Protection of Digital Mammograms on PACSs Using Data Hiding Techniques

Chang-Tsun Li, Yue Li and *Chia-Hung Wei*

Department of Computer Science, University of Warwick, UK
{ctli, yxl and rogerwei}@dcs.warwick.ac.uk

Abstract

Picture archiving and communication systems (PACS) are typical information systems, which may be undermined by unauthorized users who have illegal access to the systems. This paper proposes a role-based access control framework comprising two main components – a *content-based steganographic module* and a *reversible watermarking module*, to protect mammograms on PACSs. Within this framework, the content-based steganographic module is to hide patients' textual information into mammograms without changing the important details of the pictorial contents and to verify the authenticity and integrity of the mammograms. The reversible watermarking module, capable of masking the contents of mammograms, is for preventing unauthorized users from viewing the contents of the mammograms. The scheme is compatible with mammogram transmission and storage on PACSs. Our experiments have demonstrated that the content-based steganographic method and reversible watermarking technique can effectively protect mammograms at PACS.

Index Terms—Information Security, Steganography, Digital Watermarking, PACS, Biomedical Informatics, Data Hiding

1. INTRODUCTION

A picture archiving and communication system (PACS) integrates imaging modalities and acts as the interface between hospitals and departmental information systems in order to manage the storage and distribution of images to radiologists, physicians, specialists, clinics, and imaging centers. As medical image databases are interconnected through PACSs, those medical images are subject to security breaches, such as loss or manipulation of sensitive information, if their contents are not protected in some ways. For example, if a medical image is illegally obtained or if its content is malevolently changed, the patient's privacy, health care and legal rights could be undermined. Given the fact that medical image databases are accessed by users of various roles, e.g., doctor, administrator, interns, etc., a role-based access control mechanism is an obvious approach to the prevention of the afore-mentioned security breaches. For instance, a doctor could be given full access to the images and patients' textual information, while an intern's or administrator's access should be restricted according to the roles they are allowed to play. A common practice of managing textual information associated with images is to store the information in the header segment of the image file. Although the textual information can be protected through encryption, however the file formats are known publicly and the header field is separated from the content; that means the very location of the encrypted information is known. This opens a security gap for the attackers to manipulate the information. For example, even without knowing the secret key, an attacker can replace patient *A*'s encrypted information in the header with patient *B*'s encrypted information. This suggests that the location of the patients' information should not be made known to the unauthorized users and the information itself should be made inseparable from the pictorial contents of the images. Moreover, an overhead of the header is that it takes up physical disk spaces. We proposed in this work a role-based access control framework consisting of two key modules – a *content-based steganographic module* for hiding patients' textual information in the contents of medical

images in a non-deterministic manner so as to prevent leaks of sensitive information and to save disk space. We also propose a *reversible watermarking module* for 'masking' the contents of the images with hidden patients' textual information (called *stego-images*) in order to prevent unauthorized users from viewing the images. The main objectives set out in this work are:

1) To design a conceptual framework for protecting mammograms on PACSs. The framework should not only provide reliable protection for mammograms, but also support management functions for users with different access rights.
2) To develop a novel content-based steganographic method for hiding patients' textual information in mammograms and verifying the authenticity and integrity of mammograms. The data hiding process should not change the important pictorial details of mammograms and the data extraction process should not require the availability of original mammograms.
3) To develop a watermarking technique capable of masking the contents of mammograms for protecting mammograms against illegal access. The watermark can be removed to reveal the masked mammogram when authorization for viewing is given.

2. LITERATURE REVIEW

Main methods used in media industries for protecting digital information against malicious usage can be broadly classified into *cryptography-based* and *authorization-based* approaches. The approach of cryptography-based methods is to devise various protocols for the Internet and local area networks (LAN) to protect the digital information through encryption during the transmission in networks (Long, 2006; Xu, 2005). The idea of the authorization-based methods is to use digital signature certifications to achieve authorization for digital information storage and transmission. Since cryptography-based

methods mainly focus on image transmission while laying less emphasis on the storage and management phases, the latter is therefore considered as more desirable in achieving higher reliability and security.

An early example of authorization-based method is the framework proposed by Thomas and Sandhu (1994), which depicted a conceptual model for task-based authorization methods. The concept of task-based authorization is that whether the users can pass the authorization or not depends on the tasks the users are charged with. They discussed several authorization functions and the business activities and mapped the semantic interpretations for the practical activities to computer functions. In such a way, they attempted to bridge the gap between low-level computer techniques and the high-level requirements of image system protection. However, the main limitation of task-based authorization is the difficulty in managing the access rights on the same task performed by different users. Kern *et al*. (2004) improved Thomas and Sandhu's tasked-based authorization by proposing a model for role-based access control. Roles-based authorization is set up depending, not on the tasks the users are assigned to, but on the roles of the users in the system. However, the study by Kern *et al.* (2004) is only conceptual, with no realizable schemes proposed for practical implementation.

Focusing on picture archiving and communication systems (PACS), Zhou and Huang (2001) proposed an integrated PACS management system for mammograms on which the textual information, such as patients' medical history, is integrated with the corresponding medical images. First the textual information is hashed and embedded into the mammogram using LSB steganography, which is about hiding data in the least significant bits by many published methods (Cao et al, 2003; Fridrich & Goljan, 2004; Ker, 2007; Tian, 2003; Zhou & Huang, 2001), and then this stego-image is encrypted by a cryptosystem. An improved version of Zhou and Huang's scheme was later proposed by Cao *et al.* (2003). One drawback of both schemes (Cao, 2003; Zhou & Huang, 2001) is that they do not classify access rights by taking different roles of the users into consideration, therefore any one possessing the access key gains full access to the information, while the ones who do not have the key are completely

barred from the system, i.e., the access right is binary. Another limitation of these two schemes is that in order to extract and view the textual information, the image has to been decrypted. Once the image is decrypted, it remains unprotected and anyone can view and modify it. Planitze and Maeder (2005a, 2005b) studied the potential of digital watermarking for protecting patients' textual information and the medical images themselves on PACSs. However, they did not suggest any frameworks or practical schemes for real world applications. Osborne *et al*. (2004) proposed a multiple embedding approach using robust watermarking for medical image protection. The digital signature of an image is first embedded into the RoB (Region of Background) using Quantization Index Modulation method (QIM) (Chen & Wornell, 2001). Then a second round of watermarking is performed to serve the authentication need. Despite the novelty of the idea, this method has two major drawbacks. First, access control is not provided. Secondly, the simple QIM method they employed is an insecure embedding method.

3. THE PROPOSED CONCEPTUAL FRAMEWORK

In the context of mammogram database management, the privacy of a patient, such as the patient's identity and medical history, resides in the security of the sensitive textual information and the pictorial contents of mammograms. Recognizing the need for providing multi-level access control to the mammograms depending on the users' roles on PACSs and aiming at achieving the objectives set out earlier, we propose a conceptual role-based authorization scheme in this section. This generic framework, as shown in Figure 1, depicts the key components and allows the components to be realized using the state-of-the-art techniques as technology advances. For example, the segmentation component of the framework can be implemented with different methods provided they serve the purpose. A practical realization of the conceptual framework is proposed in next section.

Depending on the roles of the users defined by different institutions, the roles as well as the access rights can be divided into multiple levels. This work is based on the assumption that there are three types of roles / users as defined in Table 1. For instance, the doctor in charge of a case can access the patient's information, such as the patient's medical history and the mammograms; therefore, he/she should be classified as Level 2 user. An intern or trainee, on the other hand, can only access the mammograms for field work and training purposes but not the patient's medical history, so he/she is at Level 1. A system technician with only maintenance duties should not be allowed to access the patient's information and the contents of the mammograms so he/she is to be classified as Level 0 and no access key is to be issued.

The proposed framework is divided into *embedding* and *extraction* processes as shown in Figure 1. The purpose of the *embedding* process is three-fold. First, its *steganographic function* f_s embeds patients' textual information into the corresponding mammograms with stego-key K_s so that users below Level 2 gain no access to those sensitive textual information. Secondly, when hiding the patients' textual information, steganographic function f_s involves the pictorial information taken from the images' contents so that if an attacker manipulated the pictorial contents of the images, the extraction process will fail to extract the hidden textual information, thus allowing the user to know that the image is no longer trustworthy. We have demonstrated the effectiveness of involving contents of different parts in the data hiding process for facilitating authentication in (Li & Si, 2007; Li & Yang, 2003). Thirdly, the *watermarking function* f_w masks the contents of the mammogram with watermarking key K_w so that users below Level 1 cannot view the contents.

The *embedding* process starts with a segmentation operation f_p of the mammogram, aiming at partitioning the original image I_o into medically insignificant *background* area I_o^b and medically *vital* area I_O^v, which covers the breast. The segmentation function f_p for partitioning an image I_o is defined as

$$\left(I_o^v, I_o^b\right) = f_p(I_o)\,. \tag{1}$$

where I_o^v and I_o^b represent the vital area and the background area, respectively.

The patient's textual information, which is accessible only by Level 2 users, is then embedded in the mammogram using the steganographic function, f_s, to create a *stego-image* I_s, which shows only readable pictorial contents, but not the sensitive textual information, and is accessible by users at Level 1 and 2. Because we do not want to distort the pictorial contents that are supposed to be available to users at Level 1 and 2 and in the authentication process for detecting manipulation, so the steganographic function only embeds the textual information in the background area. To prevent other users from accessing the pictorial contents, the watermarking function, f_w, is then performed on stego-image I_s to mask its contents.

Because the segmentation results are content-dependent, i.e., they are different for different mammograms. The necessary conditions for replacing the hidden information in the background area with another version from a different mammogram without knowing the stego-key are 1) the attacker must be able to segment the two mammograms correctly, 2) the boundary dividing the background and vital areas in both mammograms must be the same and 3) the contents of the two mammograms must be exactly the same because the pictorial contents have to be involved in the hiding and extraction processes of the textual patient information, otherwise the correct patient information cannot be extracted even if the first two conditions were met.

As a steganographic function, f_s is to hide the patient's textual information T into I_o^b using stego-key K_s and I_o^v, it can be expressed as

$$I_s = f_s\left(I_o^b, I_o^v, T, K_s\right) \tag{2}$$

where I_s is the stego-image with hidden patient information, T.

To tighten access control further, a watermarking function, f_w, is applied to the stego-image, I_s, with the aid of a watermarking key, K_w, in order to mask the pictorial information / contents of the stego-image. A cryptosystem can certainly serve the purpose of scrambling the pictorial information by encrypting it. However, it is difficult to tell a corrupted file from a valid encrypted one before decryption is carried out. *Transparent encryption* is a technique that allows the details or the high resolution components of media to be encrypted while leaving the low resolution components visible to the viewers. This technique has been used for access control in various multimedia applications (Engel et al, 2008; Grangetto et al, 2006; Pommer & Uhl, 2003). Although similar technique can be used to serve the purpose of masking the pictorial contents of mammograms in our application, selecting images components for encryption and decryption is by no means trivial. This motivates our resort to digital watermarking, which requires less computational costs. The degree of masking can be adjusted by setting a watermarking strength factor α. The operation of the watermarking function can be express as

$$I_w = f_w(I_s, K_w, \alpha). \tag{3}$$

where I_w is the masked / watermarked version of the stego-image, I_s. As the watermarking strength factor α becomes greater, more pictorial details in the stego-image are masked.

The *extraction* process describes how users access the stego-image and extract the textual information according to the availability of access keys. The inverse watermarking function f_w^{-1} allows Level 1 and Level 2 users to unmask image I_w in order to reveal stego-image I_s by submitting K_w. By submitting both K_w and K_s, a Level 2 user can gain further access to the patient information, *T*, with the aid of the inverse steganographic function, f_s^{-1}.

4. IMPLEMENTATION OF THE CONCEPTUAL FRAMEWORK FOR MAMMOGRAMS

We have presented a conceptual framework for protecting mammogram databases on PACSs in the previous section. In this section we propose specific techniques for realizing the constituent components of the framework. Note that because of the framework's generic nature, although the techniques we proposed in this section are novel at present, they can be replaced in the future with new techniques without modifying the framework as the state-of-the-art evolves.

4.1. Pre-processing

We observed that, on average, 80% of the pixels in the background areas, I_o^b, of mammograms have a gray level of 0. So it is quite easy for the attacker to guess the embedded information without knowing K_s. For example, if the gray level of a background pixel of a *watermarked* mammogram equals 4, the probability that the embedded information equals 4 is 0.8. This is an apparent security gap to be closed. Also as described in Section 4.3, for non-zero-valued pixels, most of the times secret message can be embedded by either increasing or decreasing the gray levels, depending on which way results in lower distortion. However, to embed secret message in zero-valued pixels, the only choice is to increase the gray level, resulting in higher distortion (See Section 4.3 for details). To circumvent these two problems, for each zero-valued pixel *b*, we modify its gray level by assigning it a random number in the range of $[0, 2^{c_M-1}-1]$ generated with K_s, where C_M is the maximum number of secret bits we want to embed. Since zero-valued pixels appear in the background area only and we only hide patients' information in the background area, this pre-processing does not change the vital area.

4.2. Segmentation

The mission of the segmentation is that when given either the original image, I_o, during the embedding process or the stego-image, I_s, during the extraction process as input, the segmentation function, f_p, should partition the input image into the same bi-level output image, with one level corresponding to the background area and the other to the vital area. Figure 3(a) shows a typical mammogram with the intensity represented with 8 bits. We can see that it has a dark background with the intensity below 30 and a significantly brighter area of a breast with the intensity of most pixels above 100. Since we will hide the textual information in the background area and the distortion due to data hiding should not raise the intensity significantly, so a threshold between 50 and 100 for partitioning the images is a reasonable value. However, due to the fact that the mammograms in the database may be taken at different times with different equipments under various imaging conditions, using a heuristic constant threshold to segment mammograms is not feasible. So we proposed to use *moment-preserving thresholding* (Tsai, 1985), which is content-dependent, to perform the segmentation task.

Given a gray-scale image, *I*, with *X* × *Y* pixels, we define the intensity / gray scale at pixel (x, y) as $I(x, y)$. The *i*th *moment* of the image is defined (Tsai, 1985) as

$$m_i = \left(\frac{1}{X \times Y}\right) \sum_{x=1}^{X} \sum_{y=1}^{Y} I^i(x, y) \tag{4}$$

A transform is called *moment-preserving* if the transformed image I' still has the same moments as *I*. In the context of binary segmentation, to divided *I* into two classes of p_o and p_1 pixels with gray scale z_o and z_1, respectively, we can find a threshold *t* by first solving Eq. (5) as formulated below

$$\begin{cases} p_0 z_0^0 + p_1 z_1^0 = m_0 \\ p_0 z_0^1 + p_1 z_1^1 = m_1 \\ p_0 z_0^2 + p_1 z_1^2 = m_2 \\ p_0 z_0^3 + p_1 z_1^3 = m_3 \end{cases}. \tag{5}$$

Once z_o, z_1, p_o and p_1 are obtained, setting the threshold *t* to a value between the gray scales of p_o th and (p_o +1)th pixels will yield segmentation result I' that preserves the first four moments (i.e., m_o to m_3) of *I* (Tsai, 1985). From the above description, we know that to make sure the algorithm uses the same segmentation result in both embedding and extraction processes, when given the original image I_o and stego-image I_s, respectively, as the input image *I*, the algorithm should yield the same values for p_o and p_1. Because the significant gap between the background and vital areas in both I_o and I_s, our experiments have proved the feasibility of the use of the moment-preserving thresholding method. The reader is referred to (Tsai, 1985) for more details about moment-preserving thresholding.

After moment-preserving thresholding, some pixels with low intensity in the vital area may be classified as background pixels. Moreover, the smoother intensity transition across the boundary separating the background and the vital / breast areas may also cause misclassification. To compensate for these two types of misclassifications, a morphological operation of 'dilation' (Gonzalez & Woods, 2002) with a disk of radius equal to 5 pixels is applied to the vital area so as to allow the vital area to grow and background area to shrink.

4.3. Information Hiding through Steganographic Function

The proposed method is essentially inspired by QIM watermarking (Chen & Wornell, 2001). The idea of hiding *l*-bit secret data *t* in a pixel with gray level equal to *b* is first to 'project' *b* in a secret key-controlled manner onto a range, in which each index in the index set of {0, 1, 2, ... , 2^l-1} can be *repeatedly* used to index the values of the new range. Secondly, the projected gray level, now represented by *p* is modulated so that the new value *p'* (i.e. the gray level of the stego-pixel) lands on an index equal to the value of the *l*-bit secret data *t*. Because the indices repeat, data hiding can be achieved

by modulating the pixel in question upwards or downwards, depending on which way results in lower distortion. To extract the hidden data, the algorithm simply establishes the same range and takes the index corresponding to the gay level of the stego-pixel as the hidden data. The way of projecting the original gray level *b* to a new value *p* will be described later. For the moment, let us use Figure 2 to demonstrate the idea of embedding 3-bit secret data in the already projected gray level *p*. Figure 2 shows that the projected value, *p*, equals 11 and falls in a range, *R*, of [0, 31], which allows the index set of {0, 1, 2, ..., 7} to be repeatedly used for indexing the elements in that gray level range, with index 0 synchronised with the lower bound of the range, *R*, (i.e., 0). We can see that *p* corresponds to index 3. Now suppose the 3-bit secret data *t* equal 0. We could hide *t* in *p* by changing *p* to either 8 or 16 because they both correspond to the same index (secret data), which is 0. However, we can see that changing *p* to 16 incurs a distortion of 5 while changing it to 8 leads to a distortion of 3 only. Therefore, the algorithm will choose to change *p* to 8 (i.e, $p' = 8$). To extract the hidden data, the algorithm establishes the same projected range and takes the index corresponding to p' (i.e., 8), which is 0, as the hidden data.

Because the modulation indices are allowed to repeat, we call our steganographic method *Repetitive Index Modulation* (*RIM*) based steganography. As data hiding could be achieved by modulating either upwards or downwards, and, the probability distribution of secret data is uniform, therefore, the expected distortion D_{RIM} incurred in the hiding of a 3-bit secret data is

$$D_{RIM} = \frac{1}{8}(0+1+2+3+4+1+2+3) = 4.$$

The general form of the expected distortion D_{RIM} in terms of *difference between the original pixel and stego-pixel* incurred when embedding *l*-bit secret data is

$$D_{RIM} = \frac{1}{2^l}\left(2^{l-1} + 2\cdot\sum_{i=1}^{2^{l-1}-1} i\right)$$

$$= 2^{l-1} \tag{6}$$

Since the proposed method allows changes to be made to any bits, therefore the security is greater than LSB steganography.

Now let us describe how a gray level *b* is projected onto a range, *R*, in which repetitive indices could be used to hide secret data. In this work, we use a fixed range of [0, 2^l + *B*), where *B* is the upper bound of the gray levels (e.g, if a pixel is represented with 8 bits, then *B* = 255). Since the range is fixed / known, the projection of gray level *b* has to be done in a secret manner as follows.

$$p = r + b \tag{7}$$

where *r* is a key generated random number in the range of [0, 2^l -1]. From Eq. (7), we can see that $0 \le p < 2^l + B$. To hide the secret data, the modulation as described in Eq. (8) is carried out so that *p'* falls on the index that is equal to the secret data and closest to *p*.

$$p' = r + b' \tag{8}$$

Actually, the upper bound of *r* can be an arbitrary number greater than 2^l -1. However, without the secret key, an exhaustive attack on the steganographic method is to exhaust the 2^l possible cases for each pixel, therefore an upper bound of *r* greater than 2^l -1 is not necessary.

The afore-mentioned RIM-based steganographic method is a general data hiding idea. To hide patients' textual information *T* into a mammogram, we apply this method in a *content-based* manner. The idea is to pair up each pixel *b* in the background area (i.e., the embeddable area) with another pixel *v* picked from the vital area (i.e., the non-embeddable area) at random according to stego-key K_s and define *r* in Eq. (7) and (8) as

$$r = \left[rand\_no + b \right] \bmod 2^l \tag{9}$$

where *rand_no* is a random number in [0, 2^l -1] generated by stego-key K_s and "mod" is the modulo operation. By comparing Eq. (7) and (8) we can see that the vital information *v* is involved in the embedding process, but its value is not changed. Therefore no distortion is inflicted on *v*. Note that we will use *b* and *v* to represent the two pixels and their gray scale / intensity interchangeably. The content-based RIM steganographic function is summarized as follows.

RIM Steganographic Function f_s for Textual Information Embedding

Step 1. Establish the projection range, *R*, of [0, 2^l + *B*) and synchronize index 0 with the lower bound of *R*.

Step 2. For each pixel *b* in the background area, find its partner pixel *v* from the vital area at random according to K_s. Note we allow different pixel *b*s to be assigned the same partner *v*.

Step 3. For each pair of *b* and *v*, project the gray level *b* onto *p* in *R* using a secret key K_s and Eq. (7).

Step 4. Obtain the *l*-bit secret data *t* from the patients' textual information *T*.

Step 5. Modulate *p* according to Eq. (7) and (8) so that its modulated counterpart *p'* falls on the index equal to the secret data *t* and closest to *p*.

4.4. Pictorial Content Masking through Watermarking Function

After stego-image I_s is created by the stegonagraphic function f_s, the watermarking function f_w is performed to mask its pictorial contents. Because the purpose of the proposed watermarking function is to 'distort' the stego-image, in a reversible manner, in order to mask its pictorial details, unlike most watermarking schemes, which are aimed at reducing the distortion as much as possible if the robustness requirement is met, it embeds the watermark generated by K_w with a much greater embedding strength

α. To allow the content-based inverse steganographic function f_s^{-1} to be able to extract the textual information based on the same pictorial contents, the proposed watermarking function must be reversible. That is to say that the watermark pattern must be completely removable and the stego-image should be perfectly recoverable when the inverse watermarking function f_w^{-1} is applied. The watermarking function is summarized as follows.

Watermarking Function f_w for Masking Stego-image

Step 1. Perform Discrete Cosine Transform (DCT) on I_s. Note without loss of generality, we use the same symbol (e.g., I_s) to represent images in both spatial and transform domains.

Step 2. Perform f_w on each DCT coefficient of I_s using K_w such that

$$\begin{aligned} I_w &= f_w(I_s, K_w, \alpha) \\ &= I_s \times (1 + \alpha \cdot W) \end{aligned} \tag{10}$$

Step 3. Perform Inverse DCT on I_w

The embedding strength α can be set to achieve the required masking effect.

4.5. Extraction Process

For Level 1 and Level 2 users with K_w, by applying an inverse watermarking function f_w^{-1}, the masked stego-image I_s can be perfectly recovered according to the following algorithm.

Inverse Watermarking Function f_w^{-1} for Unmasking Stego-image

Step 1. Perform Discrete Cosine Transform (DCT) on I_w.

Step 2. Perform f_w^{-1} on each DCT coefficient of I_w using K_w such that

$$I_s = f_w^{-1}(I_w, K_w, \alpha) = \frac{1}{(1+\alpha \cdot W)} I_w \quad (11)$$

Step 3. Perform Inverse DCT on I_s.

For a Level 1 user, stego-image I_s is the only data accessible. But for Level 2 users, by using stego-key K_s, the patient's textual information can be extracted. To do so, the same moment-preserving thresholding algorithm introduced in Section 4.2 is employed to segment the stego-image into background and vital areas first.

In the extraction process, to extract the hidden information from each b', we again pair up each pixel b' in the background area with another pixel v from the vital area according to K_s. Note because the vital information v is not modulated during the embedding process, therefore we still use v, instead of v' in the extraction process. Because K_s is the same key used during both embedding and extraction processes, the same paring is guaranteed. We can see that the pairing operation involves the pictorial information in the vital / breast area in both textual information hiding and extraction processes. Should the pictorial contents of the stego-image be manipulated, the algorithm will fail to extract the textual information due to the inconsistent pictorial content, thus alerting the users of the false authenticity and integrity of the image. The inverse steganographic function f_s^{-1} for textual information extraction is formulated as follows.

Inverse Steganographic Function f_s^{-1} for Textual Information Extraction

Step 1. Establish the projection range, *R*, of [0, $2^l + B$) and synchronize index 0 with the lower bound of *R*.

Step 2. For each pixel b' in the background area, find its partner pixel *v* from the vital area at random according to K_s. Note we allow different pixel b's to be assigned the same partner *v*.

Step 3. For each stego-pixel, project its gray level *x′* onto *p′* in *R* using a secret key K_s and Eq. (7) and (9).

Step 4. Find the modulation index corresponding to *p′* and take it as the secret data *t*.

5. EXPERIMENTAL RESULTS AND DISCUSSIONS

The mammograms used in the experiments are of size 1024 × 1204 pixels from the Mammographic Image Analysis Society (MIAS) (Wang, 2004). Figure 3 shows the images produced at different stages during the embedding process. A mammogram as shown in Figure 3(a) is segmented into background and breast areas as shown in Figure 3(b). In order to reserve the medical details on the edge of the breast, dilation is performed to enlarge the breast area (Figure 3(c)) so that none of the vital / breast pixels are classified as background pixels. Figure 3(d) shows the stego-image, I_s, after the patient's textual information is embedded. Finally, the stego-image is masked to produce the marked image, I_w, as depicted in Figure 3(e) by the watermarking function to protect the whole mammogram.

To analyze the performance of the proposed scheme, we test our steganographic function f_s on 5 different mammograms with *l*, the number of bits of the patient's textual information is set to k = 2, 3 and 4, respectively. We can see from Table 2 that for all mammograms the proposed RIM steganographic method outperforms the LSB method in terms of embedding distortion, measured by *average difference between the original pixel and stego-pixel* (i.e., $|b - b'|$). Note that although the

pixels in the vital area are involved in the data hiding process according to Eq. (9), the data hiding process is applied to the background area only; therefore no distortion is inflicted on the vital area. The statistics listed in Table 2 are only relevant to the background area. Note the distortion statistics of RIM in Table 2 are slightly deviated from the expected values 1, 2, and 4 for k = 2, 3 and 4, respectively, as predicted by Eq. (6). This is because there are around 80% of the zero-valued pixels in the background area, which force the RIM steganographic method to modulate the pixels in upward direction only.

In this study, content masking is intended to prevent unauthorized people from viewing the contents of mammograms. To mask the contents of the mammograms, strength α of the reversible watermarking function in Eq. (10) can be set for different security levels. Figure 4 demonstrates the masking effects when different values of α are used. When α equals 0.5, major details in the mammogram are obscured as shown in Figure 4(a). When α is set to 10, the mammogram is completely masked as depicted in Figure 4(c).

6. CONCLUSIONS

In this work, a role-based access control framework using data hiding techniques is proposed for combating security threats faced by mammogram databases in PACSs. Access to the databases and the information contained in the mammograms are controlled through the issuance of the stego-key and the watermarking key. The scheme alleviates the drawbacks, such as separable header and storage overhead of the header, of encryption-based schemes and enhances the security by embedding the patients' textual information in the contents of the mammograms and allowing authentication to be carried out. The content-dependent steganographic function hides the patients' textual information by using the stego-key, which is only assigned to the users with the highest access right, and involving the pictorial contents in the embedding process, which allows the inverse steganographic function to carry out

authentication when extracting the hidden textual information. The reversibility of the watermarking function makes the stego-image recoverable so that the hidden textual information can be authenticated by the inverse steganographic function through the involvement of the same pictorial contents used during the embedding process. Moreover, the scheme is compatible with mammogram transmission and storage on PACS. We are currently investigating the possibilities of tailoring the proposed framework for protecting other types of medical images.

7. REFERENCES

Cao, F., Huang, H. K. & Zhou, X. Q. (2003). Medical Image Security in a HIPAA Mandated PACS Environment. *Computerized Medical Imaging and Graphics*, 27(2), 185–196.

Chen, B. & Wornell, G. W. (2001). Quantization Index Modulation: A Class of Provably Good Methods For Digital Watermarking and Information Embedding. *IEEE Transactions on Information Theory*, 47(4), 1423-1443.

Engel, D., Stütz, T. & Uhl, A. (2008). Efficient Transparent JPEG2000 Encryption. In C.-T. Li (Ed.), *Multimedia Forensics and Security*. Hershey, PA: Information Science Publishing.

Fridrich, J. & Goljan, M. (2004). On Estimation of Secret Message Length in LSB Steganography in Spatial Domain. *Proc. SPIE,Security, Steganography, and Watermarking of Multimedia Contents VIII*, 5306, 23-34.

Gonzalez, R. C. & Woods, R.E. (2002). *Digital Image Processing*, MA: Prentice Hall.

Grangetto, M., Magli, E. & Olmo, G. (2006). Multimedia Selective Encryption by Means of Randomized Arithmetic Coding. *IEEE Transactions on Multimedia*, 8(5), 905–917.

Ker, A. (2007). Steganalysis of Embedding in Two Least-Significant Bits. *IEEE Transactions on Information Forensics and Security*, 2(1), 46-54.

Kern, A., Kuhlmann, M., Kuropra, R. & Ruthert, A. (2004). A Meta Model for Authorizations in Application Security Systems and Their Integration into RBAC Administration. *Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies,* 87-96.

Li, C.-T. & Si, H. (2007). Wavelet-based Fragile Watermarking Scheme for Image Authentication. *Journal of Electronic Imaging*, 16(1), 013009-1 - 013009-9.

Li, C.-T. & Yang, F. M. (2003). One-dimensional Neighbourhood Forming Strategy for Fragile Watermarking. *Journal of Electronic Imaging*, 12(2), 284-291.

Long, M. & Wu, C. H. (2006). Energy-Efficient and Intrusion-Resilient Authentication for Ubiquitous Access to Factory Floor Information. *IEEE Transactions on Industrial Informatics,* 2(1), 40-47.

Osborne, D., Abbott, D., Sorell, M. & Rogers, D. (2004). Multiple Embedding Using Robust Watermarks for Wireless Medical Images. *Proceedings of the 3rd International Conference on Mobile and Ubiquitous Multimedia,* 245-250.

Planitz, B. M. & Maeder, A. J. (2005a). A Study of Block-based Medical Image Watermarking Using a Perceptual Similarity Metric. *Proceedings of the Workshop on Digital Image Computing: Technqiues and Applications,* 483-490.

Planitz, B. M. & Maeder, A. J. (2005b). Medical Image Watermarking: A Study on Image Degradation. *Proceedings of the Workshop on Digital Image Computing: Technqiues and Applications,* 3-8.

Pommer, A. & Uhl, A. (2003). Selective Encryption of Wavelet-Packet Encoded Image Data — Efficiency and Security. *ACM Multimedia Systems* (*Special issue on Multimedia Security*), 9(3), 279–287.

Thomas, R. K. & Sandhu, R. S. (1994). Conceptual Foundations for a Model of Task-Based Authorizations. *Computer Security Foundations Workshop VII*, 14-16.

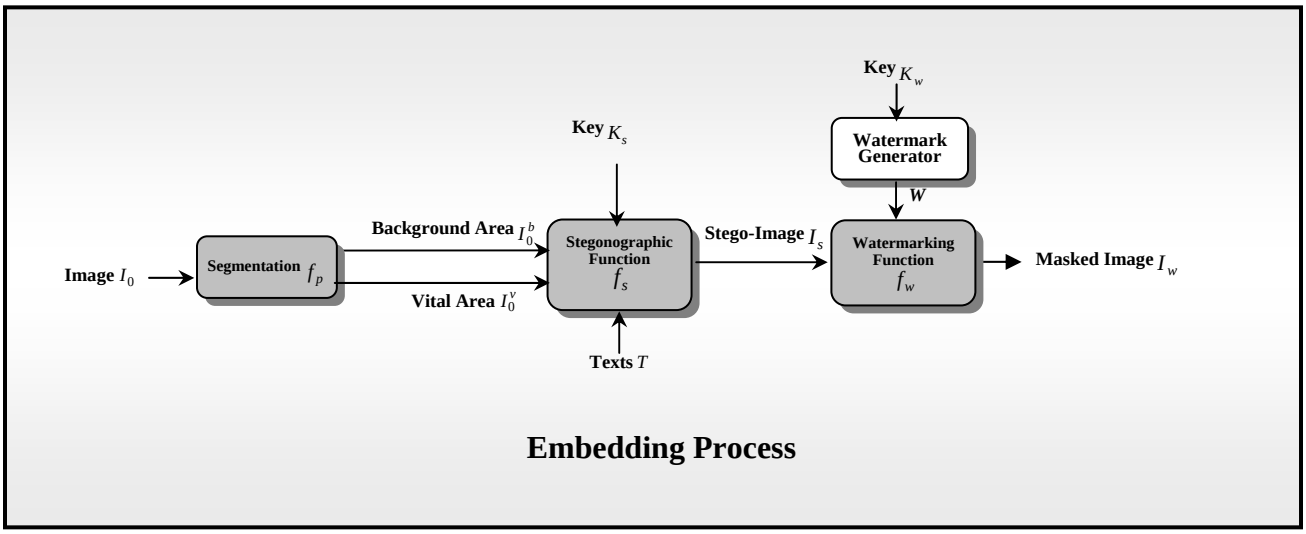
Tian, J. (2003). Reversible Data Embedding Using a Difference Expansion. *IEEE Trans. on Circuits and Systems for Video Technology*, 13(8), 890-896.

Tsai, W.H. (1985). Moment-Preserving Thresholding: a New Approach. *Computer Vision, Graphics, and Image Processing*, 29(3), 377-393.

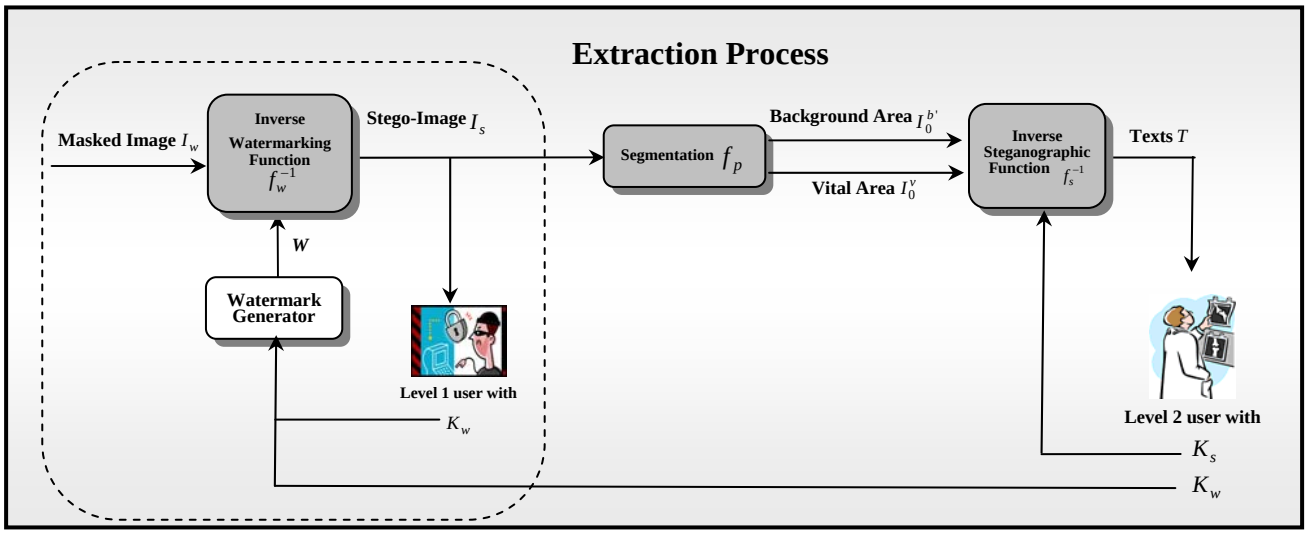
Wang, M., Lau, C., Matsen, F.A. & Kim, Y.M. (2004). Personal Health Information Management System and its Application in Referral Management. *IEEE Transactions on Information Technology in Biomedicine*, 8(3), 287-297.

Xu, Y.F., Song, R., Korba, L., Wang, L.H., Shen, W.M. & Lang, S. (2005). Distributed Device Networks with Security Constraints. *IEEE Transactions on Industrial Informatics*, 1(4), 217-225.

Zhou, X. Q. & Huang, H. K. (2001). Authenticity and Integrity of Digital Mammography Images. *IEEE Transactions on Medical Imaging*, 20(8), 784-791.



(a) The embedding process of the proposed framework



(b) The extraction process of the proposed framework

Figure 1. The proposed mammogram protection framework.

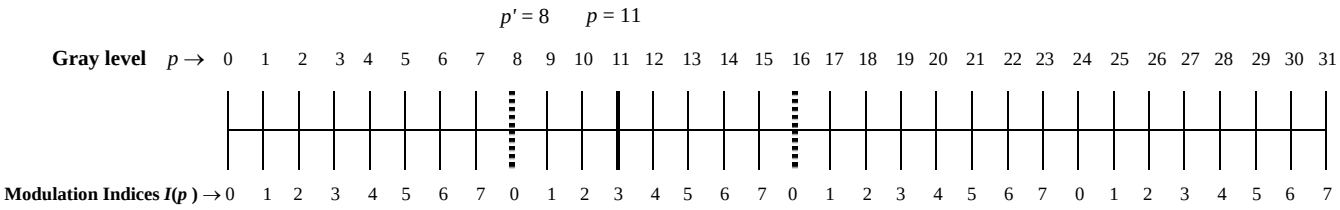


Figure 2. The method for modifying the numbers in order to embed 3-bit message.

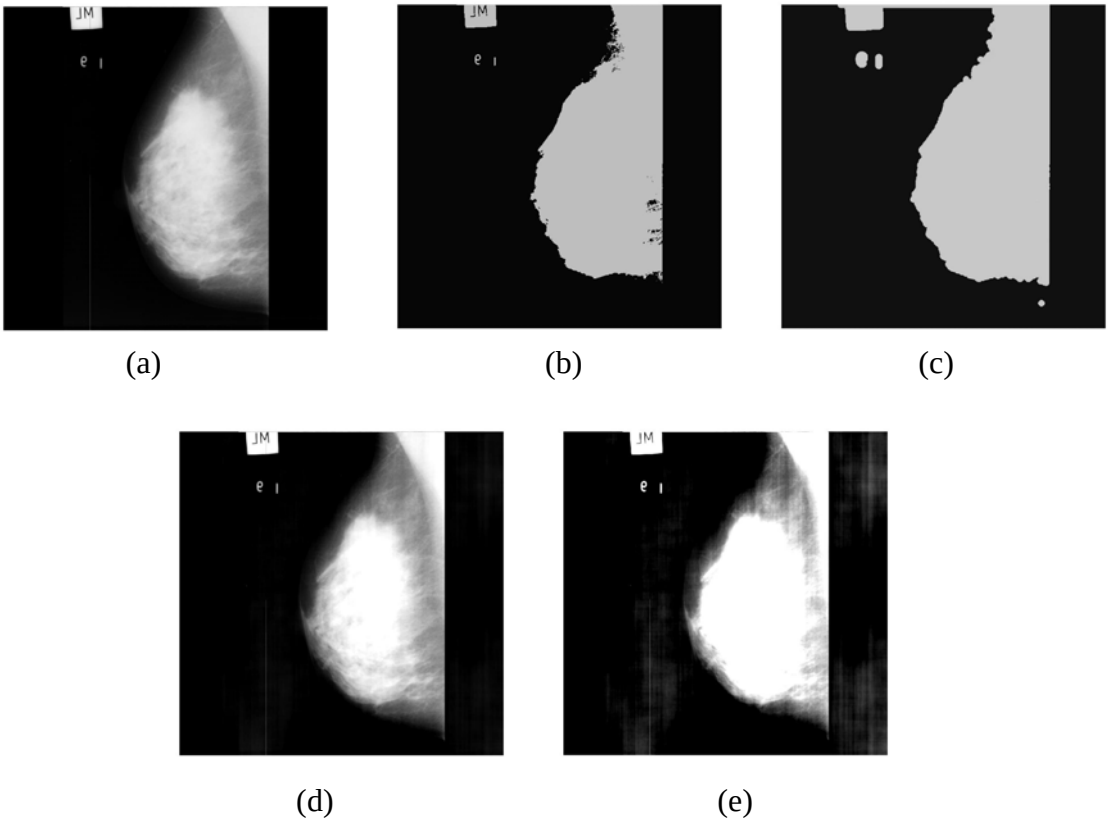
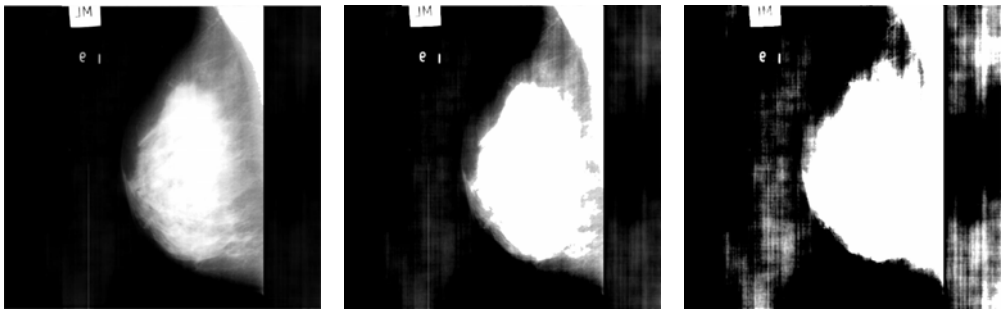


Figure 3. Embedding process. a) Original Mammogram; b) Segmented Mammogram; c) Dilated Mammogram; d) Stego-Mammogram, I_s; e) Masked Mammogram I_w.



a) $\alpha = 0.5$ b) $\alpha = 5$ c) $\alpha = 10$

Figure 4. Mammograms masked with different watermark embedding strength α

Table 1. Classification of roles of users, their access rights and keys in the conceptual framework.

Roles / users	Access rights	Access keys issued
Level 0 user	No right given. (The contents of the mammograms are marked and unavailable to the users)	no key
Level 1 user	Stego-images (i.e., the mammograms with hidden patient information which cannot be extracted)	K_w
Level 2 user	Stego-imagse and patient information	K_s, K_w

Table 2. Pperformance comparison between the proposed RIM steganographic and LSB methods in terms of embedding distortion measured by *average difference between the original pixel and stego-pixel* when the length of the secret data to be embedded in each pixel is set to k = 2, 3 and 4, respectively.

Images	***k* = 2**		***k* = 3**		***k* = 4**	
	RIM	**LSB**	**RIM**	**LSB**	**RIM**	**LSB**
Mamm1	1.14	1.18	2.14	2.40	4.54	5.07
Mamm2	1.19	1.20	2.16	2.45	4.42	5.20
Mamm3	1.15	1.17	2.16	2.45	4.32	5.11
Mamm4	1.14	1.17	2.17	2.45	4.32	5.11
Mamm5	1.15	1.17	2.13	2.50	4.35	5.11