Int. J. Communications, Network and System Sciences, **2010, 3, 801-804**
doi:10.4236/ijcns.2010.310107 Published Online October 2010 (http://www.SciRP.org/journal/ijcns)

A Secure Transfer of Identification Information in Medical Images by Steganocryptography

Shuhong Jiao[1], Robert Goutte[2]
[1]*Information and Telecom Department, Harbin Engineering University, Harbin, China*
[2]*Lab. CREATIS, UMR CNRS* 5520, *INSERM U* 630, *INSA, Université of Lyon, Bâtiment Leonard de Vinci*, 21 *avenue Jean Capelle* 69621 *VILLEURBANNE Cedex, France*
E-mail: *jiaoshuhong@hotmail.com, goutte@creatis.insa-lyon.fr*
Received July 26, 2010; *revised August* 23, 2010; *accepted September* 25, 2010

Abstract

The fast growth of the exchange traffic in medical imagery on the Internet justifies the creation of adapted tools guaranteeing the quality and the confidentiality of the information while respecting the legal and ethical constraints, specific to this field. The joint usage of steganography and cryptography brings an efficient solution, whose implementation in medical routine is realistic, thanks to the current progress in data processing (broad band Internet access and grid computing).

Keywords: Medical Image, Identification, Steganography, Cryptography

1. Introduction

The current needs in medical imaging security comes mainly from the development of the traffic on Internet (tele-expertise, telemedicine) and to establishment of medical personal file [1]. Among all possibilities it is interesting to work on the messages concealment in the image itself, then regarded as a medium coverage.

2. Objective

Insert in a medical image 2D black and white of any modality, a hidden message with all information identification (the radiologist and patient), historical of record, parameters of examination (nature, location, diagnosis and comments of the radiologist). Ideal characteristics sought:

1) Access, in reception, at the original image, without alteration or loss of information

2) The method used for the encryption must resist to attacks.

3) The hidden message must be, in reception, readable by the holder of the key.

This group of ideal conditions, with contradictory's imperatives, will be practically never satisfied. However; the proposed methods must be realized with objectives neighboring of these limits.

3. Features Specific Constraints in Medical Imagery

1) Need to use standards [2]
2) Respect of legislation
3) Rapidity and simplicity of implantation
4) Compatibility with JPEG compression

It is important to note that, in medical imagery domain, the compression, to be truly operational, shall keep useful information for the diagnosis and should relate essentially optimization of acquisition parameters, noise reduction and elimination of temporal redundancies.

4. Steganography

The steganography (Greek steganos: Covered and Graphein: Write) is the art hide a message in a medium coverage (medical image for example), so no one can distinguish the medium (original image), after the inclusion in the hidden message [3].

The hidden message can be a plain text or his encrypted version. In this latter case (which is interesting here), we use the term steganocryptography. For this, we use a prior encryption of the hidden message, before the introduction in the original image, considered here as a medium coverage. We propose to use a symmetric en-

cryption algorithm, known as international standard. En agreement with the work of W. Puech and M. Rodrigues [4], we choose the algorithm AES. This symmetric cipher uses blocs of data swapped of 128 bits and key sizes of 128, 192 or 256 bits.

4.1. Example of AES Encryption and Decryption [2]

Password: Creatisuniversitedelyon

Plaintext: Secure transfer in medical imagery

Encrypt it:

z4USOP2/O1sZdydqd4hSddOQUfRQabfKUCAoJP2drF6entGV

Decrypt it: Secure transfer in medical imagery

4.2. Conversion of this Encrypted Message in New Digital Message, ASCII 8 Bits by Character [5]

z4U50P2/O1sZdydqd4hSdd0QU……

01110100011010001010101001101010100111101010000001100100010111101001111 00…..

5. Insertion by Steganography of Digital Data in Original Digital Image

These methods require five successive steps:

The first step is to divide the image into 8 × 8 square blocks (one byte for one grey level). In the second step we compute the different DCT coefficients (Discrete Cosine Transform [6] of these different blocks.

We select, in the third step, two spectral coefficients: (a_{mn}) and (a_{kl}) in the block i. Their location, in this block requires 2 × (2 × 3) bits. These 12 bits, expressed with two ASCII characters (6 bits per character) are the beginning of the shared hidden key.

In the 4th step we use the following rule: If $b_i = 1$ and $(a_{kl}) > (a_{mn})$ or if $b_i = 0$ and $(a_{kl}) < (a_{mn})$ nothing is changed .If these conditions are not carried out we exchange the values of (a_{kl}) and (a_{mn}).

The amplitudes of the change of the spectral coefficients can be adjusted depending on the level of noise and the rounding's error. The frequency's position of the two coefficients is important. If it is located in BF, the method is robust, but risk of be visually detectable.

Instead, if it is located in HF, the original image will be virtually unchanged, but the method will be more sensitive to photometric fluctuations.

5.1. Variant

If necessary, for obtain another form of resistance to attacks, we can take different coordinates for the coefficients (a_{mn}) and (a_{kl}). In this case, it is possible, for example, with one bit, of displace the sequence for the block i, for obtain the sequence of the block $i + 1$.

If coordinates $(a_{kl})i$ = 010 and 011 ,and if coordinates $(b_{mn})i$ = 001 and 100 we obtain the key chain for the block i: 010011001100 and 001001100110 for the block $i + 1$.

The detection of these coordinates is more difficult, but it is not possible to choice a single optimal domain for these coefficients, in the spectral plan.

We have the ability to hide 1 bit per square block or, for an original image of size 1024 × 1024, to hide 16384 bits .With ASCII code ,extension UNICODE (with 8bits per characters),we obtain the possibility to hide 2048 characters in this image.

The 5th step is the extraction of the hidden message. The method is similar to that the insertion: at the reception we compare the values of the two selected coefficients The previous rule allows us to know if the bit concerned is 1 or 0.

Remark: *The marking brought a very slight loss of information, since the image in the reception is not exactly identical to original, but the quantity of bits transferred is the same.*

It is important to note this favorable factor: *Any location in the spectral domain involve an displaying in the image plane, which facilitate the invisibility of the insertion*

6. Radiographic Application

The original image **(Figure 1**) is a pulmonary radiography, obtained in tomodensitometry (X ray scanner).

We isolate on this image one block 8 × 8.

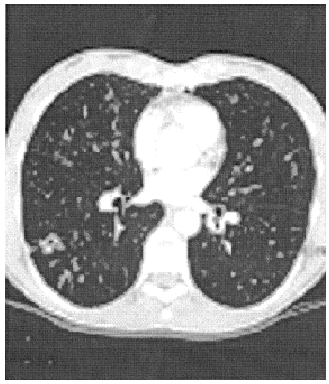

Figure 1. Pulmonary scannography

142	120	100	87	82	78	79	81
131	113	98	87	79	83	82	82
119	107	97	90	84	83	82	80
119	112	106	100	95	85	83	80
134	127	118	107	100	91	87	82
150	140	126	111	100	96	91	85
156	144	129	114	103	96	92	86
145	132	119	108	100	91	88	83

(Original block image, before transform)

After Discrete Cosine Transform DCT, we obtain this block, in the spectral domain.

3.2240	0.5578	0.1552	0.0572	0.0132	0.0177	0.0020	0.0074
0.2305	−0.0818	0.0513	0.0124	0.0143	0.0023	0.0074	−0.0042
0.0148	0.0510	0.0676	0.0211	0.0094	0.0037	0.0036	−0.0020
0.0986	0.0704	0.0268	0.0042	−0.0060	0.0037	0.0014	0.0002
−0.0270	−0.0070	0.0226	−0.0046	0.0152	−0.0070	−0.0071	0.0109
0.0156	0.0113	−0.0051	−0.0028	0.0062	−0.0026	−0.0046	0.0044
−0.0194	−0.0052	0.0026	−0.0027	0.0009	−0.0005	−0.0010	−0.0001
0.0048	0.0046	0.0007	0.0010	0.0002	−0.0011	−0.0013	0.0017

With $k = 3$, $l = 2$ and $m = 3$, $n = 3$, $a_{kl} = 0.0510$, and $a_{mn} = 0.0676$

Here: $a_{kl} = 0.0510 < a_{mn} = 0.0676$

If I want to introduce a hidden bit $b = 0$, nothing is changed.

If I want to introduce a hidden bit $b = 1$, we invert the values of a_{kl} and a_{mn}

$a_{kl} = 0.0676 > a_{mn} = 0.0510$

In this case ($b = 1$) we obtain after inverse transformation DCT^{-1}

142	120	101	88	83	78	78	79
131	113	98	87	79	83.	82	81
119	107	97	90	84	83	82	81
119	112	105	99	94	85	84	82
134	127	117	106	99	91	88	84
150	140	126	111	100	96	91	86
156	144	129	114	103	96	92	85
145	132	120	109	101	91	87	81

(bloc image after crypt)

On each pixel modified, the positive or negative error is approximately one grey level. Only 24 pixels dispersed on 64 are modified and the mean of grey levels is unchanged. The image is good and the message is not visible. Practically, in a medical image with 256 gray levels, a deviation of one pixel has no physical significance and presents no interest for visual observation or subsequent numerical processing. It results mainly from the presence of noise and artifacts of rounding obtained when quantifying.

To avoid the consequences of too large distance between these 2 factors (a_{kl} and a_{mn}) which may introduce a important disturbance of the spectrum) and also the opposed consequence of a gap too low (rendering the method unstable in presence of noise) we use, if necessary the following rule:

If the gap $a_{mn} - a_{kl}$ is $2e$, and if $0.0010 < e < 0.0120$, nothing is modify;

If $e < 0.0010$ we take $a_{kl}' = 0.5(a_{kl} + a_{mn}) - 0.0010$

and $a_{mn}' = 0.5(a_{kl} + a_{mn}) + 0.0010$

If $e > 0.0020$ we take $a_{kl}' = 0.5(a_{kl} + a_{mn}) - 0.0120$

and $a_{mn}' = 0.5(a_{kl} + a_{mn}) + 0.0120$

0.0010 and 0.0120 are too adjustable parameters, in function of the level of noise in the image and the confidential degree wished.

6.1. Example of Hidden Message

Place of examination: *Cardiologic Hospital, HEH Lyon, Service of Radiology*.
Date: 25/15/2009
Instrumentation: *Tomodensitometer, Pulmonary Scanner*
Radiologist: *Dr. Jean Martin*
Identification: *XXXXXXX*
Patient: *Michel Dupont*
Identification: *YYYYYYY* *Age*:*45 years*
Conditions of observation: *Axial Incidence transverse*

Commentaries: *This patient presents a small parenchymatous nodule of the higher segment of the lobe lower right. Presence also of a discrete bronchial dilation in the average lobe*.

This hidden message (in italic) possesses 347 characters, with spaces. In ASCII we obtain 1.421.312 bits, it is necessary to have a dimension for the original image equal or upper of 1.5 megabits. This dimension is usual in medical imagery.

Thus, in our example, the proposed coding is invisible and involves no loss of useful information.

This approach has been submitted to a panel of radiologists from hospital, specialists from different imaging modalities and their comments and proposed additions have been included in this final implementation.

7. Generalization

The method proposed is well suited to the JPEG compressed images [7] because, in this case, the compression algorithm use also the Discrete Cosine Transform (DCT). It is possible to extend this method to color images, which can be considered as a set of three images black and white (RGB). In three dimensional imaging, we can consider 8 × 8 × 8 cube and use the 3D block DCT algorithm.

8. Conclusion

The steganocryptography can transmit, with invisibility and robustness, the information accompanying a medical digital radiography. The constraints of legal requirements, safety and confidentiality are fully satisfied.

9. References

[1] Liliane DUSSERRE, Rapport du Conseil National de l'Ordre des médecins, France, 2002.

[2] Federal Information Processing Standards, Public. 197, announcing the Advanced Encryption Standards (AES), USA, 2001.

[3] Christian REY, Jean Luc DUGELAY, Panorama des méthodes de tatouage, Traitement du Signal, Vol. 18, spécial No., 2001.

[4] W. Puech and J. M. Rodrigues, "Crypto-Compression of Medical Images by Selective Encryption of DCT," 13*th European Signal Processing Conference*, EUSIPCO'05 Antalya, Turkey, 2005.

[5] Wikipedia, Encyclopédie libre, Norme ASCII.

[6] Y. Wang and P. Moulin, "Steganalysis of Block-DCT, Image Steganography," *Proceedings of IEEE Workshop on statistical Signal Processing*, St Louis, 2003, pp. 339-342.

[7] H.-W. Tseng and C.-C. Chang, "Steganography Using JPEG Compressed Image," *Fourth International Conference on Computer and Information Technology* (*CIT* 04), 2004, pp. 12-17.

