The New Navigators: from Professionals to Patients
R. Baud et al. (Eds.)
IOS Press, 2003

Image integrity verification in medical information systems

Jozsef Lenti[a], Istvan Lovanyi[a]

[a]*Budapest University of Technology and Economics, Budapest, Hungary*

Abstract

In nowadays it is a major objective to protect healthcare information against unauthorized access. Comparing conventional and electronic management of medical images the later one demands much more complex security measures. We propose a new scenario for watermark data buildup and embedding which is independent from the applied watermarking technology. In our proposed method the embedded watermark data is dependant on image and patient information too. The proposed watermark buildup method provides watermark information where it is small in size and represents a unique digest of the image and image related data. The embedded data can be considered unique with high probability even if the same algorithm was used in different medical information systems. Described procedures ensure new, more secure links between image and related data, offering further perspectives in smartcard implementations.

Keywords:

Medical Informatics; Computer Security; Data Protection; Data Security; Compromising of Data; Information Protection; Watermarking

1. Introduction

Modern healthcare is based on digital information management, where patient data and all medical information is stored and processed by computer systems. Healthcare informatics creates new perspectives but it is evident that IT based solutions cannot affect patient care. It is a main objective to protect health information of individuals against unauthorized access. Several standards define security measures to be implemented in healthcare. For instance in US HIPAA regulations cover privacy and security of patient healthcare data. DICOM, HL7, CEN251 Working Groups are also facing different aspects of the problem. [1] In this paper we are focusing on the management of medical images, discussing the verification of their integrity and authenticity, we are proposing new methods for watermark data generation.

2. Security in medical systems

The medical patient record contains various information about examinations, annotations, diagnosis information, prescriptions – in general the medical history of a patient, including medical images. Medical patient record might be collected by health professionals in various locations, and collected data is called Electronic Patient Record (EPR). Due to medical secrecy regulations collected data should be stored and handled confidentially. [2]

The authentication of patients and healthcare professionals can be based on various solutions like username and password combination, biometric and token based authentication mechanisms. Smartcards are appropriate for most medical environments, it is possible to store authentication and many additional (patient related) information on them. For authentication purposes a common solution is to store certificates on the smartcard,

which can be used for authentication, and to create digital signatures with them. Our proposed method is not based on smartcard authentication and digital signatures of the patient or the healthcare professional, but can be extended and provide further advantages in case of smartcard implementation.

In case of medical image integrity verification watermarking is one possible solution, which has several advantageous properties. If the data which carries additional information – used for integrity or authenticity verification etc. of an image – is handled separately from the image the procedure may be sensitive to errors, since there is no strict link between the image and data file. If the data is embedded in the image it ensures that the image and the additional information is handled and processed together. The number of studies on watermarking of medical images is relatively small. Anand et al. [3] proposed insertion of the encrypted EPR record into the least significant bit (LSB) of image pixels. Miaou et al. [4] proposed also a solution which is based on LSB insertion where the embedded data is composed of various patient data. The embedded information should be linked to the image and to the patient also. In case of medical images there are always associated data belonging to the image [5].

3. Building up authorative watermark data

Aiming to link the embedded watermark data to the image it is needed that the watermark information would be derived from the image data or from specific image properties. It can be a digest of the complete image or digest of specific image properties such as the LL band components in wavelet domain, or based on ROI (Region of Interest) part of the image [2]. The digest should be constructed in a way, that given a digest which is generated from a specific image it should be fairly impossible to find another image from which the same digest could be produced. A mathematic hash function can fulfill these requirements, and can be used to generate digest from images or image properties.

To connect the generated hash to the patient data a Trusted Third Party (TTP) could be used. The responsibility of the TTP would be to certify that the hash belongs to a certain patient. We propose to apply a digital signature of the TTP where a timestamped hash – which is generated from the image and from added patient information – should be digitally signed. The TTP signs the hash so there is no need to send the original image to the TTP, only the computed hash value, and authentication information about the sender. An advantage of this solution is that neither healthcare professionals nor patients need certificates, since the digital signature will be made by the TTP. Because the TTP does not have any sensitive information it can be an entity within or outside the medical information system as well.

In watermarking applications it is important to minimize the size of embedded information. In case of digitally signed documents, the digital signature and the certificate of the signer are attached to the original document, and these components are stored and processed together. The size of the digital signature itself varies depending on the applied cryptographic technique. In case of RSA signatures – which are most commonly used nowadays – the size of the signature is 1024 bit when 1024 bit keys are being used. The size of the attached certificate depends on the various extension fields which can be defined according to the X.509v3 standard, but if we suppose that 1024 bit keys are used it is at least 1024 bit long. It means that in case of RSA signatures the size of the data is increased at least with 2048 bits – since the encrypted hash and the certificate is also added to the document [6]. We propose that only the hash of the encrypted hash and the certificate should be embedded as a watermark data, which is 128 bits long, if we suppose that MD-5

algorithm is used to calculate the hash value. Our proposed watermark data generation process is the following:

1. Create the hash from the medical image (it can be based on the complete image or on image specific properties) and from patient information (the information can be any patient related information, and can also contain information about the healthcare professional who created or processed the medical image):

H=hash({medical image | specific properties of the medical image, patient related data}) (1)

2. H is sent to the TTP, a timestamp and a digital signature is added to it, then it is sent back to the medical information system (the signature is created using the private key of the TTP), the computed S is stored in the medical information system:

S={H, timestamp, digital signature of the TTP, TTP's certificate}=sign(timestamp(H),H) (2)

3. Since the size of S is at least 2048 bits long (if we suppose, that RSA signatures with 1024 bit key are used), the hash of S is computed:

$$W = \text{hash}(S) \quad (3)$$

4. The computed W is used as watermark information which should be embedded into the medical image I, where the result I_W is the watermarked image:

$$I_w = watermark\_embedding(I, W) \quad (4)$$

The first two steps are similar to a conventional digital signature generation process, although there are significant differences. In our proposed method the digital signature can be based on the complete image or on specific image properties – like the ROI data or other image specific information which is uniquely related to the image. The digital signature is created by a TTP. Since the TTP does not need the image data for signature creation the secrecy of that is provided. In the second step, the original hash and the digital signature components are sent back to the medical information system, the signature can be verified using the public key of the TTP.

In the third step the hash of the digital signature and the original hash is computed and it can be used as watermark information which should be embedded into the image data. The output of the hash function provides small size output. The most commonly used hash functions are SHA and MD-5, which are providing 160 and 128 bit output respectively. The third step – where the hash of the digital signature is computed – is weakening the security of the digital signature, but it can provide still high level of security. In case of hash functions computationally it is extremely difficult to find M if the result of the hash function H=hash(M) is given. Even slight differences in M will result completely different H values. One way hash functions have the following characteristics [6]:

- The output of the hash function is a fixed length hash value: H=hash(M), where H is of length k, and M is an arbitrary-length message
- Given M, it is easy to compute H, given H, it is hard to compute M
- Given M, it is hard to find another message, M', where H(M')=H(M). In general to provide collision-resistance it is hard to find two random messages M and M' where H(M)=H(M')

It means that that the hash value can be easily computed from the digital signature data which was generated by the TTP. Since the hash and the signature are stored in the medical information system it can be used as a link to a patient record. This link would be false if the same hash would be generated from two different signatures in the third step. It is related to the collision probabilities of the hash functions, which are upper bounded by $1/2^{128} = 2.93^{-39}$ in case of MD-5, and $1/2^{160} = 6.84^{-49}$ in case of SHA, which can be considered as an acceptable risk [6, 2].

In case of medical images it is required, that the image should be presented in high quality and in original format. In the proposed solution we suppose that reversible watermark embedding method is used.

4. Integrity verification

Suppose that a watermarked medical image I_{W1} should be verified where it is known that S_1 data – which is stored in the medical information system – should belong to the image.

1. The embedded watermark is extracted from I_{W1}:

$$W_1 = watermark\_extract(I_{W1}) \quad (5)$$

2. The hash of the stored S_1 value $W_1^{'}$ is computed and compared with the extracted watermark W_1.
3. The watermark W_1 is removed from the watermarked image I_{W1} – it is feasible since we suppose that reversible watermark embedding method was applied in the embedding process. After removing the watermark the hash $H^{'}_1$ is calculated from the unwatermarked image or from image specific properties and from patient data. S_1 contains H_1, the hash of the image or hash of image specific properties and patient data. $H^{'}_1$ is compared with H_1.
4. The digital signature of the TTP is verified, using the stored H_1, and the public key of the TTP.

If $W_1^{'}$ equals W_1 and $H^{'}_1$ equals H_1 and the digital signature of the TTP is valid it means that the image was not modified, its integrity is verified.

S cannot be calculated from patient information again, since timestamping was used in the process, which means that the same S cannot be calculated again from patient and image data – this is the reason why it should be stored in the medical information system. Comparing the extracted value with the hashed S, it can be checked that a given picture was not modified, and it really belongs to a given patient.

Suppose that a watermarked image should be verified, but there is no information which patient does the picture belongs to. The patient data can be found which the medical image belongs to by comparing the watermark data with the hashed S values stored in the medical information system. It means that the S should be found where the hash value of S is identical with the watermark data stored in the medical image. This process can be accelerated if the W values are also stored in the medical information system.

5. Attacks

Usually the aim of watermarking attacks is to destroy the embedded watermark or to prohibit its detection. If the watermark data is used for integrity verification destroying the watermark means that the image integrity cannot be verified. In this case a successful attack would mean that the watermarked medical image is modified and even after the integrity checking process the modification cannot be detected. A watermark copy attack – presented by Kutter, Voloshynovskiy and Herrigel in [7], does not destroy the embedded watermark but copies it from one image into a different one. The attack is based on watermark estimation where the estimated watermark is embedded into the target image. This attack can compromise the link between the cover image and the embedded information.

The solution offered provides watermark data which is linked to the medical image and to patient information. Because of this property it is useless to copy the watermark information from one image into another, because it can be easily detected. In the watermark copy attack a watermark W_1 from watermarked image I_{W1} is embedded into image I_2, and will result a forged watermarked image I_{W2}. In the watermark copy attack the fist step is to estimate the embedded watermark data in I_{W1}. Suppose that the attack is successful, W_1 is exactly estimated and properly embedded into I_{W2}. The attacker sends the forged I_{W2} image to the medical information system instead of I_{W1}, and the verification of I_{W2} should be done by the medical information system.

In our proposed verification process the first step is the extraction of the embedded watermark. Since we suppose that the watermark was successfully embedded into I_{W2} image W_1 watermark data will be extracted from that. If I_{W1} was not a valid medical image there is no S_1 value stored in the medical information system from which W_1 could be computed – the integrity of the image cannot be verified. The probability that the medical information system contains such S_X, from which W_1 could be computed equals with the collision probability of the hash function. If I_{W1} was a valid medical image there is an S_1 value in the medical information system from which W_1 could be computed, where $W_1 = hash(S_1)$ and where S_1 value belongs to I_{W1}. It means that in the verification process no error is detected in the second step. In the third step W_1 is removed from I_{W2} which will result the unwatermarked image I_2. From I_2 and from patient data the hash H'_1 is calculated and compared with H_1 which is part of the stored S. Since the calculated H'_1 will be different from the stored H_1 value (if I_1 and I_2 are different – and even if the patient information is the same – their hash will be different also; the probability that despite the difference the hash values will be the same equals the collision probability of the hash functions) in the third step the verification process will detect the error.

6. Conclusion

The role of image integrity verification in case of medical images has been considered. The solution offered a watermark data buildup and a verification process where the medical image integrity could be checked. The advantage of this solution is that watermark data depends on medical image and patient data as well and this connection is guaranteed by the TTP. This solution is independent from the embedding method, and it makes recommendation for the embedded watermark information. The embedded data can be

considered as unique – even if the same algorithm is used in many medical information systems, with high probability the embedded information will be unique for each medical image, where it could be used as a unique identification number. In the proposed method we did not suppose that either the healthcare professional or the patient had personal certificates to create digital signatures, but the solution can be extended to such cases where the digital signature of the patient and the healthcare professional is being used. Our steganographic algorithms and procedures ensure new, more secure links between image and related data, offering further advantages in case of smartcard implementation.

7. References

[1] Paper published by the Security and Privacy Committee. Security and Privacy: an Introduction to HIPAA. *Medical Imaging and Informatics Section*, NEMA 2001

[2] G. Coatrieux, B. Sankur, H. Maitre, Strict Integrity Control of Biomedical Images, SPIE Conf. 4314: *Security and Watermarking of Multimedia Contents III*, 22-25 Jan. 2001, San Jose USA

[3] D. Anand, U. Niranjan. Watermarking Medical Images with Patient Information, *IEEE/EMBS Conference*, Hong Kong, China, 1998, pp 703-706

[4] S. Miaou, C. Hsu, Y. Tsai, H. Tsao. A Secure Data Hiding Technique with Heterogeneous Data-Combining capability for Electronic Patient Records, *Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Healthcare Records*, IEEE-EMB, Chicago, USA, 2000

[5] N.J.G. Brown, K.E. Britton, D.L. Plummer: Standardisation in medical image management International *Journal of Medical Informatics* 48, 1998, pp 227-238

[6] Bruce Schneier. *Applied cryptography Second Edition.* John Whiley and Sons Inc. 1996

[7] Martin Kutter, Sviatoslav Voloshynovskiy, Alexander Herrigel, The watermark copy attack, Electronic Imaging 2000, Security and Watermarking of Multimedia Content II

[8] M. Steinder, S. Iren, and P. Amer. Progressively authenticated image transmission, *MILCOM'99*, Atlantic City, NJ, October 1999

[9] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec. Relevance of Watermarking in Medical Imaging. *2000 IEEE EMBS Conf. On Information Technology Applications in Biomedicine*, Nov. 2000, Arlington, USA. , p 250-255

[10]F. Mintzer, G.W. Braudaway, and M. M. Yeung. Effective and ineffective digital watermarks. *IEEE ICIP, volume III*, Santa-Barbara, Cal, October 1997, pages 9--12

[11]Ingemar Cox, Matthew Miller, Jeffrey Bloom. *Digital watermarking.* Morgan Kaufmann Publishers, 2001

[12]Lesley R. Matheson, Stephen G. Mitchell, Talal G. Shamoon, Robert E. Tarjan, Francis Zane, Robustness and security of digital watermarks, Financial *Cryptography FC-98, volume 1465 of Lecture Notes in Computes Science*, Springer, 1998, pages 227-240

[13]Akiyoshi Wakatani. Digital Watermarking for ROI Medical Images by Using Compressed Signature Image. *35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 6*, 2002 Big Island, Hawaii

8. Address for correspondence

Jozsef Lenti

Budapest University of Technology and Economics

Email: lenti@iit.bme.hu, URL: www.iit.bme.hu

Phone: +36 209 127626

Postal address:

Allende park 10., 1119 Budapest, HUNGARY