Secure Transmission of Digital Mammography Images in Public Network

Shruthija V S
Computer Science and Engineering
Reva Institute of Technology & Management
Bangalore, India.
shruthija.smiles@gmail.com

Kiran Kumari Patil
computer science and engineering
Reva Institute of Technology & Mangement
Bangalore, India
kirankumari@revainstitution.org

Abstract-**Breast Cancer is one of the dangerous diseases in most of the countries. There are many techniques for early detection of breast cancer to prevent from death. Most commonly used techniques are massive screening, physical examination, MRI scanning, X-ray, ultrasound scanning. However, these techniques have several technical limitations that reduce the diagnostic accuracy. Digital mammography technique can be used for the early dectection of breast cancer.It is most efficient and it provides additional features.Data security is a very important issue when mamommographic images transferred in public network.Generally security is characterised in terms of privacy, authenticity and integrity. All the above three aspects should be considered in a telemammography system.In this paper we describe how to implement data security in telemammography system by using public key cryptography techniques.AIDM is an effective method for image authenticity and integrity in telemammography application.**

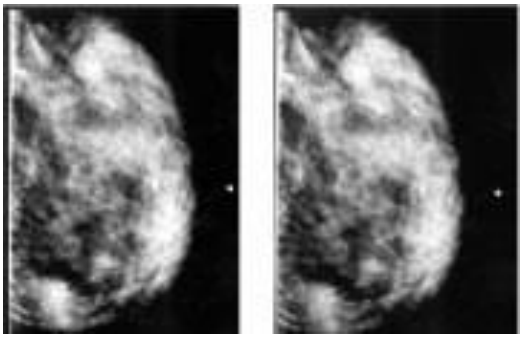
Keywords:Data embedding; cryptography; digital mammography; Image authenticity and integrity; telemammography.

I. INTRODUCTION

Breast cancer is the fourth most common cause of death among women in the United States. Current attempts to control breast cancer concentrate on early detection by means of massive screening, via periodic mammography and physical examination, because ample evidence indicates that such screening indeed can be effective in lowering the death rate. Today, film-screen mammography is the most common and effective technique for the detection of breast cancer .However, the film-screen image recording system of current mammography has several technical limitations that can reduce breast cancer diagnostic accuracy .Digital mammography can overcome most of the problems existing in film-screen mammography, and at the same time provide additional features not available with standard film-screen mammographic imaging such as contrast enhancement, digital archiving and computer-aided diagnosis.Digital mammography uses the DICOM standard in which the patient information including name, birth date, home address, gender, and history are included in the object.classes. This information is sensitive to the patient and important for radiologist's diagnosis.

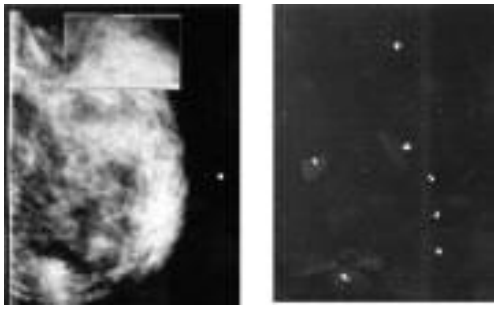
Telemammography requires the use of FFDM units at the examination site and is built on the concept of an expert center. It allows radiologists with the greatest interpretive expertise to manage and read in real time all mammography examinations. Specifically, in principle, telemammography increases efficiency, facilitates consultation and second reading, improves patient compliance, facilitates operation, supports computer-aided detection and diagnosis, allows centralized archive, distributive reading, and enhances education through telemonitoring. Some of these advantages are being validated in clinical research environment uses a high speed tele-imaging WAN connecting the examination site with the mammography expert center, so that IMs from a remote examination site can be sent to the expert center in almost real time.

Data security becomes a very important issue when mammographic images are transmitted in a public network. Fig. 1 gives an example of a digital mammogram with artificial calcifications inserted. Fig. 1(a) is the original mammogram, (b) is the mammogram with artificial calcifications added, (c) is the magnification of a region containing some added artifacts, and (d) is the subtracted images between the original and the modified mammogram. current digital technology, it is fairly easy to make modifications in a digital image. For this reason, image data integrity becomes an important issue in a public network environment. Generally, trust in digital data is characterized in terms of privacy, authenticity and integrity of the data



(a) (b)

Figure 1



(c) (d)

With. Privacy refers to denial of access to information by unauthorized individuals. Authenticity refers to validating the source of a message; i.e., that it was transmitted by a properly identified sender and is not a replay of a previously transmitted message. Integrity refers to the assurance that the data was not modified accidentally or deliberately in transit, by replacement, insertion or deletion. All the above three aspects should be considered in a telemammography system.

Many techniques can be used for data protection including network firewall, data encryption, and data embedding. Various techniques are used under different situations. For a telemammography system, since data cannot be limited within a private local area network protected by a firewall, data encryption and data embedding are the most useful approaches to adopt.

Modern cryptography can use either private-key or the public-key methods Private-key cryptography (symmetric cryptography) uses the same key for data encryption and decryption. It requires both the sender and the receiver agree on a key *a* priori before they can exchange message securely. Although computation speed of performing private-key cryptography is acceptable, it is difficult for key management. Public-key cryptography (asymmetric cryptography) uses two different keys (a key pair) for encryption and decryption. The keys in a key pair are mathematically related, but it is computationally infeasible to deduce one key from the other. In public-key cryptography, the public-key can be made public.

Anyone can use the public-key to encrypt a message, but only the owner of the corresponding private-key can decrypt it.Public-key methods are much more convenient to use because they do not share the key management problem inherent in private-key methods. However they require longer time for encryption and decryption. In real-world implementation, public keys are rarely used to encrypt actual messages. Instead, public-key cryptography is used to distribute symmetric keys which are used to encrypt and decrypt actual messages.DS is a major application of public-key cryptography. To generate a signature on an image, the owner of the private key first computes a condensed representation of the image known as an image hash value which is then encrypted by using the mathematical techniques specified in public-key cryptography to produce a DS. Any party with access to the owner's public key, image, and signature can verify the signature by the following procedure: first compute the image hash value with the same algorithm for the received image, decrypt the signature with the owner's public key to obtain the hash value computed by the owner, and compare the two image hash values. Since the mechanism of obtaining the hash is designed in such a way that even a slight change in the input string would cause the hash value to change drastically. If the two hash value are the same, the receiver (or any other party) has the confidence that the image had been signed off by the owner of the private key and that the image had not been altered after it was signed off.

In this paper, we discuss how to implement data security in a telemammography system by using existing cryptography techniques. Since privacy is a network access security issue and will not be discussed here, we will concentrate on IMs and related patient data authenticity and integrity

II. SYSTEM ANALYSIS

A. Existing System

Current attempts to control breast cancer concentrate on early detection by means of massive screening, via periodic mammography and physical examination, because ample evidence indicates that such screening indeed can be effective in lowering the death rate. Today, film-screen mammography is the most common and effective technique for the detection of breast cancer. However,the film-screen image recording system of current mammography has several technical limitations that can reduce breast cancer diagnostic accuracy. With current digital technology, it is fairly easy to make modifications in a digital image. For this reason, image data integrity becomes an important issue in a public network environment.

B. Proposed System

Digital mammography can over come most of the problems existing in film-screen mammography, and at the same time provide additional features not available with standard film-screen mammographic imaging such as contrast enhancement, digital archiving, and computer-aided diagnosis. . For a telemammography system, since data cannot be limited within a private local area network protected by a firewall, data encryption and data embedding are the most useful approaches to adopt. Data security in telemammography system is done using public key cryptography techniques.we consider examination site and expert center for data encryption and decryption respectively.In examination site key is generated using the RSA algorithm and key is encrypted with the image using the DES encryption algorithm.Further data is emdedded and sent through public network .In expert center the data is decrypted. The received image will be verified across the sent image.AIDM is an effective method for image authenticity and integrity in telemammography application.

III. SYSTEM DESIGN AND DEVELOPMENT

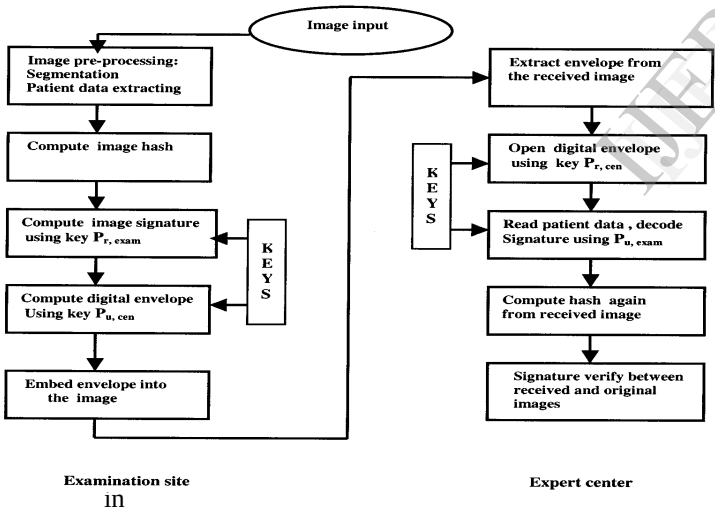


Fig.2

Fig.2 telemammography system generally consists of an examination site and an expert center, and images are transmitted from the examination site to the expert center for interpretation. Different from text files, IMs have two distinct characteristics. First, theimage size is very large. Each DICOM formatted image includes a small size header file containing sensitive patient information data and a very large image pixel data file. Second, in a16-b/pixel mammography unit the actual signal, in general, is between 12 and 14 bits, therefore, the LSB (the first bit) in each pixel is noise. This bit can be used for data embedding. Considering these characteristics, a hybrid cryptography algorithm is used to implement image authenticity and integrity in the telemammography system. When a digital mammogram is acquired at the examination site, a DS for all pixels of the image is produced and related patient data is obtained from the DICOM header. Then, both the DS and patient data are encrypted to forma digital envelope. Finally, the digital envelope is embedded into the LSB of ramdomly selected pixels of the image

IV. METHODOLOGIES

A. Data Encryption and Embedding
B. Data Extraction and Decryption
C. Digital Mammography Image

A) Data Encryption and Embedding

1)*Image-Preprocessing*: This includes segmentation of breast region and acquiring patient information from the DICOM image header. A digital mammogram can be from 4K× 5K pixels to even larger sizes. By cropping large amounts ofbackground pixels from the image, the time necessary for performing image hashing and transmission can be significantly reduced. The cropping can be done by finding the minimum rectangle covering the breast region. A method to find the minimum rectangle is given in and extracting the boundary of breast region can guarantee that data embedding is performed within the region. If the minimum rectangle is the complete image, then embedding will be performed in the entire image. Data embedded within breast tissues would be more difficult to be decoded than embedded in the background area.

2) Hashing (ID): Compute the hash value for all pixels in the image

$$\mathrm{ID} = H(\mathrm{IM})$$

Where ID-hash value of the image;H-MD5 hashing algorithm ;IM-preprocessed mammography.

MD5 has the characteristics of a one-way hash function. It is easy to generate a hash given an image (H(IM)=>ID)but virtually impossible to generate the image given a hash value(ID=>IM). Also, MD5 is “collision-resistant”. It is computationally difficult to find two images that have the same hash value. In other words, the chance of two images have the same hash value is small and it depends on the hash FFDM units, the LSB of pixels in the mammogram is mostly noise. It can be used for data embedding. This bit is excluded when calculating the image hash. Thus, only 11 bits in two bytes for each pixel in the image are used to compute the hash (shift the pixel

"right" for 1 bit, then set bit 16, 15, 14, 13, and 12 as zero).

3)Digital signature: Produce a DS based on the above image hash value

$$DS=RSA_E(P_{r,exam,}ID)$$

Where DS-DS of the mammogram;RSA_E-RSA public-key encryption algorithm; $P_{r,exam}$-private key of the examination site.

4) Digital Envelope: Concatenate the DS, and the patient data together as a data stream, and encrypt them using the DES algorithm

$$Data_{encrypted}=DES_E(key_{DES},Data_{concat})$$

Where $Data_{encrypted}$-data encrypted by DES;DES_E-DES encryption algorithm;Key_{DES}-session key produced randomly by the cryptography library;$Data_{concat}$-concatenated data stream of the DS and patient information.

The DES session key is further encrypted

$$Key_{encrypted}=RSA_E(P_{u,cen},key_{DES})$$

Where $Key_{encrypted}$ is the encrypted session key; $P_{u,cen}$ is the public key of expert center

Finally, the digital envelope is produced by concatenating the encrypted data stream and encrypted session key together

$$ENV=(Data_{encrypted})conc.(key_{encrypted})$$

5) Data Embedding: Replace the LSB of a random pixel in the segmented mammogram by one bit of the digital envelope bit stream and repeat for all bits in the bit stream.

First, a set of pseudorandom numbers X_n is generated by using the standard random generator

$$X_{n+1}=(aX_n+C)mod\ m$$

Where a-Multiplier; C-Additive constant; m-mod denoting the modulus operation.

Equation represents the standard linear congruential generator, the three parameters are determined by the size of the image. In our experiment, a, c, m were set to be 2416,37444, and 1771875, respectively, based on our experience with the digital mammography unit used. To start, both the examination site and the expert center decided a random number X_o, called the seed. The seed is then the single number through which a set of random numbers is generated using. Unlike other computer network security problems in key-management, the number of expert sites and examination sites are limited in telemammography application, the seed-management issue can be easily handled between a mutual agreements between both sites.

Second, a random walk sequence in the whole segmented image is obtained

$$WalkAddress_n=M(X_n/m)$$

Where $WalkAddress_n$- location of the randomly selected pixel in the segmented mammogram; M: Total number of pixels in the segmented mammogram

Finally, the bit stream in the envelope is embedded into the LSB of each of these randomly selected pixels along the walk sequence.

B)Data Extraction and Decryption

In the expert center, the digital mammogram along with the digital envelope is received. We can check the image authenticity and integrity by verifying the DS in the envelope using a series of reverse procedures. First, the same walk sequence in the image is generated by using the same seed known to the examination site, so that the embedded digital envelope can be extracted correctly from the LSBs of these randomly selected pixels. Then, the encrypted session key in the digital envelope is restored

$$Key_{DES}=RSA_D(P_{r,cen},Key_{encrypted})$$

Where RSA_D is the RSA public-key decryption algorithm; $P_{r,cen}$- Private key of the expert center;

After that, the digital envelope can be opened by the recovered session key, and the DS and the patient data in can be obtained

$$Data_{merged}=DES_D(key_{DES},Data_{encrypted})$$

Where DES_D is the DES decryption algorithm.

Finally, the ID is recovered by decrypting the DS

$$ID=RSA_D(P_{u,exam},DS)$$

Where $P_{u,exam}$ is the public key of the examination site.

At the same time, a second image hash value is calculated from the received image with the same hash algorithm shown in used by the examination site.If the recovered image hash value from and the second image hash value match, then the expert center can be assured that this image is really from the examination site, and that none of the pixels in the image had been modified. Therefore, the requirement of image authentication and integrity has been satisfied.

C) Digital Image Mammography:

FFDM images including large and small breasts had been tested with the AIDM in the examination site, the input is a full-field digital mammogram (Fisher Medical Imaging Corporation, Denver, CO), and the output is the image with the digital envelop embedded. In the expert center, expertscan manipulate the embedded IM and verify its authenticity and integrity.

V. CONCLUSION

DS can be used to verify image authenticity and integrity. Generally, a DS is attached to the head or the end of the image data file. In this paper, we present an algorithm, AIDM, by embedding the DS and some sensitive information such as patient ID into the image itself. Comparing to appending the DS on the head or at the end of the file, our method has several advantages. First, it does not change the file size. Second, it does not need to redefine the file format. These two advantages have an add-on value that the embedded image still confirms with the DICOM image format standard which is very important for medical image communications. Finally, because the embedded envelope in the image is invisible, it would be difficult to be removed deliberately or undeliberately. Our results demonstrate that embedding DS into a mammogram using standard data encryption technique is an effective method for verifying image authenticity and integrity in Telemammography.AIDM is an effective method for image authenticity and integrity in telemammography application.

VI. REFERENCES

[1]C. C. Boring, T. S. Squires, and T. Tong, *Cancer Statistics*, vol. 42, pp. 19–38, 1992.

[2]S. A. Feig, "Decreased breast cancer mortality through mammographic screening: Results of clinical trials," *Radiology*, vol. 167, pp. 659–665, 1988.

[3]M. Yaffe, Digital mammography, in RSNA Categorical Course in Physics, pp. 271–282, 1993.

[4]Digital Imaging and Communications in Medicine(DICOM). Rosslyn, VA: National Electrical Manufacturers' Association, 1996, PS3.1-1996-3.

[5]S. L. Lou, E. A. Sickles, and H. K. Huang *et al.*, "Full-field direct digital mammograms: Technical components, studyprotocols, and preliminary results," *IEEE Trans. Inform. Technol. Biomed.*, vol. 1, pp. 270–278,June 1997.

[6] E. A. Sickles, Physics aspects of breast imaging—Current and future considerations: Computer-aided diagnosis and telemammography: Clinical perspective telemammography, in RSNA Categorical Course in Breast Imaging, pp. 283–285, 1999.