Assessment of Steganographic Methods in Medical Imaging

Rafael A. Sampaio, Marcel P. Jackowski
Department of Computer Science
Institute of Mathematics and Statistics
University of São Paulo, Brazil
{rsampaio, mjack}@ime.usp.br

Abstract—DICOM standard is well-established regarding storage, printing, and transmission of medical images. However, there are no security methods that preserve metadata confidentiality, nor image authenticity. This work assesses three steganographic methods – least significant bit insertion (LSB), division into blocks, mean change modified method (MCMM) – and verify their feasibility for clinical use in medical imaging. Integrating MCMM in DICOM standard would provide a breakthrough for information security in medical imaging, deterring fraud, privacy invasion, while preserving diagnostic information.

Keywords—Steganography; DICOM security; medical imaging.

I. INTRODUCTION

Digital Imaging and Communications In Medicine (DICOM) is a well-established standard of storing, printing and transmitting medical image information. However there are no security methods for DICOM, since it stores the data in tags unqualifiedly editable. Images originated from medical examinations may be shared inadvertently exposing such information, without being able to verify authenticity and misuse.

Steganography is comprised by a set of techniques that allows one to write messages and hide them, for example, in images, in such a way that no one suspects of their existence. This paper presents an assessment of steganographic methods applicable to the DICOM standard.

Contributions: This work assesses three previously published steganographic methods and verify their feasibility for clinical use in medical imaging. The purpose is to add security and confidentiality to the information contained in DICOM, while not compromising their diagnostic information.

A. Related work

While work has been done on assessing authenticity of medical images [1], [2], [3], [4] no previous investigation on embedding DICOM tag information into their respective images has been reported in the literature. In this work, we explore three steganographic methods for embedding textual information in medical images: the least significant bit insertion [5]; division into blocks and mean modification [6]; and the mean change modified method [6].

II. MEDICAL IMAGES AND DICOM

Modern medicine has advanced greatly in recent years and this progress has been shared with other sciences.

Fig. 1. Magnetic resonance image slice of a human brain in which hyperintense regions indicate tissue abnormality.

Due to the increasing use of computers in clinical applications, American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA) recognized the need to establish a standard for transferring of images and related information among multiple devices. Thus, in 1983, ACR and NEMA decided to develop a standard to enable the transmission of medical images, facilitate the development of systems for storing images, and integrate these with other hospital information. Thus it would be possible to create a database beyond geographical boundaries.

In 1985, ACR-NEMA published version 1.0 of this standard, which is known today as DICOM – Digital Imaging and Communications in Medicine. Today, DICOM is a well-established standard of storing, printing and transmitting information in medical imaging [7].

DICOM image files have two components: a header, that contains confidential patient information, the location where the examination was performed, the equipment, among others; and a grayscale matrix, representing image intensities. The
header consists of a set of tags, which currently consists of more than 3300 fields. A comprehensive list can be found in [8], [9]. See examples in tables I and II.

Considering the relevance of the DICOM standard for the dissemination of medical images, it is important to emphasize that DICOM does not provide transmission security or data protection [10]. In other words, it is possible to obtain an image illegally and tamper with it, without being able to detect misuse, verify image authenticity, or validate the information represented by the tags. Pianykh illustrates how fragile security is by simply using a text editor to altering tags. Ultimately, though, encryption techniques can be used to improve security.

III. STEGANOGRAPHY

Steganography is a science which deals with invisible communications, i.e., the embedding of secret messages that should not be detected during communication. Because steganography can be used as a tool to maintain privacy in communications, it is natural that human beings attack it. For this reason, several methods were developed to detect the presence of secret messages and eventually decode them.

The main property of a steganographic system is to be statistically undetectable, i.e., it should be impossible for an eavesdropper to say that Alice and Bob are communicating.

Note that an eavesdropper needs only to detect the presence of a secret message for the steganographic system be considered broken. The security of a steganographic method is based on the assumption that an eavesdropper is not able to prove that a given communication contains a secret message.

Three standard steganographic methods are next described and later assessed for usability in medical imaging.

A. The least significant bit insertion

This method assumes that information in a 24-bit digital image is represented by an array of triplets, and these triplets correspond to intensities of red, green and blue (RGB model). Each pixel of the image can be described by a triple of values associated to each color. In the case of 8-bit images, the image is represented by an array of grayscale values.

The least significant bit insertion method is the most obvious and also the most well-known for hiding information in images. The change of the least significant bit should cause an image alteration that is barely noticeable.

Consider the binary representation of information $S$ to be hidden. The least significant bit of each pixel in the image is overwritten by $S_i \in \chi = \{0, ..., 2^{n_c} - 1\}$, for $1 \leq i \leq |S|$ and $n_c$ is the number of bits in graphical palette. So

$$S_i = \sum_{k=1}^{n_c} b[i,k] \cdot 2^{n_c-k},$$

where $(b[i,1], ..., b[i,n_c])$ is the binary representation of $S_i$, and $b[i,n_c]$ is least significant bit.

For 24-bit images, the changes are minimal and virtually imperceptible to the human eye when $|S|$ is reasonable. The 8-bit images, however, undergo significant changes and are easily detected by histogram attack, where pixel intensity frequencies have changed their distribution [5].

This method is quite vulnerable to geometric transformations and filtering as well as compression schemes (such as JPEG) because it involves changes in the least significant bits and the steganographic information is destroyed.

Another weakness is the easy retrieval of information that is intended to be hidden. Fridrich proposed a permutation of bits from a sequence of pseudo-random numbers generated by a key shared between Alice and Bob [5]. Still, an attack via histogram analysis could prove successful.

B. Division into blocks and mean modification

Another approach is to divide the image into blocks of a sufficiently large size. In other words, such a block must be able to store information $S$ and not induce apparent difference before and after the steganography.

Let $B$ a block of size $m \times n$, the mean value of this block will be changed to represent the k-th bit of $S$. For this, Mortazavian et al. describe this process of decision making [6]: calculate the mean value $M_i$ of block $B$; calculate $M_{S_i}(j)$, which corresponds to the j-th mean center of the spectrum with the symbol $S_i$; calculate the new mean

$$M_d(i) = \arg \min_{j=1,2,3...} |M_{S_i}(j) - M_i|.$$

Let $\Delta M(i) = M_d(i) - M(i)$ corresponds to the change to be produced in each pixel of $B$, aiming the lowest possible degradation in the image and also pointing to the bit that stores information $S_i$. The table III found in Mortazavian et al. [6] illustrates some values.
Using steganography and its subsequent extraction algorithm.

But it will increase intensities of each pixel so that total change required is reached.

Finally, the elements

\[ B_{ij} \leftarrow B_{ij} + [\Delta M(i)] \]

are modified, and \([\,]\) represents rounding to the nearest integer \(\Delta M(i)\). Although this method offers better results than the least significant bit insertion, a few issues are highlighted by Mortazavian et al. in [6]:

1) The block effect is apparent in uniform regions of the image, although the size has been properly chosen;
2) The value of \(\Delta M(i)\) is rounded to the next integer, which can modify the expected mean;
3) It requires the preprocessing of the image to define the range of gray tones, which can cause changes in image brightness or eliminate small details;
4) The modification is not optimal: all pixels are changed, making the changes noticeable. Changing fewer pixels may provide better results.

C. Mean change modified method

Seeking an improvement to the algorithm proposed in the previous subsection, Mortazavian et al. devised a technique that shuffles the image pixels prior to steganography. This minimizes the block effect, and adds security. The generator of pseudo-random numbers shuffles the pixels according to a certain seed. This seed can be seen as a key shared between Alice and Bob.

In addition, the algorithm must reduce (or increase) the grayscale intensities of pixels being modified until expected mean is reached. However, this algorithm must avoid substantial changes to a particular region. For that, a switch mode that will be constrained by a certain threshold is used, so the algorithm will not reduce the grayscale palette by a large amount to achieve expected mean if that degrades the image, but it will increase intensities of each pixel so that total change required is reached.

**Pseudocode:** Mortazavian et al. defines in [6]:

- \(N1\): number of pixels whose values are above \(\Delta M(i)\), i.e., those to be modified;
- \(\Delta G_T\): amount of alteration required to mean of block be closer to \(M_d(i)\), given by \(\Delta G_T = |\Delta M(i)| \cdot N\), where \(N\) is total number of pixels;
- \(M_{d2}(i), \Delta M_2(i), N2\) and \(\Delta G_{T2}\) are defined equivalently by \(M_d(i), \Delta M(i), N1\) and \(\Delta G_T\) in switch mode.

We describe below the algorithm for encoding content using steganography and its subsequent extraction algorithm.

**Encoding algorithm:**

1) Encode the message into binary representation;
2) Draw pseudo-random numbers using the key as seed and re-ordain the image pixels (shuffled image);
3) Take \(i = 1\);
4) Select \(N\) pixels, from \((i-1) \times N + 1\) to \(i \times N\), which will be stored in \(CB(i)\);
5) Calculate \(M(i)\);
6) Calculate \(M_d(i)\) – decision-making step;
7) Calculate \(N1\);
8) Calculate \(\Delta G_T\);
9) If \(\Delta M(i) < 0\), then:
   a) \(s = 1\) – defines the operation to occur in switch mode;
10) Else: \(s = -1\);
11) If \(\Delta G_T > 2K \cdot N1\), then:
   a) Calculate \(M_{d2}(i) = M_d(i) + 2K\), where \(K\) is spectrum width, the acceptable threshold;
   b) Calculate \(N2\);
   c) Calculate \(\Delta G_{T2} = N2 \cdot \Delta M_2(i)\), with \(\Delta M_2(i) = 2K - |\Delta M(i)|\);
   d) Add \(1 \times s\) units, \(\Delta G_{T2}\) times, to the pixels of \(CB(i)\), whose values are less than 255;
12) Else: Add \(-1 \times s\) units, \(\Delta G_T\) times, to the pixels of \(CB(i)\), whose values are greater than 0;
13) Write \(CB(i)\) in shuffled image;
14) While there are bits to be encoded, increase \(i\) and repeat from step 4;
15) Unshuffle image with steganographic blocks to build the required image.

The extraction algorithm is essentially the application of the above algorithm in the opposite direction. By using the shared key, it will be possible to generate a sequence of pseudo-random numbers again. Consequently, the decision will be repeated, delivering the correct extraction of each encoded bit.

**Extraction algorithm:**

1) Generate decision-making table;
2) Generate shuffling indexes from pseudo-random numbers sequence using the shared key;
3) Shuffle steganographic image;
4) Take \(i = 1\);
5) Select \(N\) pixels, from \((i-1) \times N + 1\) to \(i \times N\), which will be stored in \(SB(i)\);
6) Define \(M_{SB}\), the mean value of \(SB(i)\);
7) Define \(b(i)\) related to mean spectrum interval where \(M_{SB}\) is, using decision-making table;
8) If there is content to be decoded, increase \(i\) and repeat from step 5;
9) Reveal the content behind steganography.

The Mean Change Modified Method fights each one of the weaknesses of previous algorithms: perceptibility of steganography caused by block effect, unwanted change of stored information by means of decision-making table and degradation of image.
We have implemented the MCMM algorithm described in the last section – the source code is available upon contacting the authors.

IV. RESULTS

Two approaches were adopted to assess the results of steganographic methods: a qualitative, that evaluates how significantly image alterations can be visually detected - and quantitative, that measures the degree of similarity between the image before and after steganography to hide all nonempty DICOM tags of a magnetic resonance image brain slice.

Qualitative analysis: In this analysis the difference images were computed by the software ImageMagick v6 [12]. Using the method of Least Significant Bit Insertion, the results are unsatisfactory for medical imaging applications. The area of abnormality is increased, as shown in Figure 2.

Fig. 2. (a) Original image. (b) Image after LSB. (c) Difference image.

Division into blocks and mean modification method causes unwanted effects in the image so security can be challenged. Note the block effect in comparison, as shown in Figure 3.

Fig. 3. (a) Original image. (b) Image after Division into Blocks method. (c) Difference image.

Mean change modified method yields the best visual results with respect to image degradation (See Figure 4).

Quantitative analysis: Three criteria were considered for comparing images before and after steganography [13]. Let matrix A correspond to the original image and matrix B represent the image after steganography.

1) Sum of Squares of Differences (SSD):

\[ SSD = \frac{1}{N} \sum_{i,j} |A_{ij} - B_{ij}|^2 \]

2) Sum of Absolute Differences (SAD):

\[ SAD = \frac{1}{N} \sum_{i,j} |A_{ij} - B_{ij}| \]

3) Maximum Absolute Difference (MAD):

\[ MAD = \frac{1}{N} \max_{i,j} |A_{ij} - B_{ij}| \]

Comparison was made between each of steganographic methods using the previous metrics with the same set of medical images2 (see table IV).

As can be seen in the qualitative analysis, MCMM depicts the largest similarity between images before and after steganography, considering all the SSD, SAD, and MAD metrics.

V. CONCLUSION

DICOM standard is well-established regarding storage, printing, and transmission of medical images. However, there are no security methods that preserve metadata confidentiality, nor image authenticity.

This work shows that Mean Change Modified Method provides an efficient technique to hide information within image pixels. MCMM causes no apparent degradation, preserving their clinical information. Thus, from a key shared between the sender and receiver, it is possible that one encodes confidential DICOM tags within the image pixels, and extracts them later. Any intentional change or accidental in tags will not interfere with hidden information, which guarantees authenticity. In addition, MCMM method preserves embedded diagnostic information better than LSB and Division into Blocks methods, given the comparison table IV. However, a more detailed analysis must still be performed.

<table>
<thead>
<tr>
<th>Comparison of Steganographic Methods</th>
<th>LSB Insertion</th>
<th>Division into blocks</th>
<th>MCMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSD</td>
<td>1449</td>
<td>109</td>
<td>14</td>
</tr>
<tr>
<td>SAD</td>
<td>18</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>MAD</td>
<td>$2.14 \cdot 10^{-3}$</td>
<td>$9.16 \cdot 10^{-4}$</td>
<td>$5.29 \cdot 10^{-4}$</td>
</tr>
</tbody>
</table>

2Namely BU001015-V01 (13.95 MB), MR (32.63 MB), CT (255.02 kB), chest (3.72 MB), mammo (3.29 MB), skull (12.06 MB), available for free on MicroDicom [14]
Integrating MCMM in the DICOM standard would provide a breakthrough for information security in medical imaging, deterring fraud, privacy invasion, while preserving diagnostic information.

REFERENCES


