International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Data Activity in Homomorphically Encrypted Medical Pictures for Corroboratory their Reliableness in Each En Crypted and Special Domains

Yadavalli Gopi*1, Shaik Dil Bahar2

*1Assistant Professor, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

2PG Student, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

In this paper, we propose another plan of information stowing away of encoded pictures with the end goal of checking the unwavering quality of a picture into both scrambled and spatial spaces. This plan couples the Quantization Index Modulation (QIM) and the Parlier cryptosystem. It depends on the inclusion of the picture, before its encryption, of a predefined watermark, a "pre-watermark". Message addition (resp. extraction) is directed into (resp. from) the scrambled picture utilizing an adjusted form of QIM. It is the effect of this inclusion procedure onto the "pre-watermark" that offers access to the message in the spatial space, i.e. after the picture has been decoded. With our plan, encryption/unscrambling forms are very autonomous of message implanting/extraction. One does not have to know the encryption/unscrambling key for concealing a message into the encoded picture. Analyses led on ultrasound medicinal pictures demonstrate that the picture bending is low while offering a high limit that can bolster distinctive watermarking based security destinations.

Keywords: Watermarking, Encryption, Distortion, Reliability, Biomedicalimaging,Biomedicaltrasonics, Cryptography, Medical Image Processing, Security of Data

I. INTRODUCTION

Distributed computing administrations end up plainly vital answers for the capacity and ceaseless accessibility of information provided by various sources. Because of the outsourcing of information and administrations, they are presented to numerous dangers that unequivocally increment security prerequisites as far as [1]: privacy, accessibility and unwavering quality (i.e. trustworthiness and verification). Among accessible security components, encryption is normally utilized to guarantee restorative information classification. Nevertheless, once decoded, one snippet of data is never again secured and it turns out to be difficult to check its uprightness and its starting point. Starting here of view, encryption shows up as a "from the earlier" insurance. Watermarking has been proposed as a correlative instrument that can enhance security of restorative pictures. When it is connected to pictures, watermarking adjusts or regulates the picture pixels' dim level esteems in an intangible route, with a specific end goal to encode or embed some security properties (i.e. the watermark) into it. As characterized, such an ensured picture can be gotten to while staying secured by these shrouded security traits that can be utilized for instance for confirming the picture unwavering quality (i.e., its trustworthiness, its causes and its connection to one patient). Along these lines, joining watermarking with encryption may permit us guaranteeing a from the earlier/a posteriori insurance in the meantime. Practically speaking, watermarking is typically led before encryption or amid the encryption/unscrambling forms. Nonetheless, to watermark outsoared information without jeopardizing security and information classification, distinctive methodologies have been proposed in order to install a message specifically into the scrambled picture, in the system of copyright insurance. Three classifications of methodologies can be recognized by the accessibility of the inserted message into the spatial space (i.e. after decoding process) as well as in the encoded space: —

Message accessible in the spatial area (MSD)- The plan proposed in [2] misuses homomorphism encryption, which permits altering a scrambled picture for the inserting of a watermark.

Message accessible in the encoded area (MED)- As case, in [3], the picture is right off the bat separated into patches. Before encryption, some patches are supplanted by patches registered from their scanty coefficients while the leftover blunders in the middle of patches are reversibly implanted into whatever is left of patches; leaving in this way some free space by next is utilized for message inserting in the scrambled area

Message accessible in both scrambled and spatial spaces (MSED)- the majority of these techniques depend on fractional encryption [4] or invariant encryption [5]. With those techniques, just a few sections of the host picture are encoded while whatever is left of it is watermarked. As of late, a novel idea, called VRBE (Vacating Room Before Encryption) has been proposed in [6]. Its standard is to reversibly watermark a picture before scrambling it to abandon some free space into the encoded area for message inserting. Be that as it may, to make conceivable the recovery of this free space into the encoded area, the picture must be revamped before encryption. Additionally, the unscrambling procedure is changed in order to make conceivable message extraction in the spatial space. As case, in [6] watermark able positions in the encoded picture are put toward the start of the bit stream and, at the gathering, watermarked positions are not decoded.

For whom? What reports were given/asked? Who replied? What? At the point when? As to archives?
Keeping in mind the end goal to find the procedure that began the blunder and to give it an estimation of legitimate confirmation, the accompanying needs should be fulfilled [4]:
N1 – Whole transmitted information must be spared with the iden-tity of all professionals, the name of the patient, the date and the season of the exchange.
N2 – The date, time and substance of the appropriate response of the ref-erent expert must be unequivocally connected to the reports he got before sending it.
N3 – Save the substance of the appropriate response of the referent with the identifiers of the doctor, the pro, the date and the season of the exchange.
N4 – Both experts must be recognized in such a way they can't disavow their particular messages;
N5 – All components required in the exchange must be put away, without any methods for change, and rendered mixed up from an unapproved get to.

Cryptography and watermarking instruments can add to a fitting reaction to these security needs if effectively dealt with by mean of a convention. Undoubtedly, cryptographic mecha-nisms give encryption and computerized signature offices which are the premise of security administrations like privacy, uprightness and non-renouncement. Be that as it may, once unscrambled or its computerized sig-nature erased or lost, one snippet of data is never again ace tected and it turns out to be difficult to check its respectability and its cause. Starting here of view, these cryptographic means, particularly encryption, rather show up as "from the earlier" security systems. Watermarking is later however is integral to cryp-tography [5]. Essentially, connected to one picture, it intangibly regulates its pixel dark esteems in order to encode a message inside it. Since the message is joined to the picture pixels, it can be recovered after a picture record arrange transformation. Watermarking has been proposed in the human services space with the end goal of checking information genuineness and uprightness [6] and for expanding information classification by blending quiet information and a picture into a watermarked picture [7]. As characterized, watermarking is an "a posteriori" control instrument as the picture content is as yet accessible for elucidation while staying secured.

These days, distinctive conventions [8–19] consolidate them keeping in mind the end goal to profit by the complementarity of these two components regarding from the earlier/a posteriori insurance, and thusly to give a superior security reaction. A large portion of them concentrate on the copyright assurance in the structure of video on request (VOD), where the goal is to recognize the individual (backer or beneficiary) at the starting point of an illicit appropriation by mean of a watermark (a unique mark). Conventions build up which elements, among the backer (the vender), the beneficiary (the purchaser) or an outsider, produce the watermark and when this later is implant ded inside a duplicate: at the merchant or beneficiary side or mostly at the dealer and beneficiary sides. We propose recognizing four classes of conventions relying upon the way they consolidate en-cryption and watermarking:

- "Watermarking Followed by Encryption" (WFE) [8,9,17] - where the guarantor creates and inserts the beneficiary finger print within a copy before encrypting it. Herein, the seller is considered as honest.
- “Encryption Followed by Watermarking” (EFW) [10–12, 18,19] - these methods take advantage of homomorphic en-cryption [20]. The homomorphic property allows the inser-tion within an encrypted copy of an encrypted watermark. This operation conducted in the encrypted domain is like inserting the watermark in the clear text. In that way, the issuer cannot access and has no idea of what the watermark or the watermarked copy look like. Hence, the buyer cannot claim that an unauthorized copy containing its fingerprint was created by the seller.
- “Joint Decryption–Watermarking” (JDW) [13–15,21,22] where watermarking is conducted during the decryption process.
- “Shared Watermark Insertion” (SWI) between the issuer and the recipient – the basic idea of this protocol is that both agreed on a watermark on which content they have no idea about. One solution proposed by Cheung et al. is based on commutative encryption [16].

Security targets in telemedicine (see N1, N5) contrast from that of VOD. As opposed to concentrating on backstabber following, the convention must acquire prove request to help the distinguishing proof of doctors' liabilities. This proof should help us to follow or figure out which information took an interest in the trade.

In this work, keeping in mind the end goal to give a superior reaction to the security needs in telemedicine, we propose another protected teleassistance convention. This one exploits Joint Watermarking–Encryption (JWE), a current system for burrow it al content (e.g. pictures, medicinal report) security which at the same time offers privacy, respectability, realness and traceability functionalities [23,24]. Not at all as if watermarking and encryption blend calculations utilized by the VOD protocols, which offer access to watermarking functionalities (i.e. the implanted message) just in the spatial area, the JWE instrument offers watermarking functionalities in both encoded and spatial spaces. With JWE, one can pick up in time calculation since it is not important to unscramble the picture to get to the watermark, an exorbitant operation specifically when a gigantic volume of information is considered. In the meantime, having the capacity to access to picture security traits while not decoding the picture keeps up classification insurance coherence. As we will see, the utilization of JWE approach enables us to better accomplish security goals in telemedicine. Moreover, the JWE system is consistent with DICOM,1 the standard of reference for restorative pictures

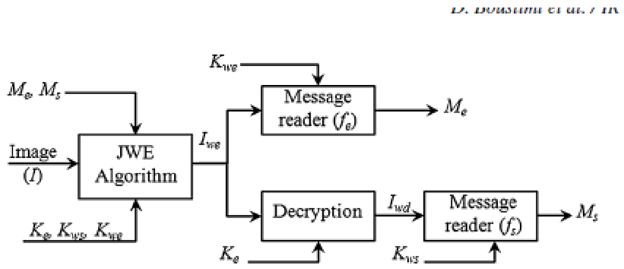

Figure 1. General overview of our system. I , I_{we} , I_{wd} , K_e , K_{ws} and K_{we} de-note the original image, the watermarked encrypted image, the watermarked decrypted image, the encryption key and the watermarking keys for the spatial and encrypted domain, respectively. M_e and M_s are the messages available in the encrypted domain and in the spatial domain, respectively.

II. An overview of joint watermarking–encryption algorithm

2.1. JWE: general principles

i. The JWE calculation, initially contemplated by Bouslimi et al. in the structure of medicinal imaging [23,24], has been proposed for the target of guaranteeing classification (by encryption) and offering watermarking functionalities like unwavering quality control in the spatial area, i.e. after picture has been unscrambled, and the scrambled space. To do as such, it conducts information encryption and watermarking in a solitary operation process and enables the client to embed two messages, Ms and Me , that will be accessible in the spatial and scrambled spaces, separately (see Fig. 1). Ms and Me can be some security traits (e.g. advanced signa-ture, special recognizable proof number) that for instance enable one client to confirm the picture honesty and validness despite the fact that this picture is encoded.
ii. To total up, in the event that we consider the JWE work Wemb, the joint watermarked–encrypted variant Iwe of a picture I is given as:

$$Iwe = Wemb(I, Ms , Me , Ke , Kws , Kwe) \qquad (1)$$

where Ke , Kws and Kwe are the encryption key and the wa- termarking keys in the spatial and encoded spaces, respec- tively. Two watermarking capacities fe and fsare considered so as to extricate installed messages Me and Ms from Iwe and its
unscrambled variant Iwd , separately:

$$Me = fe (Iwe , Kwe);$$

$$Ms = fs (Iwd , Kws) \qquad (2)$$

2.2. JWE execution in light of QIM

The accompanying execution blends the Quantization Index Modulation (QIM) [25], and an encryption calculation E, which can be a stream figure calculation (e.g. RC42) or a piece figure calculation (e.g. AES3). It permits embeddings one-piece mei of Me and one-piece msi of Ms inside a square Xi of the picture I. Before depicting how mei and msi are inserted into Xi amid its encryption, let us review the standards of QIM.

III. Liabilities Id Through A Safe Teleassistance Convention In Light of JWE

3.1. Teleassistance situation

To rearrange the introduction of our convention, let us consider the situation where a doctor (P) asks a specialist or a referent doctor (R) for a second sentiment (Fig. 3). The underlying solicitation may comprise of pictures and some other components that can take an interest in the basic leadership. The master breaks down the demand and returns his answer by methods for a report sent to P went with, if important, of any snippets of data that help his supposition. Thus, we expect that every element or on-screen character required in the exchange has its own particular cryptographic public–private key combine.

3.2. Cryptographic and watermarking apparatuses' motivations

In the proposed convention, for one record, encryption guarantees information classification (N 5) while the watermarking usefulness adds to:

i. protect the record honesty by embeddings into the report a proof of its respectability,

ii. assess the record's starting point and its connection to one patient (N 1, N 3) by installing the identifiers of the diverse substances required in the trade,prove the identifier of the practitioner who received the document (N 1, N 3) by inserting his identifier.

We also suggest exploiting watermarking so as to introduce a secure link 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 docu-ment: practitioners and patient identifiers, its unique identifier (e.g. the DICOM UID), the transaction timestamp and a digi-tal signature of the documents to which it is related with (N 2). Non-repudiation need (N 4) is commonly achieved with digital signatures.

3.3. Proposed protocol

As stated and depicted in Fig. 2, our protocol takes advan-tage of a trusted third party, which will be in charge of key management and watermark generation. This choice is because the practitioners can be dishonest. They can try, for exam-ple, to falsify transaction data. Our protocol consists of 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

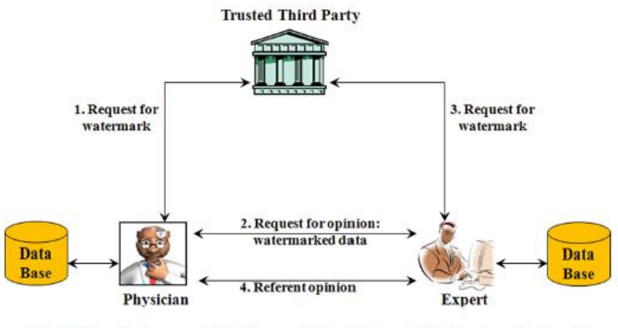

Fig. 3. Teleassistance scenario and interactions between actors in the proposed protocol.

IV. Security Analysis

Among the issues and attacks to be considered [27], our protocol is more concerned by: the “issue of non-repudiation” where the physician or the expert denies the emission or re- ception of data; the collusion attack” where both physicians cooperate to circumvent the protocol creating false evidencethat acquit them; The “traceability issue” which aim is to iden-tify the persons at the origin of a isclosure. We come back on each of them in the following.

4.1. Non-repudiation issue

In our protocol, both physicians cannot deny they sent/re-ceived data due to the following facts: i) they embed their own identifiers (available in the encrypted domain) while signing encrypted data (see Section 2 and [23]); ii) each of them has acknowledged good data reception of data. Then, they can-not repudiate data sending and reception. However, since the trusted third party keeps no tracks about which data have been exchanged, the physician and the expert may deny an exchange took place. In practice, such a situation is not realist in case of litigation due to the fact that only the physician P will be con-sidered as responsible. It is therefore not of his interest to deny an exchange occurred.

4.2. Collusion Attack

P and R may repeat the steps of the protocol in order to build evidence that acquit them. For instance, they can ask the TTP to generate new watermarks or insert watermarks previ- ously generated into documents different from those originally bexchanged. This can be easily detected by the TTP through the timestamp and the images' identifiers extracted from the water-marks which will not correspond with those presented by the colluders.

4.3. Traceability Issue

In case the referent discloses the document received from the physician, this latter one will be considered responsible. It is almost the same for the response of the expert. We retrieve an issue of traitor tracing, as in VOD scenario, similar to which an appropriate solution consists in using homomorphic encryption [10–12]. In that case, our protocol remains the same.

V. CONCLUSION

In this paper, we have proposed another protected tele-help convention. It exploits joint watermarking–encryption calculation, which at the same time permits: securing communica-tion as far as classification; giving verification of information relia-bility regardless of the possibility that these ones are encoded; giving confirmation a trade happened and which information were included by methods for secure connections set up between them. With our convention it is conceivable to recover reports that are content related. Hide thermore, the utilization of the JWE calculation makes the proposed convention consistent with the DICOM standard. It is impervious to non-disavowal issue and agreement assault, however delicate to follow capacity issue; issue we are as of now concentrating on.

VI. REFERENCES

[1]. Allaert FA, Weinberg D, Dusserre P, Yvon PJ, Dusserre L, Retaillau B, et al. Evaluation of an international telepathology system between Boston (USA) and Dijon: glass slides versus telediagnostic television monitor. J Telemed Telecare 1996;2(Suppl 1):27-30.

[2]. Decret n 2010-1229 du 19 octobre 2010 relatif a la telemedecine.

[3]. Allaert A, Quantin C. Responsabilites et remunerations des actes de tele-expertise. J Gest Econ Med 2012;30(4):219-29.

[4]. Coatrieux G, Quantin C, Allaert FA, Auverlot B, Roux Ch. Watermarking - a new way to bring evidence in case of telemedicine litigation. Stud Health Technol Inform 2011;169:611-5.

[5]. Coatrieux G, Maître H, Sankur B, Rolland Y, Collorec R. Relevance of watermarking in medical imaging. In: Proc. IEEE-EMBS int. conf. on information technology applications in biomedicine. 2000. p. 250-5.

[6]. Bouslimi D, Coatrieux G, Roux Ch. A joint watermarking/encryption al-gorithm for verifying medical image integrity and authenticity in both encrypted and spatial domains. In: Proc. int. conf. IEEE-EMBC. 2011. p. 8066-9.

[7]. Rajendra Acharya U, Niranjan UC, Iyengar SS, Kannathal N, Min LC. Simultaneous storage of patient information with medical images in the frequency domain. Comput Methods Programs Biomed 2004;76:13-9.

[8]. Loytynoja M, Cvejic N, Lahetkangas E, Seppanen T. Audio encryption using fragile watermarking. In: Proc. fifth international conference on in-formation, communications and signal processing. 2005. p. 881-5.

[9]. Seungwoo H, Hakjae K, Sungju L, Yongwha C. Analyzing the secure and energy efficient transmissions of compressed fingerprint images using en-cryption and watermarking. In: International conference on information security and assurance. 2008. p. 316-20.

[10]. Memon ND, Wong PW. A buyer-seller watermarking protocol. IEEE Trans Image Process 2001;10(4):643-9.

[11]. Charpentier A, Fontaine C, Furon T, Cox I. An asymmetric fingerprint-ing scheme based on Tardos codes. In: 13th international conference on information hiding, vol. 6958. 2011. p. 43-58.

[12]. Rial A, Deng M, Bianchi T, Piva A, Preneel B. A provably secure anony-mous buyer-seller watermarking protocol. IEEE Trans Inf Forensics Secur 2010;5(4):920-31.

[13]. Anderson R, Manifavas C. Chameleon - a new kind of stream cipher. In: Proceedings of the 4th international workshop on fast software encryption, vol. 1267. 1997. p. 107-13.

[14]. Piva A, Bianchi T, De Rosa A. Secure client-side ST-DM watermark em-bedding. IEEE Trans Inf Forensics Secur 2010;5(1):13-26.

[15]. Celik M, Lemma AN, Katzenbeisser S, van der Veen M. Secure em-bedding of spread spectrum watermarks using look-up-tables. In: Proc. international conference on acoustics, speech and signal processing, vol. 2. Hawaii (USA): IEEE Press; 2007. p. 153-6.

[16]. Cheung S, Leung H, Wang C. A commutative encrypted protocol for the privacy protection of watermarks in digital contents. In: Proceedings of the 37th annual Hawaii international conference on system sciences, vol. 4. 2004. p. 40094a.

[17]. Metkar SP, Lichade MV. Digital image security improvement by inte-grating watermarking and encryption technique. In: IEEE international conference on signal processing, computing and control. 2013. p. 1-6.

[18]. Kuribayashi M. On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol. EURASIP J Multimed Inf Secur 2010;2010:1:1-1:11.

[19]. Lei C-L, Yu P-L, Tsai P-L, Chan M-H. An efficient and anony-mous buyer-seller watermarking protocol. IEEE Trans Image Process 2004;13:1618-26.

[20]. Fontaine C, Galand F. A survey of homomorphic encryption for nonspe-cialists. EURASIP J Multimed Inf Secur 2007;2007(1):1-15.

[21]. Prangjarote P, Lin C-Y, Yeh C-H. High efficient joint fingerprinting and decryption for multimedia distribution. In: 9th international conference on information, communications and signal processing. 2013. p. 1-5.

[22]. Bianchi T, Piva A. TTP-free asymmetric fingerprinting protocol based on client side embedding. In: IEEE international conference on acoustics, speech and signal processing. 2014. p. 3987-91.

[23]. Bouslimi D, Coatrieux G, Cozic M, Roux C. A joint encryption/water-marking system for verifying the reliability of medical images. IEEE TITB 2012;16:891-9.

[24]. Bouslimi D, Coatrieux G, Roux Ch. A joint encryption/watermarking algorithm for verifying the reliability of medical images: applica-tion to echographic images. Comput Methods Programs Biomed 2011;106(1):47-54.

[25]. Chen B, Wornell GW. Quantization index modulation: a class of prov-ably good methods for digital watermarking and information embedding. IEEE Trans Inf Theory 2001;47(4):1423-43.

[26]. Coatrieux G, Quantin C, Montagner J, Fassa M, Allaërt F-A, Roux Ch. Watermarking medical images with anonymous patient identification to verify authenticity. Stud Health Technol Inform 2008;136:667-72.

[27]. Deng M, Preneel B. Attacks on two buyer-seller watermarking protocols and an improvement for revocable anonymity. In: Proc. ISECS. 2008. p. 923-9.

[28]. http://esante.gouv.fr/espace-cps/guide/la-cps-carte-d-identite-electronique-des-professionnels-de-sante.