A Novel Watermarking Technique for Medical Image Authentication

K Pushpala, R Nigudkar

Wipro Technologies, Bangalore, India

Abstract

Medical images are stored in PACS (Picture Archiving and Communication Systems) that are accessed over the intranet by radiologists for diagnosis. These days the trend is shifting towards a web based interface for accessing PACS (image) data. This calls for thorough security measures in the information system of the hospital to ensure integrity of medical image data that is being transferred over the public network.

The paper analyses various watermarking techniques with a perspective of applying them to medical images stored on the PACS. It discusses the applicability of invertible watermarking technique for ensuring integrity of medical images.

Any modification to the watermarked DICOM (Digital Imaging and Communications in Medicine) image can be detected with high reliability using invertible fragile watermarking system. A unique content based digital signature can be generated from the image data (pixel data) which would be embedded inside the image in an imperceptible way without increasing the data size that need to be transferred. This signature can be extracted at the radiologist viewer work stations and used for the authentication while the modified pixel data is restored back to original if the image is found to be authentic.

This kind of distortion free (erasable) embedding procedure would ensure image retrieval without any modification to pixel data after the authentication process that caters to the unique need of medical images for diagnosis.

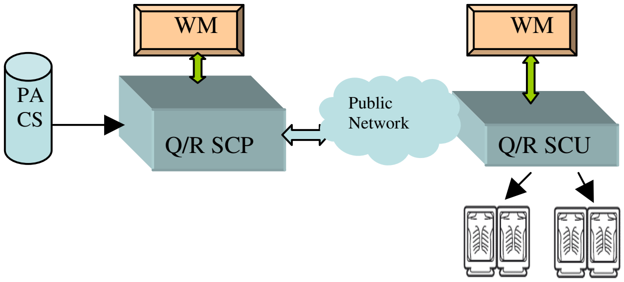
1. Introduction

The rules regarding patient data confidentiality are governed by ethics and legislative rules. As per existing regulations all patient records need to be secured and information confidentiality needs to be maintained. For medical images, no modifications are allowed during data transfer over networks for obvious legal reasons [1] and a potential risk of a physician misinterpreting an image

With increase in teleradiology and trend of PACS solutions moving towards a web based interface has catapulted the data security issues to the fore front. Confidentiality of the image data can be achieved by using mechanisms like access control, encryption, firewall etc on the PACS server. Integrity of the image data information can be maintained by encryption of information while transferring over the network.

However additionally, authentication technique needs to be implemented to ascertain whether confidentiality and integrity of data has been maintained.

The medical Image authentication scenario will be as shown below. The Q/R (Query Retrieve) SCP (Service Class Provider) and SCU (Service Class User) will use watermarking encoder and decoder before sending and receiving image data respectively.



Embedding the data in an Invertible manner without expanding the original image or append the data fulfills the Medical Image transfer issues adequately. Encryption mechanisms require additional data to be transmitted and also hinder file format changes.

In contrast, information that is embedded in the image is not modified due to compatible file format conversion, no bandwidth increase to communicate the additional information and a effective security of data is obtained because the embedded information is inconspicuous and imperceptible. A secret key can be used to embed and extract the data which will provide another layer of security.

2. Methods

2.1. Medical image authentication requirements

Following are the needs for applying authentication techniques to medical images.

0276−6547/05 $20.00 © 2005 IEEE

1. The Water Marking (WM) technique should be Invertible. That means once the image has been verified, the water marked image should be reverted to the original image by removing the water mark.
2. Even a single bit modification to the watermarked image must lead to unsuccessful verification.
3. Amount of data that needs to be transferred should not change (increase) due to usage of WM technique.
4. Watermarking mechanism and authentication/reconstruction of image should be efficient that uses minimum computer resources.
5. WM technique should support all data formats (8-bit, RGB, 16-bit). Because the DICOM [2] data can be in 8-bit,12-bit,16-bit or in RGB format.
6. There should be minimal perceptible changes in the watermarked image. The watermarked image should visually be the same as the original image. Although this is not a stringent requirement as the user views the restored image.
7. Compression of image data should not be hampered due to introduction of watermarks
8. WM implementation should be available as a separate module pluggable with any DICOM service implementation.
9. There should be no impact on the stored images in the PACS server due to introduction of watermark.
10. WM technique for authentication should be applied while transferring image data (in DICOM format) over the network.

2.2. New invertible fragile watermarking system for medical image authentication

The proposed watermarking technique derives from Invertible Authentication [3] and LAW [4] (Localized Loss-less Authentication Watermark) methods such that it satisfies the above requirements in an efficient way.

The technique supports multiple KBP (Key Bit Planes) for water marking. A Header need to be prepared which will contain the information like key bit plane numbers and number of hash bits in each of the bit planes. The header is of 10 bytes size and will be embedded in the last 80 bits of the LSB [5] plane of the image. The header information will be used to decode the embedded information in the image data.

2.2.1. Structure of the header

The header contains all the information required for decoding the image. The structure shown below is for 8-bit images and it can be easily extended to 16 or 24 bit images.

Element	Length in Bits	Frequency	Length of Field (in Bits)
Hash size	8	6 (from 2nd to 7th bit planes)	48
Compressed-Size (for last KBP)	32	1	32
Total			80

The "Compressed-Size" field is necessary to find out the compressed data size in the last KBP. E.g. if the accumulated sum of all the redundancies till 7th bit planes is less than or equal to the hash size then the 8th bit plane's compression size will be put in to the last field. If the redundant size of any bit plane is greater than 20 bytes (Secured Hashing Algorithm, SHA1) 20 will be put in the "Hash Size" field and that KBP's size after compression will be put in the "Compressed Size" field. Value '0' in "Hash Size" field indicates the corresponding bit plane is not a key-bit plane.

2.2.2. Encoding algorithm

1. For the original Image I (mxn) identify the key bitplane(s). Bit plane compression starts from the 2nd (next to LSB) bit plane to the most significant bit plane and stops if the accumulated sum of redundancies of bit planes is greater than or equal to hash size (20 bytes for SHA1). Least Significant Bit plane will not be considered as a Key bit plane as the last 80 bits of the least significant bit plane will be replaced by header. The data corresponding to the last Bit Plane will be compressed along with the first key bit plane to avoid loss of data due to header information being put in the last bit plane.
2. Bits available after compression for a Key Bit Plane will be padded with zeros. E.g if 512 bits have been compressed to 312 bits, the remaining 200 bits will be set to 0.
3. Prepare and embed the header in the last 80 bits of the LSB. This image will be called as Compressed Image C (mxn).
4. Append the user supplied password to the compressed image and take hash (H) over the compressed image data.

5. Embed the hash in the Key Bit Planes redundant space staring from the first identified key bit plane. (Hash will be embedded in parts if necessary, for example if 1st key bit plane is providing 64 bits and 2nd key bit plane is providing 64 bits redundancy then the hash will be divided accordingly and embedded in to the corresponding bit planes). This is the Watermarked image which can be transferred over the network to the receiver.

2.2.3. Decoding algorithm

1. Extract the Header from the LSB. Analyze the header and extract all the hash bits and make the corresponding bits to 0's in the image. This is the compressed image C (mxn) that was generated in the encoding algorithm.
2. Append the user supplied password to C (mxn) and compute the hash of the data. Compare the extracted hash with the computed hash. Image is inferred to be authentic if the two match.
3. If the image is found to be authentic then decompress the key bit plane and put back the bit planes to restore the original un watermarked image. The first decompressed key bit plane will have 80 bits of LSB.

The proposed technique authenticates the watermarked image before the restoration step thus eliminating the restoration step for tampered images.

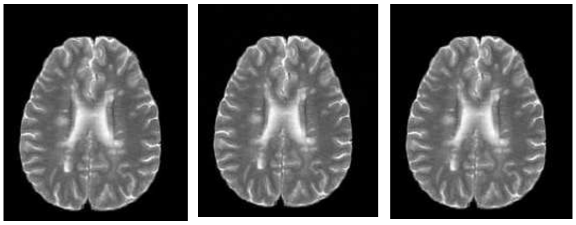
2.3. Advantages

1. Restoration step will be done only for those images that are successfully authenticated at the decoder.
2. Any of the lossless compression algorithms can be used.
3. Concept of multiple key-bitplane is introduced where in the hash can be embedded in multiple bit planes in parts. So the algorithm will not fail even if none of the bit planes provides space for embedding the complete Hash data. The hash in such cases would be distributed across multiple bit planes.
4. Taking hash of the image along with a shared Key will ensure detection of any changes made to the image even if the attacker knows the algorithm.

3. Results

The implementation of the proposed algorithm uses SHA1 [6] hashing algorithm, Huffman encoding and JBIG [7] (Joint Bi-level Image Experts Group) encoding. If the key bit plane happens to be in the lower bit plane then the changes in the watermarked image will not be perceptible to the normal eye.

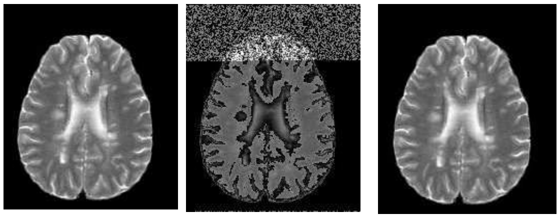
Figure (1) shows one of the slices of a MS (Multiple Sclerosis) lesion data set of height and width 256 x 256. The example uses 2^{nd} bit plane as the KBP.



(a)Original Image (b) Watermarked Image (c)Restored Image

Figure (1) Authentication of MS lesion Slice

The figure [2] shows watermarking being embedded in the most significant bit plane. The decoding algorithm will be a part of storage SCU and the user will view the restored image [c] as shown below.



(a)Original Image (b) Watermarked Image (c)Restored Image

Figure (2) Authentication of MS lesion Slice

4. Discussion and conclusions

The existing watermarking techniques can be used for authenticating images in applications like satellite image transfers, topography image transfers etc effectively. But medical image authentication demands some unique requirements mentioned in section 2.1. The proposed algorithm improves upon the existing watermarking techniques which suits the requirements of transferring medical image data on public networks. The proposed algorithm provides a foolproof method of transferring medical images that are being used by radiologists for diagnosing ailments.

Acknowledgements

We thank Wipro Technologies for providing us an opportunity and the required resources to work on this paper.

References

[1] Health Insurance Reform; Security Standards; Final Rule. 45 CFR Parts 160, 162, and 164.Federal Register.Vol. 68, No. 34, Thursday February 20, 2003.

[2] Digital Imaging and Communications in Medicine Ver 3.0, Part 5 - Data Structures and Encoding,2004, pp 46-46

[3] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Proc. of SPIE Sec. and Watermarking of Multimedia Cont. III , Jan 2001, pp. 197–208.

[4] M. Celik, G. Sharma, A.M. Tekalp, and E. Saber, "Localized Lossless Authentication Watermark (LAW)", Proc.of EI SPIE, Security and Watermarking of Multimedia Contents V, vol. 5020, Santa Clara, , 2003., pp. 689–698.

[5] R.C Gonzalez and R.E Woods "Digital Image Processing" , Addition Wesley Publishing company, inc., 1993

[6] Federal Information Processing Standards (FIPS) Publication 180-1, Secure Hash Standard (SHS), U.S. DoC/NIST, April 17, 1995.

[7] K. Sayood,, "Introduction to Data Compression", Morgan Kaufmann Series in Multimedia and Information Systems, 2000.

Address for correspondence

Kalyan Sreenivas Pushpala
Sr Project Engineer - Medical Devices,
Embedded & Product Engineering Solutions
Wipro Technologies,
No 92, 2nd Main Road,
Keonics Electronics City
Bangalore - 560100
e-mail - Kalyan.pushpala@wipro.com
Kallu_sreein@yahoo.com

Rakesh Nigudkar
Project Manager – Medical Devices,
Embedded & Product Engineering Solutions
Wipro Technologies.
No 92, 2nd Main Road,
Keonics Electronics City
Bangalore - 560100
e-mail - Rakesh.nigudkar@wipro.com