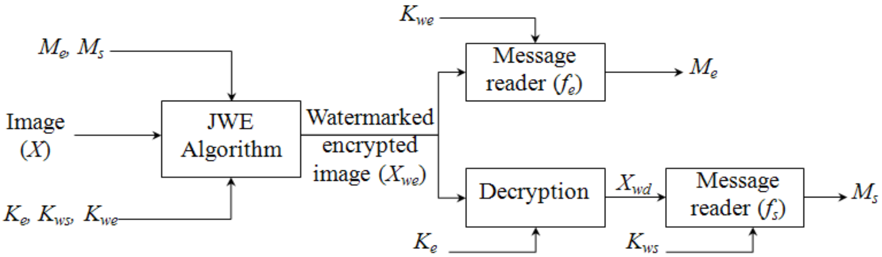

Figure 1. General system architecture of a JWE algorithm. M_e, M_s, K_e, K_{ws} and K_{we} are the message available in the encrypted domain, the message available in the spatial domain, the encryption key and the watermarking keys in the spatial and the encrypted domain, respectively.

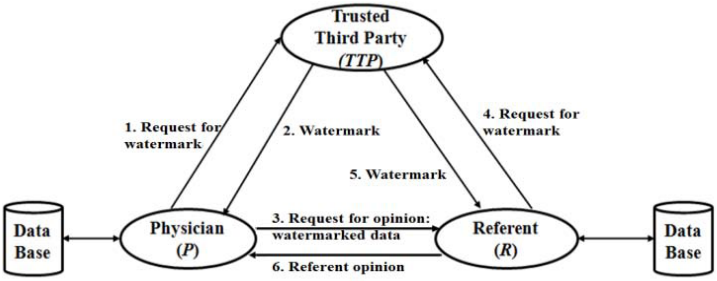

Figure 2. Teleassistance scenario and interactions between actors in the proposed protocol.

2. Liabilities identification through a secure teleassistance protocol based on JWE

In the proposed protocol, for one document, encryption ensures data confidentiality (*N5*) while the watermarking functionality contributes to: i) protect the document integrity (*N1*) by inserting into the document a proof of its integrity, ii) assess the document's origin and its attachment to one patient (*N1,N2*) by embedding the identifiers of the different entities involved in the exchange, iii) prove the identifier of the practitioner who received the document (*N3*) by inserting his identifier. We also suggest exploiting watermarking so as to introduce a secure link in between exchanged data not only for linking one document to the users and the transactions but also between the documents themselves. To do so, we embed within one document: practitioners and patient identifiers, its unique identifier (e.g. the DICOM UID), the transaction timestamp and a digital signature of the documents to which it is related with (*N2*). *N*on-repudiation need (*N4*), is commonly achieved with digital signatures.

To simplify the presentation of our protocol, let us consider the case where a physician (*P*) asks a Referent Physician (*R*) for a 2nd opinion (see fig. 2). The initial request may consist in images and any other elements that can participate to the decision making. Let's consider *X* is one element of this request. *R* analyzes the request and returns his answer by means of a report *Y* sent to *P*. Herein, we assume that each actor *u* involved in the transaction possesses its own public-private key pair (pK_u,sK_u). For reason of simplicity, we consider in the sequel that *X* and *Y* are images. Our protocol takes advantage of a third tierce party (*TTP*) considering that *P* and *R* can be dishonest trying, to falsify transaction data. Our protocol consists in three sub-protocols, we describe thereafter: “Request for Opinion”, “Opinion Response” and “Verification” which is called in case of litigation and where all evidence are sent to the *TTP*.

2.1. "Request for Opinion" sub-protocol

This three step sub-protocol allows *P* to securely send to *R* a document *X* while securely linking this latter to the recipient and the transaction by means of a watermark.

Step1: Generation of the watermark W^X: *P* requests the *TTP* for a watermark W^X by sending to it into an encrypted form: its identifier as well as those of *R,* the document and the patient; along with a digital signature. Based on this signature, the *TTP* verifies the origin and the integrity of the request before secretly generating W^X based on the received data and the transaction timestamp. Then, the *TTP* sends to *P*, W^X encrypted with pK_P along with its digital signature ($\mathrm{DS}_{\mathrm{TTP}}$ (W^X)). From W^X, the *TTP* will be able to re-link *X* to *P*, *R*, the patient and the transaction time and date (*N1*). When *P* receives the message, it decrypts W^X and verifies its signature so as to be sure that W^X was issued by the *TTP.*

Step2: Request transmission phase: Using the JWE algorithm (see section 1), *P* embeds within *X* two watermarks: W^X, which will be available in the spatial domain (i.e. M_s=W^X) and W^{eX}, which contains a reliability proof of *X* that will be available in the encrypted domain (i.e. $M_e = W^{eX}$). The obtained encrypted watermarked version X_{we} of *X* is then sent to *R*. *P* also saves $\mathrm{DS}_{\mathrm{TTP}}$($W^X$) and X_{we} in its database so as to ensure *N1*. DS_{TTP} (W^X) will serve as evidence proving that W^X was generated by the *TTP* and that it is the watermark we should retrieve into the decrypted version X_{wd} of X_{we}.

Step 3: Transmission of receipt acknowledgement: Using K_{we}, *R* extracts W^{eX} from the received encrypted data and verifies their integrity and origin without decrypting them. If it is ok, *R* returns to *P* an acknowledgement receipt which corresponds to the digital signature of X_{wd}: DS_{R}(X_{wd}). Notice that *R* cannot access to W^X because he does not know the spatial domain watermarking key K_{ws}. On its side, *P* save DS_{R}(X_{wd}) so that *R* will not be able to deny the reception of the request (*N4*).

2.2. "Opinion Response" sub-protocol

This three step sub-protocol aims at linking the different data involved in the response with the entities involved in the transaction as well as linking documents involved in the request and the response (*N3*). To do so, two watermarks are used.

Step1: Generation of the watermark W^Y: like *P*, *R* request the generation its watermark W^Y. After having generated W^Y based on the transaction timestamp and the identifiers of *P, R* and *Y* received from *R*, the *TTP* sends it along with $\mathrm{DS}_{\mathrm{TTP}}$($W^Y$) to *R*.

Step2: Referent opinion transmission: Before sending its answer *Y*, *R* generates a watermark *W* so as to link *Y* with *X*, using as example a digital signature of *X*. Then, he concatenates *W* with reliability proof of *Y* so as to build the watermark W^{eY}. W^{eY} and W^Y are next embedded using the JWE algorithm. The obtained watermarked encrypted document, Y_{we}, is transmitted to *P*. *R* securely also sends the watermarking key in the encrypted domain, K_{we}^r. *P* saves DS_{TTP} (W^Y) and Y_{we} (*N2*).

Step3: Transmission of receipt acknowledgement: After having verified the integrity/origin of *Y* and its link with *X* based on W^{eY}, *P* confirms the message reception by sending to *R* the digital signature the decrypted version Y_{wd} of Y_{we}: DS_{P}(Y_{wd}).

2.3. "Verification" sub-protocol

In case of litigation, *P* and *R* have to send their respective evidences to the *TTP*, it means: {DS_{TTP} (W^X), X_{wd}, DS_R(X_{wd}), DS_{TTP} (W^Y), Y_{wd}, DS_P(Y_{wd})}. Based on these elements of proof, the *TTP* verifies that: 1) the watermarks it has generated and embedded by *P* and *R* are the good ones. This task is conducted by comparing the watermarks' digital signatures extracted from X_{wd} and Y_{wd} to $DS_{TTP}(W^X)$ and $DS_{TTP}(W^Y)$; *2)* X_{wd} and Y_{wd} brought as evidence by *P* and *R* correspond to those really exchanged. For this, it is sufficient enough to verify DS_R (X_{wd}) and DS_P (Y_{wd}).

3. Security analysis

Among the issues and attacks to be considered [7], our protocol is more concerned by: the "*issue of non-repudiation*" and the "*collusion attack*". Regarding non-repudiation issues, both physicians cannot deny they sent/received data due to the facts: i) they embed their own identifiers (available in the encrypted domain) while signing encrypted data (see [5]); ii) each of them has acknowledged good data reception of data. In the case of a collusion attack- *P* and *R* may repeat the steps of the protocol in order to build evidence that innocent them. This can be detected through the timestamps and the images' identifiers, which will not correspond to those presented by the colluders.

4. Conclusion

In this paper, we have proposed a new secure teleassistance protocol. It takes advantage of Joint Watermarking-Encryption algorithm which simultaneously allows: securing communication in terms of confidentiality; providing proof of data reliability even if these ones are encrypted; providing evidence an exchange occurred and which data were involved by means of secure links established between them. With our protocol it is possible to retrieve documents that are content related. It is resistant to non-repudiation issue and collusion attack.

References

[1] C. Quantin, D.O. Jaquet-Chiffelle, G. Coatrieux, E. Benzenine, F.A. Allaërt, Medical record search engines, using pseudonymised patient identity: An alternative to centralised medical records, *International Journal of Medical Informatics* 80 (2011), 6-11.

[2] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine.

[3] A. Allaert, C. Quantin, Responsabilités et rémunérations des actes de télé-expertise, *Journal de Gestion et d'Economie Médicales* 30 (2012), 219-229.

[4] G. Coatrieux, C. Quantin, F.A. Allaert, B. Auverlot, Ch. Roux, Watermarking- a new way to bring evidence in case of telemedicine litigation, *Stud Health Technol Inform* 169 (2011), 611-615.

[5] D. Bouslimi, G. Coatrieux, M. Cozic, Ch. Roux, A joint encryption/watermarking system for verifying the reliability of medical images, *IEEE Transactions on Information Technology in Biomedicine* 16 (2012), 891–899.

[6] D. Bouslimi, G. Coatrieux, M. Cozic, Ch. Roux, A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images, *Computer Methods and Programs in Biomedicine* 106 (2012), 47-54.

[7] M. Deng, B. Preneel, Attacks on Two Buyer-Seller Watermarking Protocols and an Improvement for Revocable Anonymity, *Proc. ISECS* (2008), 923-929.

[8] G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, Ch. Roux, Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting, *IEEE Transactions on Information Forensics and Security* 8 (2013), 111-120.