Medical image security and EPR hiding using Shamir's secret sharing scheme

Mustafa Ulutas, Güzin Ulutas*, Vasif V. Nabiýev

Dept. of Computer Engineering, Karadeniz Technical University, 61080 Trabzon, Turkey

Abstract

Medical applications such as telediagnosis require information exchange over insecure networks. Therefore, protection of the integrity and confidentiality of the medical images is an important issue. Another issue is to store electronic patient record (EPR) in the medical image by steganographic or watermarking techniques. Studies reported in the literature deal with some of these issues but not all of them are satisfied in a single method. A medical image is distributed among a number of clinicians in telediagnosis and each one of them has all the information about the patient’s medical condition. However, disclosing all the information about an important patient’s medical condition to each of the clinicians is a security issue. This paper proposes a \((k, n)\) secret sharing scheme which shares medical images among a health team of \(n\) clinicians such that at least \(k\) of them must gather to reveal the medical image to diagnose. Shamir’s secret sharing scheme is used to address all of these security issues in one method. The proposed method can store longer EPR strings along with better authenticity and confidentiality properties while satisfying all the requirements as shown in the results.

1. Introduction

Processing and handling medical information by computers and sharing them over high-speed network infrastructure has become a common practice since wide deployment of low cost computing and networking hardware. Currently, medical text files and images are stored on disks of medical database systems for fast and reliable storage and retrieval. Besides, previously acquired images on films and written text are also digitized and archived for compatibility. Another motivation is to have complete medical information of patients available in one consistent application rather than on several information systems. Medical applications, such as telediagnosis, and teleconsultation require information exchange over an unsecure network. Protection of the integrity and confidentiality of medical images is an issue in the management of patients’ medical records. Confidentiality states that unauthorized parties should not be granted to access medical images during transmission. Integrity, on the other hand, implies that images should not be modified in any way during transmission.

Researchers proposed watermarking techniques and reported findings in the literature to satisfy both integrity and confidentiality requirements (Shih and Ta Wu, 2005; Woo et al., 2005; Zhou et al., 2001; Chao et al., 2002; Luo et al., 2003; Giakoumaki et al., 2003; Cheng et al., 2005; Acharya et al., 2004; Nayak et al., 2004; Srinivasan et al., 2004; Anand and Niranjan, 1998; Coatrieux et al., 2006; Coatrieux et al., 2008; Osman et al., 2008; Acharya et al., 2003; Kallel et al., 2009; Memon et al., 2009) while hiding EPR in medical image to make it more usable. Both fragile and robust watermarking techniques are used for integrity control and EPR hiding.

Shih and Ta Wu (2005) proposed a robust technique embedding the watermark or textual data around the Region of Interest (ROI) of a medical image based on genetic algorithms in 2005. They embed the signature image and the fragile watermark into the frequency domain of non-ROI part of a medical image. Woo et al. (2005) used a multiple watermarking method that consists of an annotation part and a fragile part. Encrypted EPR can be embedded in an annotation watermark and tampering can be detected using a fragile watermark. Their method also adopted hash-block-chaining watermarking approach in the fragile watermarking to improve security. Zhou et al. (2001) presented a method that attaches digital signature and EPR into the medical image. Their method uses LSB replacing technique to embed the signature. Chao et al. (2002) proposed a secure data hiding technique based on the bipolar multiple-base conversion to allow a variety of EPR data to be hidden within the same mark image. The mark image could be the mark of a hospital used to identify the origin of an EPR. Their technique allows separation and restoration of hidden data by authorized users.

Luo et al. (2003) presented a lossless scheme for medical image processing. Their method provides relatively high data embedding rate and original image can be recovered distortion free. Giakoumaki et al. (2003) presented a wavelet based multiple watermarking approach. Their method addresses confidentiality protection and both origin and data authentication problems by
using three separate watermarks: a robust watermark containing the doctor’s digital signature for authentication, a caption watermark with patient’s personal data, and a fragile watermark for the purpose of data integrity control.

Cheng et al. (2005) proposed a method for both record indexing and integrity protection of medical images. Hash result of the ROI is generated by Message Digest 5 (MD5) and embedded along with EPR into non-ROI parts of the medical image. Furthermore, their method is robust to some image processing attacks, cropping, sharpening, compression, and their combinations. Acharya et al. (2004) adapted watermarking for interleaving EPR with medical images during JPEG compression to reduce storage. Text files are encrypted using logarithmic technique and then interleaved in the frequency domain.

Nayak et al.’s method is based on the use of Error Correcting Codes (ECC) for reliable and robust transmission and storage of medical images with concealed patient information. EPR is coded with ECC to make it more robust to noise introduced during transmission. Their method shows that, ECC will correct the errors introduced in EPR but there is a limit for error correction. Srinivasan et al. (2004) used Bit-Plane Complexity Segmentation (BPCS) Steganography to hide medical records in color cervical images. Anand and Niranjan (1998) used LSB technique in spatial domain. Text file is encrypted using a log function. Their technique is very simple and runs very fast which makes it suitable when immediate diagnosis is required.

Coatrieux et al. (2006) focused on the complementary role of watermarking with respect to medical information security. Their work emphasized that watermarking enables a security layer at the information level providing authentication and traceability at the interface with security services in and between medical information systems. Coatrieux et al. (2008) emphasized that the ability to verify that the information belongs to the correct patient and is issued from the right source are major concerns. Their work combines an anonymized pivot number identifier with national patient identifiers to guarantee privacy and interoperability. Osman et al. (2008) proposed a novel approach to blind reversible data hiding based on integer wavelet transform in 2008. Encryption of EPR is done to provide additional security in their method. Acharya et al. (2003) adapted watermarking for interleaving patient information with medical images to reduce storage. The graphical signals are interleaved with the image. Their technique used error-correcting codes to enhance reliability of transmission and storage of medical images interleaved with patient information. Kallel et al. (2009) presented a project, which allows practitioners to use telecommunication technologies to provide early diagnosis. They proposed a reversible watermarking method used for integrity verification. They also evaluate medical image visual quality after watermark embedding.

Memon et al. (2009) proposed a method to embed the watermark information in non-ROI. Encryption of the embedded data is also done to provide additional security using of Bose–Chaudhuri–Hocquengham (BCH) in their method. Hu et al. (2010) proposed a new e-health security architecture that is contract oriented instead of session oriented which exists in most of the literature. Proposed HPKI (Hybrid Public Key Infrastructure) can be constructed from existing cryptographic technologies where various relevant security standards, tools and products are available.

In recent years, researchers used Steganography to hide EPR into medical image and used Cryptography to protect the confidentiality of the medical image (Srinivasan et al., 2004; Ho et al., 2004; Nayak et al., 2009; Li et al., 2005; Lou et al., 2009; Hu and Han, 2009). Lou et al. (2009) proposed a multiple-layer data hiding technique in spatial domain in 2009. Their work utilizes a reduced difference expansion method to embed the bit-stream in the least significant bits (LSBs) of the expanded differences. The original image can be restored after extracting the hidden data from the stego image. Another method proposed by Hu and Han (2009) makes use of a pixel based scrambling scheme to distribute the digital medical image in a secure way in 2009. Their scheme uses scrambling key derived from chaotic attractors to provide a good cryptographic strength. Their work aimed to transform the medical image into noise like image to protect the confidentiality of the image.

Secure storage and transmission is crucial in medical image security. However, recipient may copy and distribute patient’s data to others not eligible to access patient’s medical records. Disclosing information about a political leader’s or high ranking military officer’s health may cause undesirable effects and should be avoided at all costs as a government policy. Li et al. (2005) emphasized this issue in their work. Their work uses Image Adaptive Watermarking. The holder creates a broadcast image not suitable for diagnosis. Before the image can be used to diagnose an illness, a clinician must decode this image using his/her own watermark key. In their scheme, a trusted third party is in charge of the watermark key generation, distribution and update. Broadcast image looks like a medical image and has a low PSNR value. Their scheme distributes watermark keys to people in a multicast environment. In other words, one can sniff multicast messages, capture keys and view medical images. Their scheme does not consider hiding EPR in medical images.

Techniques mentioned above are designed for different requirements. Lou et al. (2009) used Steganography to hide the EPR in the medical image. Integrity and confidentiality of the medical image is not evaluated by their work. Hu and Han (2009) used Cryptography to transform medical images into noise like form to protect them. However, noisy images may attract malicious user’s attention and EPR hiding is not considered. Li et al. (2005) provided a method to protect medical images against unauthorized release. However, broadcast images exhibit clues that they are medical images. EPR hiding is not taken into account in their scheme. In 2005, Ho et al. (2004) used fragile watermarking technique to authenticate the biomedical image. However, watermarked medical image has low PSNR values and EPR hiding is not considered. Nayak et al. (2009) proposed a method using reversible Steganography to hide EPR in medical images. Their method is not capable to prove the confidentiality and authenticity of the medical image. Besides, embedding capacity of their method is related to the number of pixels at the peak point of the medical image histogram.

Each method outlined above satisfies a set of different security requirements (confidentiality, authenticity, EPR hiding) for medical image sharing. A method will be proposed to ensure the secrecy of a medical image, which satisfies the following requirements.

(i) Electronic patient records should be hidden in medical images to reduce storage requirements and network bandwidth.

(ii) Shared medical image should look like a natural image and should not attract eavesdroppers’ attention (confidentiality).

(iii) A single person should not be allowed to diagnose political leaders or high-ranking military officers since it is not adequate to trust only one.

(iv) Recipient could authenticate received images to make sure that they are not modified in any way during transmission (authenticity).

The proposed secret medical image sharing method meets all four requirements listed above by using Shamir’s secret sharing scheme (Shamir, 1979). Shamir proposed a method to partition a secret among a number of participants in 1979. His scheme is called $(k, n)$ secret sharing scheme in the literature. A secret is divided among $n$ participants. Each participant gets a piece of secret called share. If any $k$ or more shares gather, the secret is revealed. Any number of shares less than $k$ cannot be used to reveal the secret.
Shamir's secret sharing scheme uses a polynomial approach. The secret is assumed to be the constant term of the polynomial. Evaluation of the polynomial for unique values of \( x \) yields share values. In 2002, Thien and Lin (2002) adapted Shamir's scheme in secret image sharing area. After this pioneer research, Lin and Tsai (2004) used Steganography to make shares look like natural images in 2004.

Medical images are shared among \( n \) participants in this work. Holder selects \( n \) natural cover images. After selection, Shamir's approach is used for partitioning the medical image into \( n \) noise like shares. EPR of the patient is also hidden in the shares at this step. Then Steganography is used to hide these shares into \( n \) natural cover images since noise like shares may draw eavesdroppers' attention. Generated stego images look like cover images and do not attract attention since cover images are selected from natural images. Thus, images distributed to clinicians are not supposed do draw attention. If any \( k \) or more participants gather, the medical image can be revealed. In other words, at least \( k \) of the \( n \) clinicians must gather to evaluate the image and diagnose. It is assumed that at least \( k \) clinician is an adequate security measure to view the medical image to diagnose.

Thus, a novel biomedical image sharing mechanism is proposed to satisfy all security requirements mentioned above. The method generates shares with EPR hidden and saves an extra access to the patients' database. Shares look like natural images and do not draw attention which keeps them confidential. At least a group of \( k \) people should gather to reveal a patient's medical image whose medical condition should be kept secret enforced by the government policy. In other words, participants do not have access to medical information unless they gather which reduces the probability of disclosure to unauthorized parties about patient's medical condition. Moreover, the revealing algorithm has a mechanism to check shares and indicates if they are modified by a participant or corrupted during transmission and is not authentic.

The outline of the paper is as follows. Some background information on Shamir's secret sharing scheme is given in Section 2. Section 3 describes the details of the proposed scheme used for sharing medical images. Section 4 shows the experimental results of the proposed method. The conclusions are given in Section 5.

2. Review of shamir's secret sharing scheme

Shamir proposed \((k, n)\) threshold mechanism also called secret sharing scheme based on polynomial interpolation in 1979 (Shamir, 1979). Dealer constructs \( n \) shares denoted by \((S_1, S_2, \ldots, S_n)\), from a secret \( S \). The dealer selects a large prime number \( p \) and a \((k − 1)\) degree polynomial is constructed as in (1) to compute shares using the secret:

\[
F(x) = (S + a_1x + a_2x^2 + \cdots + a_{k−1}x^{k−1}) \mod p
\]  

(1)

Coefficients of the polynomial \((a_1, a_2, \ldots, a_{k−1})\) are randomly selected from integers within the range \([0, p)\). The dealer then computes shares as in (2):

\[
y_1 = (1, F(1)); y_2 = (2, F(2)), \ldots, y_n = (1, F(n))
\]  

(2)

Each share is a pair of two integers satisfying \( x_i \neq 0 \). If any \( k \) of the \( n \) pairs gathers, involved participants can reconstruct polynomial \( F(x) \) using Lagrange's interpolation technique. Therefore, all the coefficients of the polynomial are recovered. The constant term of the polynomial is the secret \( S \). Any number of participants less than \( k \) cannot recover the secret at all. Therefore, Shamir's secret sharing scheme is a perfect secret sharing scheme.

A special case where \( k = 3 \) is given in Fig. 1. Three shares are required to reconstruct the secret in this case. The polynomial is a 2nd degree and the secret is the point where the line intersects with the \( y \)-axis. Namely, this point is \((0, F(0))\).

![Fig. 1. An example of (3, 8) secret sharing scheme.](image)

Each share is a point on the polynomial. Any three or more points determine the polynomial and hence the secret. Prime number \( p \) and secret \( S \) are selected as \( 31, 7 \) respectively in this example. Other coefficients of the polynomial \((19, 21)\) are selected randomly in the range of \([0, 31)\) as in (3):

\[
f(x) = (7 + 19x + 21x^2) \mod 31
\]  

(3)

The proposed method use Shamir's method to share a medical image and corresponding EPR among \( n \) clinicians. In this way, none has all the information about the patient. Medical image will not be revealed rendering diagnosis impossible unless at least \( k \) or more clinicians gather.

3. The proposed sharing scheme

Details of the proposed sharing scheme are given in this section. There are two sub procedures: partitioning and retrieving. Partitioning procedure consists of four phases. Initialization is the first phase and is used to determine unique \( x \) values for each participant. Thus, it eliminates the need to select unique \( x \) values and then distribute them over insecure networks. Medical image and EPR are partitioned into shares by sharing algorithm in the second phase. The length of the EPR that can be embedded into the cover images is dependent on the size and bit depth of the medical image. Since Shamir's secret sharing method is employed, shares look like noisy images and may attract attention. The third phase makes use of Steganography with OPAP (Optimal Pixel Adjustment Process) to embed noise like share images into natural cover images selected by the dealer. Therefore, natural looking stego images do not draw attention during storage and transmission. The fourth phase of the partitioning procedure is the protecting phase and generates certificates for each participant.

At least \( k \) or more out of \( n \) clinicians can reconstruct the medical image by using the retrieving procedure. Retrieving procedure consists of two sub phases called verification and reconstruction. Verification phase authenticates the integrity of the share images. After the verification phase, Lagrange's interpolation technique is used by the reconstruction phase to recover the secret medical image. The details of the partitioning and retrieving procedures are given below.

3.1. Partitioning procedure

Partitioning procedure consists of four sub phases; initialization, sharing, embedding and protecting phases. Each phase is explained with details in this section.

3.1.1. Initialization phase

Shamir's framework used in second phase necessitates some intercommunication between the dealer and participants as emphasized in Zhao et al. (2009). Dealer must choose a unique
x value for each participant before the sharing procedure. Thus, the method needs a secure channel between the holder and participants during the transmission of x values. 

**Proposed method**

**1. The dealer**

D computes N = pq where p = 3 mod 4 and q = 3 mod 4. 

**2. D chooses an integer**

g ∈ [N1/2, N] such that g is relatively prime to p and q and publishes {g, N}. 

**3. Each participant randomly chooses a**

s_i ∈ [2, N] as her/his own secret shadow and computes R_i = g^s_i mod N. 

**4. Each participant provides their own R_i to D.** Dealer must ensure that R_i ≠ R_j for all participants. One R_i = R_j, dealer should demand these participants to choose new secret shadows. 

**5. Dealer randomly chooses an integer**

s_0 ∈ [2, N] such that s_0 is relatively prime to (p − 1) and (q − 1). D computes R_0 = g^s_0 mod N and publishes R_0. 

**6. D computes**

x_i = R_i mod N, i = 1, 2, · · · , N values for each participant. 

All participants choose a secret shadow, s_i and compute R_i value using own secret shadows as in step 3. The dealer assigns x values to each participant using R_i values in step 6. A participant can calculate x value assigned by the dealer, using own secret shadow and publicly known value R_0, x_i = R_i mod N during the reconstruction procedure. Therefore, the algorithm may use insecure channels between the dealer and participants since x values are calculated separately by both parties and never transmitted over the channel. Dealer also guarantees to generate unique shares by using unique secret shadows for all participants as in step 4. Therefore, the initialization phase ensures 

- unique shares by using unique x values, 
- x values are calculated independently by both the dealer and participants before the sharing procedure. Thus an insecure channel between the dealer and participants is sufficient, 
- even if one gathers any k shares from the network, one can not recover the secret image unless corresponding x values for those shares are known. 

3.1.2. **Sharing phase**

Medical image and EPR of the patient are shared among participants in this phase. Natural looking shares assure the confidentiality of both medical image and EPR. The method has also built-in authentication ability since the medical image and EPR cannot be revealed even if any one of k shares is modified. Previous research reported in the literature deal with any one of these desired capabilities: confidentiality, integrity or EPR hiding whereas the proposed method satisfies all of these requirements using a secret sharing scheme. 

Medical image M of size W × H pixel and depth b-bit to represent 2^b shades of gray is assumed, M = \{m_i | m_i ∈ [0 – (2^b − 1)], i = 1, 2, · · · , W × H\}. All pixel values are transformed into base 251 notation since modulus p in the polynomial is set to 251. Medical image is processed one pixel at a time by the sharing algorithm. Let the value of current pixel in a medical image M be m_i and EPR of the patient be E = \{e_i | e_i ∈ [0, 251], i = 1, 2, · · · , L\}. It is assumed that EPR is a string of text (or bytes) of length L. Each element in EPR is an ASCII character. 

Each pixel of the medical image corresponds to one pixel in share images which results in same share size with the medical image. The (k − 1)-degree polynomial in (4) is used to compute shared pixel values for medical image pixels m_i. Each pixel of the medical image is converted into base 251 notation. 

\[ (m_1, m_2, · · · , m_i, \log_{251}(e_i)) \]

denote a pixel m_i of the medical image with b-bit depth. Two or more coefficients of the Shamir’s polynomial represent medical image pixel m_i according to bit depth of the medical image. At least two coefficients of the polynomial are sufficient to represent either an 8-bit, 10-bit or 12-bit depth medical pixel. The number of coefficients required to represent a medical image of b-bit depth is \( \log_{251}(2^b) \). In other words, medical image’s pixel depth also determines threshold value k of the proposed method since 

k > \( \log_{251}(2^b) \). 

Shamir’s polynomial is constructed as in (4) by the proposed method for a 12-bit depth medical image: 

\[ F(x) = (m_1 + m_2x + e_{i+1}x^2 + e_{i+2}x^3 + · · · + e_{i+k}x^{k−1}) \mod 251 \] 

(4)

A pixel from the medical image and EPR are used as the coefficients (m_1, m_2, e_i, e_{i+1}, · · · , e_{i+k}) of the polynomial. Since a 12-bit depth medical image is assumed, first two coefficients of the polynomial are sufficient to code current medical pixel value. The algorithm evaluates the polynomial to generate n pairs of (x_i, F(x_i)) where F(x_i) is the brightness value of corresponding pixel at ith share and x_i’s are unique integers for participants determined in the initialization phase of the partitioning procedure. Each participant also calculates his own x_i during the retrieving procedure. Thus, proposed method does not necessitate any secure transmission between the dealer and participants. 

All pixels of secret medical image as well as EPR byte stream are utilized to create the shares. In other words, shares carry both medical image and EPR. Share images look like random noise and thus draw attention of the malicious users. Confidentiality of the shares is realized by Steganography, which is used to embed shares into meaningful cover images as explained below. 

3.1.3. **Embedding phase**

Steganography is used to hide shares into natural looking cover images. The dealer should select n natural looking cover images of size 2W × 2H to hide a W × H secret image for a (k, n) secret sharing scheme. 

Share images are processed pixel by pixel during embedding. Let n share images be \( SH^1, SH^2, · · · , SH^n \). Pixel values for ith share
image are defined as
\[ SH^i = \{ sh^i_j | j = 1, 2, \cdots, W \times H, sh^i_j \in \{0, 255\} \} \] (5)

Let the cover image used to hide ith share image be \( C^i \). Share image pixel values are embedded into corresponding \( 2 \times 2 \) pixel groups called cover blocks in cover image. Therefore, two LSBs of each pixel in the corresponding cover block is used to hide the shared pixel with eight bits. The proposed method makes use of OPAP to diminish the distortion of the cover images (Chan and Cheng, 2004). Let corresponding cover block for jth pixel in ith cover image be \( C^i_j \). Let four pixels of the corresponding cover block be \((a, b, c, d)\) respectively. Proposed method hides \( sh^i_j \) into pixels \((a, b, c, d)\) respectively by using OPAP (Chan and Cheng, 2004). The method first splits \( sh^i_j \) into two-bit streams and then embeds each stream in corresponding pixels to generate modified cover pixels as \((a', b', c', d')\). Therefore, embedding error for pixels in a cover block \((\delta_a, \delta_b, \delta_c, \delta_d)\), is determined by (6):
\[ \delta_a = a' - a, \delta_b = b' - b, \delta_c = c' - c, \delta_d = d' - d \] (6)

Embedding error for pixel \( a \) can be further segmented into three intervals, such that
\[ 2^{2-1} < \delta_a < 2^2 \]
\[ -2^{2-1} < \delta_a < 2^{2-1} \]
\[ -2^2 < \delta_a < -2^{2-1} \] (7)

OPAP modifies \( a' \) to form the stego pixel \( a'' \) based on the three intervals as in (8):
\[ \begin{cases}
2^{2-1} < \delta_a < 2^2 \Rightarrow a'' = a' - 2^2 \\
2^2 < \delta_a < 2^{2-1} \Rightarrow a'' = a' + 2^2 \\
-2^{2-1} < \delta_a < -2^2 \Rightarrow a'' = a' - 2^2 \\
-2^2 < \delta_a < -2^{2-1} \Rightarrow a'' = a' + 2^2
\end{cases} \] (8)

The new value of \( a \) will be \( a'' \) by using OPAP. Other pixels in the cover block are also modified as in the above procedure. Each pixel in the ith share image is embedded into the corresponding cover block at the ith cover image resulting natural looking stego images. Participating clinicians get stego images that contain embedded share information. Shared medical image is recovered for further processing or teleconsultation if any. The mathematical background of QR is also used in this phase. The last phase of the partitioning procedure is used to provide share authentication. Dealer constructs certificates for all participants in Lin et al. (2009) in order to identify modified share images. MD5, a well-known hash function with 128-bit output, is employed to determine the alterations on the share images. Share images combined with corresponding x values are input to the hash function.

Protecting phase uses quadratic residues (QR) approach as in Lin et al. (2009). Selected prime value \( N \) in the initialization phase is also used in this phase. The mathematical background of QR is given in this section. A number \( a \) is a QR modulo \( n \) if it is congruent to a perfect square. If there is an integer \( x \) such that \( x^2 \equiv a \mod n \) then \( a \) is a QR modulo \( n \), otherwise \( a \) is a non-quadratic residue (NQR) modulo \( n \). Extending from the above definition, there are four cases for \( a \) since \( N \) is the product of two primes \( p \) and \( q \).

Case 1. \( a \) is a QR to both \( p \) and \( q \).
Case 2. \( a \) is a QR to \( p \), but \( a \) is an NQR to \( q \).
Case 3. \( a \) is an NQR to \( p \), but \( a \) is a QR to \( q \).
Case 4. \( a \) is an NQR to both \( p \) and \( q \).

Assume that QRp and NQRp denote a set of integers that are quadratic residues and non quadratic residues modulo \( p \) respectively. Four parameters \((a, \beta, \gamma, \delta)\) are used to make a number QR both \( p \) and \( q \) can be defined as the following (11):
\[ \begin{align*}
\alpha &\in \text{QRp} \cap \text{QRq} \\
\beta &\in \text{QRp} \cap \text{NQRq} \\
\gamma &\in \text{NQRp} \cap \text{QRq} \\
\delta &\in \text{NQRp} \cap \text{NQRq}
\end{align*} \] (11)

A number \( a \) must be a QR to both \( p \) and \( q \) by multiplying corresponding parameter \( (\alpha, \beta, \gamma, \delta) \). If \( a \) is QR to both \( p \) and \( q \), it is also QR to \( N \). Steps of the protecting phase can be given as the following.

1. Dealer generates four modifiers \((\alpha, \beta, \gamma, \delta)\).
2. Dealer computes \( s_h = H(STk || x_k) \) where \( k = 1, 2, \cdots, n \) and \( H(\cdot) \) is MD5 hash function with 128-bit output.
(3) Dealer computes $h'_k$ as in (12):

$$h'_k = \begin{cases} h_k \times \alpha, id_k = 1 \\ h_k \times \beta, id_k = 2 \\ h_k \times \gamma, id_k = 3 \\ h_k \times \delta, id_k = 4 \end{cases} \quad \forall h_k \in QRp \cap QRq \quad \forall h_k \in NQRp \cap QRq$$

(4) Dealer constructs certificate, $Cert_k = \left( \left( (h'_k)^{1/2} \mod N \right) \| id_k \| b \right)$ where $b$ denotes the bit depth of the medical image.

Certificate for each participant contain summary information about his share image and corresponding x value. Thus, participants can detect any alteration performed on share image by using his certificate during the retrieving procedure. Our method uses protection mechanism proposed by Lin et al. (2009). Other methods in secret image sharing use block based authentication mechanism. Each block on the share images contains authentication bits and must be authenticated during the retrieving procedure. Such an authentication mechanism raises time complexity problem for medical images with higher resolution. The proposed method realizes authentication overall image using certificates.

3.2. Retrieving procedure

Retrieving procedure consists of two sub phases: verification and reconstruction. First phase is used to authenticate the share images. Certificates gathered by participants are used to test the integrity of the shares. The retrieving procedure is canceled if a modification on a share image is detected by the verification phase. Otherwise, reconstruction phase reveals the medical image and EPR. The details of these phases are explained below.

3.2.1. Verification phase

Participants can verify stego images for integrity using their own certificates. Certificate contains summary information about the secret image and corresponding x value. Reconstruction phase starts upon verification of all k stego images. Verification phase applied by the retrieving procedure is given below:

1. Extract $id_k$ and $b$ from certificate.
2. Determine $\lambda_k$ from $(\alpha^{-1}, \beta^{-1}, \gamma^{-1}, \delta^{-1})$ according to $id_k$.
3. Compute $h'_k = ((h'_k)^{1/2} \mod N)$.
4. Compute $h_k = h'_k \times \lambda_k \mod N$.
5. Compute $H(ST_k \| x_k)$ and compare with $h_k$. Stego image is authenticated if they are the same and assumed modified otherwise.

Verification phase performs share authentication using certificates before the reconstruction phase. Reconstructed secret image would have some erroneous pixels if such an authentication mechanism were not used in the proposed method. Even though erroneous pixels on the reconstructed secret image cannot be perceived by the human visual system, it may interfere the diagnosis. Using a formal method for share authentication overcomes such problems.

3.2.2. Reconstruction phase

Participating clinicians gather their stego images in the reconstruction phase to reconstruct the medical image. Any k of them will be sufficient to reconstruct the medical image. Since $x, F(x)$ pairs are embedded into 4 pixel blocks in stego images, corresponding stego blocks from k stego images denote $[((x_1, F(x_1)), (x_2, F(x_2)), \ldots, (x_k, F(x_k)))$ pairs. These pairs are used by Lagrange’s technique to interpolate the stego block. Coefficients of the polynomial determine secret medical image pixel value and EPR. The details of the algorithm are explained below.

Participants should compute their $x_i$ value once at the beginning of the algorithm before dividing the stego images into stego blocks. Parameters determined in the initialization phase by both participants and the dealer are used to compute $x_i$ value of each participant. $R_k$ that is broadcasted by the dealer and randomly chosen $s_i$ by the participants during the initialization phase are used to compute $x_i$ values. Each participant computes his/her own $x_i$ as in (13):

$$x_i = R'_i \mod N$$

Value of $x_i$ will be used in the Lagrange’s interpolation to recover the secret medical image pixel values. After this step, each stego image is divided into sets of four pixel blocks called stego blocks to be used to retrieve hidden shared pixels, $F(x_1), F(x_2), \ldots, F(x_k)$.

Assume that k stego image denoted by $(ST_1, ST_2, \ldots, ST_k)$ are used to reconstruct the medical image. Corresponding stego blocks from k stego images are used to retrieve the relative secret pixel in the reconstructed secret medical image. A stego block in ith stego image is shown in Fig. 3. Let four pixel values in ith stego block denoted by $(a^i, b^i, c^i, d^i)$. Pixel values are used to determine $F(x_i)$ value that has been embedded in this stego block during the embedding procedure using OPAP by the dealer. (14) is used to extract the $F(x_i)$ value from the current stego block:

$$F(x_i) = (a^i \mod 4) \cdot 64 + (b^i \mod 4) \cdot 16 + (c^i \mod 4) \cdot 4 + (d^i \mod 4)$$

Other stego blocks from the remaining stego images are also used in the same manner to extract corresponding $F(x_1), F(x_2), \ldots, F(x_k)$ values. Values of corresponding $x_i$ s have also been computed from (13). Then, Lagrange’s interpolation formula is used to interpolate coefficients of the polynomial from $((x_1, F(x_1)), (x_2, F(x_2)), \ldots, (x_k, F(x_k)))$ pairs obtained from stego blocks.

Let first $y = \left[ \log_{2512} (2^9) \right]$ terms of the interpolated polynomial be $s_1, \ldots, s_y$. Corresponding secret pixel value, $m_i$, is calculated as in (15) using the coefficients of the polynomial:

$$m_i = (s_1 \cdot 251^{y-1} + s_2 \cdot 251^{y-2} + \ldots + s_y)$$

Participants extract the value of $b$ from the certificate during verification phase. The rest of the coefficients of the polynomial are utilized to encode consecutive EPR characters. Each coefficient of the interpolated polynomial corresponds to an ASCII character code.

The revealing procedure is repeated until all stego blocks from k stego images are processed. Steps mentioned above are applied to all corresponding cover blocks from k stego images. Both medical image and related EPR is recovered from k stego images of participating clinicians at the end of the reconstruction phase.

Lagrange’s interpolation cannot be used to interpolate correct coefficients of the polynomial unless all stego blocks of the k shares are authentic and not modified in any way during transmission on the Internet or storage. Thus, it is easy for clinicians to perceive any alteration performed on the stego images.

4. Discussion and experimental results

Results of the tests performed to demonstrate the feasibility of the proposed scheme are reported in this section. The method out-
OPAP is used to limit the modification of the cover images (Chang and Cheng, 2004). Each pixel of a share is embedded into a block of size $2 \times 2$ in the corresponding cover image. Therefore, cover images must be $2N \times 2M$ for medical images of size $N \times M$. Eight bit gray level, $512 \times 512$ ‘window’, ‘house’, ‘lighthouse’ and ‘parrots’ are selected as natural looking cover images as given in Fig. 6.

Stego images are created by hiding the share images into cover images. The criterion for the visual quality of the stego images is the peak-to-signal-noise-ratio (PSNR) and is defined as

$$\text{PSNR} = 10 \log_{10} \left( \frac{2^b - 1}{\text{MSE}} \right)^2 \text{ dB} \tag{16}$$

where MSE is the mean squared error between cover and stego image. MSE is defined as

$$\text{MSE} = \frac{1}{4MN} \sum_{i=1}^{2M} \sum_{j=1}^{2N} (c_{ij} - s_{ij})^2 \tag{17}$$

where $c_{ij}$ and $s_{ij}$ denote the cover and stego pixel values, respectively. Fig. 7 shows the stego images with their PSNR values. Computed average PSNR for stego images is 46.3 dB approximately. Since, last two bits are used during the embedding procedure; each pixel of stego images holds two bits of shared information. Average PSNR of stego images drops to 44.1 dB approximately, if traditional LSB coding scheme is used which proves the effectiveness of OPAP in increasing the PSNR value. Stego images generated by the proposed method to distribute among four clinicians are given in Fig. 7.

Even though each has a share, none of the clinicians has all the information about the patient. Hu et al.’s method uses scrambling function to hide the medical image from the malicious eyes. Scrambling function generates noisy images. Transmission of noise like images may attract the attention of the malicious users. Proposed method uses Steganography to hide noise like shares into cover images and neither medical image nor EPR can be reconstructed even if any one of the stego images are slightly modified during transmission. On the other hand, even if $n-k$ shares become corrupt unintentionally, it is still possible to reconstruct the secret image and EPR. Hu et al.’s method does not consider EPR at all.

During the revealing procedure, proposed method uses Lagrange’s interpolation technique to recover both the medical image and EPR. Medical image and EPR of the patient are recovered by these factors. NOC for a medical image of size $N \times M$ is

$$\text{NOC} = \frac{(NM)}{k} \left( k - \lceil \log_{2512} 2^k \rceil \right) \tag{18}$$

where $NOC$ is the number of characters (NOC) an EPR can have is determined by these factors. NOC for a medical image of size $N \times M$ is

Since the experiment is performed for a $(3, 4)$ scheme and a 12-bit depth $256 \times 256$ MR image is considered, the proposed method
codes each 12-bit pixel of the image into first two coefficients of the Shamir’s polynomial. Other coefficient is used to code a single character of EPR since a second degree polynomial is used. In this regard NOC is computed to be 21,845 for a 12-bit medical image of size $256 \times 256$. Nayak et al.’s work proposed in 2009 suggests the reversible Steganography to embed the EPR into medical image. However, their scheme uses reversible Steganography to embed the EPR information into cover image (Nayak et al., 2009). The number of bits that can be embedded into medical image is equal to the number of pixels, which is associated with the peak point. Number of pixels that can be used to embed the EPR is 116,081. In other words, Nayak et al.’s method can hide a maximum 14,510 bytes into the same size medical image. The proposed method can hide longer EPR strings compared to Nayak et al.’s method. Lou et al.’s method uses multiple layer data hiding to embed the EPR with Steganography. Their embedding capacity for the first layer is approximately 14,863 bytes (Lou et al., 2009). Proposed method has higher embedding capacity compared with other methods as depicted.

Wide varieties of formats concerning modality are used to represent medical images. A two-dimensional (2D) medical image has a size of $M \times N \times b$ bits consists of $M$ pixels in the height and $N$ pixels in the width (Castelli and Bergman, 2002). It can be used to display $2^b$ shades of gray. Table 1 lists the average image size in megabytes per examination generated by medical imaging technologies (Wong and Huang, 1997; Castelli and Bergman, 2002). A 12-bit image is represented by 2 bytes in memory. Modality of the medical image determines the size of an image and the number of consecutive images taken in one patient examination. One examination (about 40 image slices) of X-ray CT with uniform image slice size of $512 \times 512 \times 12$ bits is around 20 MB whereas a digital mammography image usually generates 32 MB of data. Another important property of medical images is the higher dimensionality, such as 3D or 4D (Rahman et al., 2004). In a typical examination, image acquisition device (CT or MRI machine) generates about 20–200 images corresponding to a series of cross-sectional slices through the patient’s body. Higher dimensional medical images are often reorganized as collections of these 2D slices, where the added dimensions may be thickness of slices, time line or the same body part imaged with different modalities (Robb, 1999). Effect of the bit depth and resolution on the run time is analyzed respectively below.

Bit depth of the medical image does not affect run time of the retrieving procedure. Bit depth determines the lower bound of the threshold value $k$ the dealer can choose as $k > \lceil \log_{2^{512}} 2^b \rceil$. However, bit depth affects the total number of characters that can be embedded into stego images as can be seen in (18). Medical images of 8, 10 and 12-bit depth require two coefficients of Shamir’s polynomial. The remaining $k - 2$ coefficients of the polynomial are used to code EPR characters. Likewise, 16-bit depth medical images require three coefficients of the polynomial and threshold value of $k$ must be greater than 3. Higher bit depth necessitates increased number of coefficients in Shamir’s polynomial. The remaining $k - 2$ coefficients of the polynomial are used to code EPR characters. Likewise, 16-bit depth medical images require three coefficients of the polynomial and threshold value of $k$ must be greater than 3. Higher bit depth necessitates increased number of coefficients in Shamir’s polynomial to code the secret pixel value (2 coefficients for 8, 10, or 12 and 3 for 16-bit images). As a result, fewer coefficients can be used to accommodate EPR as bit depth of the medical image is increased. A new metric, embedding capacity per pixel ($ecpp = NOC/NM = 1 - \left[ \frac{\log_{2^{512}} 2^b}{k} \right]$), is derived from (18) to show the effect of the bit depth. For constant
Fig. 6. Used cover images with the size of 512 × 512 during the experiments.

$k$, embedding capacity per pixel decreases as the bit depth of image is increased. For example, $ecpp$ is $1 - (2/k)$ for 8, 10 or 12 bit medical images whereas it is reduced to $1 - (3/k)$ for 16 bit medical images.

The effect of image resolution on the run time are also tested on different medical imaging modalities; a 12-bit $256 \times 256$ MR image, a 12-bit $512 \times 512$ Computerized Tomography (CT) image, a 12-bit $1024 \times 1024$ Fluoroscopy image, a 12-bit $2048 \times 2048$ Computerized Radiography (CR) and a 12-bit $4096 \times 4096$ Mammography image. Test images are downloaded from the Internet and represent a good collection of different modalities as can be seen in Fig. 9 (Barre, 1999; Heath et al., 2001). The run time of all resolutions is plotted for distinct $k$ values ($k = \{2, 3, 4\}$) as in Fig. 10 and a linear proportional characteristic is visible from the graph. Experiments indicate that run time of the retrieving procedure is approximately proportional to image resolution. 12 bit high dynamic range medical images are used (in Fig. 9) since bit depth has no effect on the run time as explained above.

Increased run time is observed for larger values of $k$ for the same image since the number of coefficients to be solved by the Lagrange’s interpolation formula is dependent on $k$. For example, the retrieving procedure run for about 45.6 s for 12 bit $2048 \times 2048$ pixel CR image and a threshold value $k = 3$ and about 36.8 s for $k = 2$ for the same image as illustrated in Fig. 10.

Testing the authentication capability of the proposed method is the last experiment in this section. Watermarking medical images is generally preferred in the literature to guarantee the remote handling security. It allows permanent association of image content with proofs of its reliability by modifying the image pixel

<table>
<thead>
<tr>
<th>Modality</th>
<th>Image dimension (pixels)</th>
<th>Gray level (bits)</th>
<th>Avg. size/exam (Mbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nuclear medicine (PET, SPECT)</td>
<td>$128 \times 128$</td>
<td>12</td>
<td>1–2</td>
</tr>
<tr>
<td>Magnetic resonance imaging</td>
<td>$256 \times 256$</td>
<td>12</td>
<td>8–20</td>
</tr>
<tr>
<td>Ultrasound</td>
<td>$512 \times 512$</td>
<td>8</td>
<td>5–10</td>
</tr>
<tr>
<td>Computed Tomography</td>
<td>$512 \times 512$</td>
<td>12</td>
<td>20–40</td>
</tr>
<tr>
<td>Spiral or helical CT</td>
<td>$512 \times 512$</td>
<td>12</td>
<td>80–160</td>
</tr>
<tr>
<td>Digitized electronic microscopy</td>
<td>$512 \times 512$</td>
<td>8</td>
<td>Varies</td>
</tr>
<tr>
<td>Digitized color microscopy</td>
<td>$512 \times 512$</td>
<td>24</td>
<td>Varies</td>
</tr>
<tr>
<td>Digital subtraction angiography (per run)</td>
<td>$512 \times 512$ or $1024 \times 1024$</td>
<td>8</td>
<td>100–500</td>
</tr>
<tr>
<td>Digitized X-rays</td>
<td>$2048 \times 2048$</td>
<td>12</td>
<td>8</td>
</tr>
<tr>
<td>Computed radiography</td>
<td>$2048 \times 2048$</td>
<td>12</td>
<td>8</td>
</tr>
<tr>
<td>Digitized mammography</td>
<td>$4096 \times 4096$</td>
<td>12</td>
<td>128 (4 images)</td>
</tr>
</tbody>
</table>
values. Ho et al. (2004) used fragile watermarks for authentication purposes in 2005. Fragile watermarking ensures content authentication of medical images. However, their method generates medical image whose PSNR value is approximately 40 dB with watermark information. That is to say, distortion on the medical image after revealing the watermark is consistent. Besides, their work does not consider EPR. The transmission of medical images over the Internet after embedding procedure risks the confidentiality of the medical image. The proposed method ensures the authentication of the biomedical images with two factors. Nature

Fig. 7. Obtained stego images from embedding procedure with PSNR values.

Fig. 8. (a) Reconstructed secret image with no distortion. (b) Extracted EPR information.
Fig. 9. Medical images with different modalities (a) $256 \times 256$ MR image with 12 bit; (b) $512 \times 512$ CT image with 12 bit; (c) $1024 \times 1024$ Fluoroscopy image with 12 bit; (d) $2048 \times 2048$ CR image with 12 bit; (e) $4096 \times 4096$ Mammography image with 12 bit.
of the Shamir’s approach (Shamir, 1979) and certificates that contain summary information about the stego images are the factors that provide authentication ability to the proposed method.

First factor ensures that Lagrange’s interpolation formula yields incorrect coefficients and causes the participants to perceive the distortion if any share is modified. This property can be used to authenticate the shares. Fig. 11(a) and (b) shows a partially modified share and corresponding reconstructed image where modified areas are easy to identify. Noisy regions of the reconstructed image designate areas modified (or corrupted) during its transmission over the Internet. Proposed method does not need to embed a fragile watermark into medical images to ensure the authentication ability.

Second factor is the use of certificates to ensure the stego image’s integrity. In the verification phase, each participant computes a hash value with own stego image and $x_k$. Dealer has also calculated summary information about this stego image with related $x_k$ using same hash function and embedded it into corresponding certificate during the protecting phase. Therefore, stego images are assumed authentic if the hash value computed by the participant is equal to the value extracted from the certificate. The dealer uses $x_k$ values with corresponding stego images during the protecting phase. Value of $x_k$ is known only by the dealer and related participant. One cannot construct a fake stego block with a fake certificate since he/she does not know related $x_k$ value.

5. Conclusion

This paper presents a method that provides medical image sharing among clinicians based on Shamir’s secret sharing scheme. The method prevents unintentional disclosure of medical information to those who are not allowed to access it. $N$ clinicians share medical image and corresponding EPR information. Each clinician gets a natural looking stego image. Medical image and EPR can be recovered if any $k$ of $n$ gather, Thus before consultation, none of them has information about the patient whose medical condition might be important on the government policy.

Besides, the proposed method provides EPR hiding, confidentiality and authenticity together. Research reported by others in the literature generally deal with one of them. Polynomial coefficients used in Shamir’s secret sharing scheme provide us to hide the EPR information and medical image together. Embedding capacity for EPR record is higher than other methods in the literature. On the other hand, reconstructed medical image has no distortion. Share images transmitted over the Internet looks like natural image by using Steganography. Furthermore, it employs OPAP to improve
the PSNR of shares. Reconstructed image contains removed regions that correspond to modified regions if any of the shares is corrupted during the transmission. Therefore, our method ensures the authenticity of the medical image.

A medical image sharing scheme to provide privacy, confidentiality and authenticity, overlooked by many, is proposed in this paper. The proposed method emphasizes and provides three desired capabilities together: confidentiality, authenticity and EPR hiding.

Acknowledgements

This research was supported by the Research Fund of Karadeniz Technical University (Project No. 2008.112.009.1). The authors would like to thank the reviewers for their valuable comments.

References


