Efficient erasable watermark embedding in medical images

József Lenti
Department of Engineering and Information Technology
Budapest University of Technology and Economics
Pázmány Péter sétány 1/D, H-1117
Budapest
Hungary
lenti@iit.bme.hu

István Loványi
Department of Engineering and Information Technology
Budapest University of Technology and Economics
Pázmány Péter sétány 1/D, H-1117
Budapest
Hungary
lovanyi@iit.bme.hu

Zoltán Dezső
Department of Engineering and Information Technology
Budapest University of Technology and Economics
Pázmány Péter sétány 1/D, H-1117
Budapest
Hungary
dz335@hszk.bme.hu

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. Medical image integrity verification using watermark technology may have several advantageous properties.**

In case of medical images it is important that the original image should be kept intact. When a watermark is embedded into an image it will be modified – the degree of the modification depends on the applied embedding mechanism and on the size of the embedded data. The embedded data can be used for various purposes like ownership or integrity verification. If the original image should be provided to the receiver erasable watermark mechanism must be used in the embedding process. In this article we propose a new scenario for the construction process of erasable watermarks.

I. INTRODUCTION

Modern healthcare is based on digital information management, where the patient data and all the medical information is stored and processed by computer systems. Extensive use of computer based applications and the development of the information infrastructure provides new possibilities for telemedicine applications like telediagnosis, teleconsulting and telesurgery. Till nowadays healthcare focused mainly on the treatment of the patient. Healthcare informatics creates new perspectives. On the other hand it is evident that introduction of new IT based solutions cannot affect patient care. Many healthcare practitioners may have gathered experience dealing only with paper and film. Even to maintain the security for electronically handled information different measures are required. 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. The main three concepts of medical security are: confidentiality, reliability and availability [1].

In this paper we are focusing on the management of medical images, discussing the watermark embedding mechanism. We are proposing method for watermark data embedding, where the embedded watermark is erasable but still secure. Our proposed method could be applied to all types of medical images which are electronically maintained without hurting the conventional image handling principles.

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

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 image watermarking of medical images is relatively small. Anand et al. [2] proposed insertion of the encrypted EPR record into the least significant bit (LSB) of image pixels. Miaou et al. [3] proposed also a solution which is based on LSB insertion where the embedded data composed of various patient data.

In case of medical image reliability verification it should be checked that the image has not been modified by any non-authorized person and that the image belongs to a claimed patient. To ensure these 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 [4]. These can be for example the technical parameters of image acquisition or visualization, type of contrast media, clinical data such as the context of the medical examination, patient identifier, etc.. In most cases associated data is necessary to set up a diagnosis. In medical information systems – especially when they try to interoperate with each other – there is a need for unique image identification technique which could guarantee the consistency of the image and associated information. In this paper we propose a watermark data embedding and buildup procedure – independent from the applied watermarking technology. We propose a watermark data buildup procedure, where the embedded data is linked to the image and to patient information too. The information associated to medical images can be considered as patient related data, which varies depending on the type of the medical image – these could be different in case of MRI

images, X-Ray images and so on. In this paper we do not focus on the specification of image related data, we are considering it as a patient-related data, where the content can be image-dependant.

II. ERASABLE WATERMARK EMBEDDING MECHANISM

In some application such as medical images even the minimal distortion caused by the embedding process is unacceptable. An engineer might be convinced that for example a small amount of embedded data will not change the doctor's interpretation of an image, but probably the same arguments would be less persuasive in a courtroom. In these cases the only way to guarantee that no significant changes has been made is for there to be no change at all.
Erasability requires that the original work can be recovered from the watermarked work. The construction of an erasable watermark poses a fundamental problem [5]; theoretically it is impossible to make an erasable watermark that can be embedded in 100% of the content. Friedrich et al. [6, 7] have proposed a variety of algorithms that try to work around this issue.
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 [8]. This digest should be unique – a different digest should be generated from each different image. 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. An algorithm is provided in [9] which fulfils these requirements.
Medical images – such like other images – can be segmented, the Region Of Interest (ROI) part can be determined. The remaining part of the image can be segmented further based on other principles. Our embedding mechanism uses segmenting algorithms which are independent of the embedding mechanism, but the same segmenting methods should be used on the watermark embedding and on the receiving side.
The proposed embedding method is the following:

1. $ROI = \{I_{Bx}\}$ where $roi(I_{Bx}) = 1$ x=1..N (1)

where I=$\{ I_{Bx} \}$ x=1..N
Which means that the ROI part will contain those image blocks where the roi() function provides a positive result.
The original image I consists of N I_{Bx} image blocks. The roi(I_B) function selects the Region Of Interest parts of the image which means that those image blocks will be part of the ROI where the roi() result is 1.

$$roi(I_B) = \begin{cases} 1 \rightarrow I_B \in ROI \\ 0 \rightarrow I_B \notin ROI \end{cases} \quad (2)$$

$$O = \{I_{Bx}\} \text{where } roi(I_{Bx}) = 0 \text{ x=1..N} \quad (3)$$

O will contain those image blocks which are not part of the ROI region, where the roi() function gives negative result.

2. Generation on the embedded watermark data W_D based on the image, and on selected part of the EPR data as described in detail in [9].
3. Select those O_i blocks where W_D can be embedded into. We suppose – since the embedded data is small – that it is always possible for the emb() function to embed the watermark data into O_i blocks. Since medical images have high resolution image block size should be chosen such a way where the embedding of the given data size is feasible. The embedding function which embeds W_D into the original image I is emb(I, W_D) and its result is the watermarked image I_W.

$$O = \{O_i\} \text{ i=1..M} \quad (4)$$

$$O' = \{O_i\} \text{ where } roi(emb(emb(O_i, W_D), W_D)) = 1, \text{ i=1..M} \quad (5)$$

$$O'' = \{O_i\} \text{ where } roi(emb(emb(O_i, W_D), W_D)) = 0, \text{ i=1..M} \quad (6)$$

where O'' will contain those image blocks where the generated watermark data W_D can be embedded. Image blocks of O'' will contain the embedded watermark information, the image blocks of O' will not contain embedded information.
4. Embed the generated watermark data W_D into O'' blocks:

$$O''_W = \{emb(O_j, W_D)\} \text{ where } O_j \in O'' \text{ and j=1..M} \quad (7)$$

The embedding function emb() embeds the generated watermark data into each image block in O''.

5. The O'' blocks in the original image I will be replaced by O''_W blocks, the result will be the watermarked image I_W:

$$I_W = \begin{cases} I_{WBk} = I_{Bk} \text{ where } I_{Bk} \in ROI \text{ k=1..N} \\ I_{WBk} = I_{Bk} \text{ where } I_{Bk} \in O' \text{ k=1..N} \\ I_{WBk} = O_W'' \text{ where } I_{Bk} \in O'' \text{ k=1..N} \end{cases} \quad (8)$$

The embedded W_D is generated by the Trusted Third Party (TTP) and unique for each picture, it depends on the image and some selected EPR information [9]. We propose to work with the embedding key – it is used during the watermark embedding and detecting process – which is calculated from the ROI part of the image. It can be for example the first 56 bit of the hash output of the ROI data (the required key size depends on the applied embedding algorithm) [10].

The image integrity verification process is the following:

1. $ROI = \{I_{Bx}\}$ where $roi(I_{Bx}) = 1$ x=1..N (9)

where I={ I_{Bx} } x=1..N

$$roi(I_B) = \begin{cases} 1 \rightarrow I_B \in ROI \\ 0 \rightarrow I_B \notin ROI \end{cases} \quad (10)$$

$$O = \{roi(I_{Bx}) = 0\} \text{ x=1..N} \quad (11)$$

2. Determine those O_i blocks where W_D was embedded into.

$$O = \{O_i\} \text{ i=1..M}$$

$$O' = \{O_i\} \text{ where } roi(emb(emb(O_i, W_D), W_D)) = 1 \text{ i=1..M} \quad (12)$$

$$O_W'' = \{O_i\} \text{where } roi(emb(emb(O_i, W_D), W_D)) = 0 \text{ i=1..M} \quad (13)$$

O_W'' contains those image blocks where watermark data W_D is embedded.

3. Extract the watermark data W'_D from O_W'' blocks:

$W'_D = \{ext(O_j)\}$ where $O_j \in O_W''$ j=1..M, (14)

during the extracting process the same watermarking key should be used as in the embedding process.The ext() function extracts the embedded watermark data from image blocks.

The integrity verification is done by comparing the extracted W'_D and the original watermark data W_D. If these are identical the image integrity is intact. The details of integrity verification is described in [9].

4. Since the watermarking key and the embedded data is known at the receiver side – if the image integrity verification was successful – the embedded watermark can be removed:

$$O'' = \{rem(O_i, W_D)\} \text{ i=1..M} \quad (15)$$

The rem() function removes the embedded watermark data from image blocks, it is possible if the embedded data and the key is known which was used during the embedding procedure. In this case both of that are known and the removal is possible. Because the embedding function and the embedded information are known for the receiver of the image for the removal there the knowledge of the original image block is not required for the removal [5, 10].

III. ANALYSIS OF THE EMBEDDING ALGORITHM

Since the image blocks in the ROI part of the original image will not be modified during the embedding process the image can be seen and analyzed even before the image integrity verification would be processed and the embedded information would be extracted. If the roi() function selects the most important part of the image properly than the relevant part of the image will be shown on the watermarked image intact.

In general the key which is used during the embedding process should be kept secret – in case of copyright protection application it is possible to remove the embedded copyright information if the attacker has this key. If in the proposed algorithm the embedded watermark is removed than during the verification procedure it would be detected that the image doesn't contain appropriate watermark and the verification would give a negative result. The embedded watermark can be removed knowing the algorithm details, so it is not possible to use it like copyright protection. The attacker could succeed only if he would be able to modify the image and afterward embed such a watermark data where the integrity checking process wouldn't detect the change. Since the watermark data generation is based on the image and some related data and in the calculation process a TTP is also involved it is not possible to modify the image – this alteration would be detected during the verification process, when the validity of W_D is checked. To generate a false W_D data is considered to be impossible since the private encryption key of the TTP would be required which is considered to be kept secure.

IV. CONCLUSION

The offered solution offers erasable watermark embedding possibility where the embedded watermark could be used for integrity verification purposes. The embedding solution cannot be used to hide copyright information into images, but for image integrity verification it offers erasability. The watermarked image can be analyzed even before the integrity verification would have been finished and the watermark removal would have happened since the ROI part of the image will not be modified during the embedding procedure.

V. ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions of the Hungarian Ministry of Education by granting the R&D project IKTA 144/2000.

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

[3] 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

[4] 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

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

[6] J. Friedrich, M. Goljan and M. Du, *"Invertible Authentication"*, "Proceedings of SPIE, Security and Watermarking of Multimedia Contents", 2001

[7] M. Goljan, J. Friedrich and R. Du, "Distortion-free Data Embedding for Images", *Fourth International Information Hiding Workshop*, 2001

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

[9] Jozsef Lenti, Istvan Lovanyi. *"Image integrity verification in medical information systems"*, "Proceeding of MIE2003, The New Navigators: from Professionals to Patients, Medical Image Information Systems", pp 286-291

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