

# EPR Hidden Medical Image Secret Sharing using DNA Cryptography

L.Jani Anbarasi <sup>#1</sup>, Dr.G.S.Anandha Mala <sup>\*2</sup>,

<sup>#</sup>Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, India.

<sup>1</sup>jani\_lj\_2000@yahoo.com

<sup>\*</sup>Professor & Head, Department of CSE, St. Joseph's College of Engineering, Chennai, India.

<sup>2</sup>gs.anandhamala@gmail.com

**Abstract**—Security of medical images is an important issue, since applications such as Tele diagnosis exchange information over insecure communication channels. In this paper, Shamir secret sharing algorithm combined with DNA cryptography is proposed. The method involves the dispersion of medical image and Electronic Patient Record (EPR) into shadow images, aiming at better security characteristics. The EPR is hidden into the medical image using DNA hiding techniques. Huffman encoding is used to compress the DNA encoded secret image, which is then securely shared into shadow images using Shamir secret sharing. Then, the shadows are embedded into a host image using steganographic technique with modular operation. During reconstruction, at least t shadows are pooled to reconstruct the compressed secret image, which is again decoded using Huffman decoding to reveal the DNA encoded secret image. The medical image and EPR are separated using the reverse technique of DNA hiding. The simulation results and the security analysis prove that this method can hide longer EPR strings along with better confidentiality and authenticity. Better PSNR is achieved and the correlation coefficient shows that this also has the ability of resisting various attacks.

**Keyword**- Threshold Secret Sharing, DNA Cryptography, Huffman Encoding Steganographic, Image Processing

## I. INTRODUCTION

Storing medical images and text files on computers have given way for high storage and retrieval. Complete information about a patient is available at one place rather than on distributed systems. Applications such as telemedicine and teleconsultation require information exchange over an insecure network. Protection of integrity and confidentiality of patients' records and medical images is a security issue. Medical images should not be modified while transmission in an unsecured public channel. In addition, these medical images and records are used as a legal document for legal trials, insurance claims and as well as educational material for medical research. Security of medical images enhanced with integrity, confidentiality and authentication has become a research area.[27][30][32].

Researchers have proposed both fragile and robust watermarking techniques to hide the Electronic Patient Records (EPR) into the medical images, which satisfy both confidentiality and integrity. Thien et al.,[26] Shih and Ta Wu (2005)[24] proposed a fragile watermark technique based on genetic algorithm in which the non – Region of Interest (ROI) part of the medical image is embedded with the signature image and the fragile watermark. Zhou *et al.* (2001)[34] used the LSB technique to embed the signature and the EPR into the medical image. Woo *et al.* (2005)[31] method consists of two parts: annotation part and the fragile part. In the annotation part the encrypted EPR is embedded and the fragile part is used to identify the tampering of data. Chao *et al.* (2002)[8] hides a variety of EPR in to a mark image. Hidden data are separated by the authorized users. Luo *et al.* (2003)[18] proposed a method of hiding with high embedding rate and the original image can be recovered without loss. Hash value of ROI part of the medical image was embedded along with EPR into a non-ROI part of the medical image by Cheng *et al.* (2005)[9], which provides integrity of medical images. Wavelet-based multiple watermarking was proposed by Giakoumaki *et al.* (2003)[13], whereas EPR was watermarked during compression by Acharya *et al.* (2004)[2], which reduced the storage level. Viswanathan (2009)[28] proposed a binary embedding, which recovers both the EPR and the medical image without loss.

Osamah *et al.* (2010)[22] proposed a technique by dividing the image into three regions, ROI, Region of Non-Interest (RONI), and the border. A two dimensional Difference Expression (DE) is adapted, which can hide an EPR, authenticate ROI, and recover the tampered areas. This scheme can recover the medical image without loss. Coatrieux *et al.* (2006)[10] proposed a watermarking technique, which enabled a security layer providing a better authentication. Acharya *et al.* (2003)[1] used graphical signals EPR watermarking for interleaving with medical image. Error correcting codes were used to enhance the security during transmission and storage.

Coatrieux *et al.* (2008)[11] proposed a technique, which verifies the information whether it belongs to the correct patient and are issued from the right source. C.G. Boncelet (2006)[5] proposed a technique to enable the integrity of the medical image by embedding digital signature or Message Authentication Code computed over

the medical image. Memon *et al.* (2009)[19] presented a method where Bose–Chaudhuri–Hocquengham (BCH) security is used to encrypt the data which is then embedded in non – ROI part of the medical image.

In recent years, researchers have used steganography to hide the EPR into medical images and cryptographic techniques were used to protect the confidentiality. Lou *et al.* (2009)[17] adapted a multiple layer hiding technique which utilizes reduced data hiding technique to embed the bits in the least significant bits. This is a lossless scheme, which reconstructs both the embedded EPR and the multiple secret. Hu and Han (2009)[14] used a pixel-based scrambling derived from chaos, which provides a good cryptographic strength. All the proposed research work shows that the security requirements are satisfied for medical images. But disclosing the information of patients to a single person is not encouraged, so Mustafa Ulutas *et al.*(2011)[20] proposed secret medical image sharing based on Shamir's secret sharing, which reduces storage requirements, and network bandwidth, and meets security requirements like confidentiality and authenticity.

Shamir (1979)[23] and Blakley (1979) [4]introduced a  $(t, n)$  threshold secret sharing scheme, which divides a data  $D$  into  $n$  pieces of shadows. The data  $D$  is reconstructed when  $t$  or more shadows are pooled together. Knowledge of  $t - 1$  piece of shadows reveals no information about the data.

Wang and Su (2006)[29] and Chang *et al.* (2008)[7] discussed problems like pixel expansion, contrast, and meaningless shadows in secret sharing. Since eavesdroppers will be attracted towards meaningless shadows, these shadows are embedded into a cover image, and stego images are generated using steganographic technique. The meaningful cover image avoids the suspicion of intruders.

Lin and Tsai (2004)[16] and Lin *et al.* (2010)[15] proposed a technique based on the Shamir model, where the shadows are embedded into a cover image to hide the secret. However, the reconstructed secret image has distortions, because of the truncation of gray pixels for values larger than 250. In medical and sensitive images, even small distortions are not accepted. To overcome these problems, two pixels are used to represent the gray values larger than 250.

Adleman (1994) [3]worked out the first experiment on DNA computing in 1994, and later some researchers found lots of good characteristics of DNA computing such as massive parallelism, huge storage and ultra-low power consumption. Xiao *et al.* (2006)[33] proposed a DNA cryptography as a new emerging cryptographic technique in which the DNA is used as an information carrier. Gehani *et al.* (2000)[12] proposed an image encryption scheme based on one-time pad cryptography using DNA strands. Celland *et al.* (1999)[6] proposed a novel encoding method, which is able to take the place of the traditional binary encoding. Nucleotides are used as a quaternary code, which encodes the secret message into a DNA sequence by expressing each letter by three nucleotides. For example, the letter A is denoted as a sequence CGA, and the letter B as CCA. H.J. Shiu *et al* (2010) [25]proposed various data hiding techniques with high security.

In this paper, medical image and the EPR are encoded using DNA encoding technique. The encoded EPR is hidden into the encoded medical image using DNA hiding technique. Huffman encoding is used to compress the resulting encoded image, which is securely shared into shadows and are distributed among various clinicians using  $(t, n)$  Shamir's secret sharing scheme. The size of the generated shadows is smaller than the secret medical image. Steganography is used to hide these shadows into a natural looking cover image in order to avoid suspicion of intruders. At least 't' clinicians must gather to reconstruct the secret medical image and the EPR. At least 't' clinician is an adequate security measure to reconstruct the medical image and the EPR to diagnose. The method also hides longer EPR string. Thus, a medical image secret sharing is proposed, which satisfies the security constraints.

The outline of the paper is as follows: some background information on Shamir's secret sharing scheme and DNA Hiding is given in Section 2. Section 3 describes the details of the proposed scheme used for securely sharing medical images along with the EPR. Section 4 shows the experimental results of the proposed method. The conclusions are given in Section 5.

## II. RELATED WORKS

### A. Shamir's Secret Sharing Scheme

Secret sharing was introduced by Shamir (1979). A  $(t, n)$  secret sharing scheme was used to distribute a secret 'S' among 'n' participants such that at least 't' participants could reconstruct the secret 'S', but less than 't' cannot obtain it. This scheme is said to be perfect only if participants less than 't' cannot recover the secret. Shamir's secret sharing approach used a secret 'S' and a prime number 'm' to generate a  $(t-1)^{\text{th}}$  degree polynomial, which is given below:

$$F(X) = S + C_1X^1 + \dots + C_{t-1}X^{t-1} \text{ mod } m \quad (1)$$

The Coefficients  $C_1, C_2 \dots C_{t-1}$  are random integers within the range  $[0, m-1]$ . The secret shadows are calculated from (1) as follows

$$Y_1 = F(K_1), Y_2 = F(K_2), \dots, Y_n = F(K_n)$$

where  $Y_i$  ( $1 \leq i \leq n$ ) represents the computed shadow value, calculated using the secret key of each participant  $K_i$  ( $1 \leq i \leq n$ ), and is securely issued to the participants by the dealer. At least 't' participants pool their shadows to reconstruct the secret and less than that cannot.

Lagrange interpolation technique uses the secret shadow and the participants' key to reconstruct the secret without loss is given as follows

$$h(x) = \sum_{i=1}^t Y_i \prod_{i=1, i \neq j}^t \frac{x - k_j}{k_i - k_j} \text{ mod } 2^8$$

**B. DNA Cryptography**

DNA computing is a form of computing, which uses DNA, biochemistry and molecular biology for performing computations instead of traditional silicon-based computer technology. A DNA sequence is composed of four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T complement each other, as G and C. In a binary system 0 and 1 are complementary; similarly, 00 and 11, 01 and 10 are also complementary pairs. The four bases can be expressed as 00, 01, 10, and 11. Thus, 24 kinds of coding schemes are possible, but only 8 kinds of coding schemes satisfy the complementary rule of Watson–Crick(1953).The encoding rules are given in Table 1. In the proposed scheme, the DNA coding is used to hide the EPR into the secret medical image. Each pixel of the secret image can be expressed as a DNA sequence of size 4. For example, if the pixel value is 183, the binary sequence is 10110111. By applying the DNA encoding Rule 6, the DNA sequence is obtained as AGTG.

TABLE 1  
DNA Coding Schemes

+	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

**C. DNA Hiding Using Insertion Method**

Different biological properties were used to hide data in DNA in an efficient and secured way. H. J. Shiu (2010) proposed DNA-based hiding techniques. Hiding a secret message  $M=01001100$  into a DNA sequence  $S=ACGGTTCCAATGC$  is as follows. Using DNA Rule 2, the sequence is converted into a binary sequence 0001101011101010000111001. A random seed  $k=3$  are chosen and the DNA sequence is divided in such a way that each segment has 3 bits: 000, 110, 101, 111, 010, 100, 001, 110, and 01. A random seed  $r=1$  is chosen such that one bit from 'M' is inserted at the beginning of every segments of 'S'. Use the inverse function of DNA coding rule 2 to generate a fake DNA sequence S' AATGCCCTGGTAACCGC. Thus, the secret message is hidden into a DNA sequence. During the reverse process, the sequence is divided into segments having  $r+k$  values from which the message and DNA sequence are extracted without loss.

**III. PROPOSED WORK**

The proposed secret sharing scheme is explained in this section. The overall architecture is divided into two sub-procedures: Secret sharing and Retrieving. The secret sharing procedure has three phases: DNA hiding and encoding, Shamir secret sharing, and embedding phase .A group of 't' or more clinicians can reconstruct the medical image and the EPR during the retrieving procedure. Lagrange interpolation technique is used to reconstruct followed by Huffman decoding and DNA recovery technique

**A. Secret Sharing Procedure**

Secret sharing is performed in three phases: Hiding of EPR into the medical image using DNA hiding technique followed by compression using Huffman encoding is performed in the first phase and partitioning into shadows using Shamir's model in the second phase. The generated shadows look like noisy images and may attract attention of intruders. The third phase makes use of steganography with modular operation to embed the meaningless shadow images into natural cover images. These meaningful shadows are distributed to 'n' clinicians. Each phase is explained in detail in this section.

**1) Data Hiding Phase:**

**Input:** Secret medical image S, random number seed k and r, secret EPR message M and the DNA coding rule.

**Output:** Compressed secret  $S''$ .

Step1: Code the secret  $S$  and the EPR  $M$  into binary sequence  $S_1$  and  $M_1$  respectively.

Step2: Sequentially divide the secret EPR  $M_1$  into segments with length  $r$  in order. Denote these segments as  $m_1, m_2, \dots, m_t$ . Pad the residual part of  $m_t$  having the length  $r$ .

Step3: Sequentially divide the secret medical image  $S_1$  into segments with length  $k$  in order. Denote these segments as  $s_1, s_2, \dots, s_t$ . Pad the residual part of  $s_t$  having the length  $k$ .

Step4: Insert each  $m_i, 1 \leq i \leq t$  of  $M_1$  before  $s_i$  of  $S_1$  to generate a new binary sequence  $S_2$ .

Step5: Transform the sequence  $S_2$  into a fake DNA sequence using DNA coding rule resulting in DNA encoded secret image  $S'$ .

Step6: Apply Huffman coding scheme on the DNA encoded secret image  $S'$  to obtain the compressed secret image  $S''$ .

2) *Secret Sharing Phase:* In this proposed work the image pixels are used as the coefficients of the Shamir polynomial instead of random numbers. All the calculations are performed in  $GF(2^8)$  in order to avoid loss of data.

Step1: Step1: In (1) substitute the pixels of the Compressed secret image  $S''$  as the coefficients of the polynomial.

$$F(X) = S_1'' + S_2''X^1 + \dots + S_{t-1}''X^{t-1} \text{ mod } 2^8 \quad (2)$$

Where  $S_1'' \dots S_{t-1}''$  are the pixel values used as the coefficients.

Step2: The secret keys  $I_i (1 \leq i \leq n)$  of each clinicians are substituted as value of  $X$  in (2) to generate distinct shadows.  $Y_i (1 \leq i \leq n)$  represents the computed shadow value.

$$Y_1 = F(I_1), Y_2 = F(I_2), \dots, Y_n = F(I_n)$$

3) *Embedding Phase:* To avoid the suspicion of intruders, most of the existing secret image sharing schemes uses a steganographic algorithm for embedding the shadow into a cover image. Since the shadows are calculated using a finite field  $GF(2^8)$  all the values of the secret image lie between  $(0 \leq S \leq 255)$ . Lin and Chan's scheme (2010) produced a camouflaged pixel using

$$Q_i = \left\lfloor \frac{O_i}{k} \right\rfloor \times k$$

$$q_i = Q_i + Y_i \quad (3)$$

where  $Q_i$  is the quantized value of the host image  $O_i$ ,  $q_i$  represents the  $i^{\text{th}}$  camouflaged pixel and  $Y_i$  is the shadow value. In order to increase the embedding capacity, the shadow value  $Y_i$  is convert to base 5 conversion, where  $Y_{ij} (j= 1, 2, \dots, 4)$  are the values of each generated shadow. For example, consider the pixel value  $Y_i$  as 255, and base 5 representation of 255 ie  $Y_{ij}$  is  $(2\ 0\ 1\ 0)_5$ . The maximum number of pixels required for hiding is 4. The host image chosen for embedding the shadow should have twice the size of the shadow. So, the embedding capacity is  $\lfloor m*n \rfloor / 4$ . The value of  $k$  used in the process is 10 as given in paper (2010).

Using the following equation (4) the stego images are generated.

$$V_{ij} = \left\lfloor \frac{O_{i+(j-1)}}{10} \right\rfloor \times 10 + Y_{ij} \quad j= 1, 2, \dots, 4 \quad (4)$$

where  $Y_{ij}$  is the value obtained by the base-5 representation. The generated stego images are distributed to clinicians by the dealer.

### B. Retrieving Procedure

This procedure consists of two sub-phases: Shadow Retrieval and Reconstruction phase, DNA decoding and recovery process. Atleast 't' clinicians pool their shadow images to reconstruct the medical image and the EPR. The details of these phases are explained below.

1) *Shadow Retrieval and Reconstruction Phase:* The dealer retrieves the shadows from the stego images pooled by the clinicians during the reconstruction phase. The following equation is used to retrieve the shadow pixel values,

$$Y_{ij} = V_{ij} \text{ mod } 5 \quad j= 1, 2, \dots, 4 \quad (5)$$

where each  $Y_{ij}$  is the value obtained by the base-5 representation. These  $Y_{ij}$  values are converted to decimal representation, which is reconstructed into the shadow pixel value  $Y_i$  without loss.

The pooled shadows  $Y_i$  ( $1 \leq i \leq t$ ) and the secret keys of each clinician are denoted as  $\{[I_1, Y_1], [I_2, Y_2] \dots [I_t, Y_t]\}$  pairs. Lagrange interpolation technique (6) uses these pairs to reconstruct the polynomial. Coefficients of the polynomial determine the compressed secret image  $S''$ .

$$h(X) = \sum_{i=1}^t Y_i \prod_{i=1, i \neq j}^t \frac{x - I_j}{I_i - I_j} \text{ mod } 2^8 \quad (6)$$

$$h(X) = S_1'' + S_2'' X^1 + \dots + S_{t-1}'' X^{t-1} \text{ mod } 2^8$$

## 2) DNA Recovery and Decoding phase:

**Input:** Compressed secret image  $S''$ , Random number  $k$  and  $r$ , DNA coding rule used during hiding process.

**Output:** Hidden secret EPR,  $M$ .

Step1: Apply Huffman decoding technique to the Compressed secret image  $S'$  to reveal the DNA encoded secret image  $S'$ .

Step2:  $S'$  is coded into a binary sequence  $B_1$ .

Step3: Divide  $B_1$  into  $p$  binary segments with length  $r+k$  in order. Denote these segments as  $b_1, b_2 \dots b_p$ .

Step4: For each segment of  $b_i$ ,  $1 \leq i \leq p$  of  $B_1$ , extract the first  $r$  bits called  $m_i$ .

Step5: For each segment of  $b_i$ ,  $1 \leq i \leq p$  of  $B_1$ , extract the last  $k$  bits called  $s_i$ .

Step6: Concatenate all  $s_i$ 's,  $1 \leq i \leq p$  to be  $B_2$ .

Step7: Concatenate all  $m_i$ 's,  $1 \leq i \leq p+1$  to be  $M_1$ .

Step8: Transform the sequence  $B_2$  and  $M_1$  using DNA coding rule resulting in the secret medical image  $S$  and the EPR  $M$ .

## IV. SIMULATION AND EXPERIMENTAL RESULTS

The proposed scheme is tested for various medical images. The algorithm is coded and tested in Matlab 7.6. The medical images considered are 8-bit depth gray level CT (Computerised tomography) image of size  $256 \times 256$  are shown in Figure 1. The corresponding EPR is given in Figure 2.

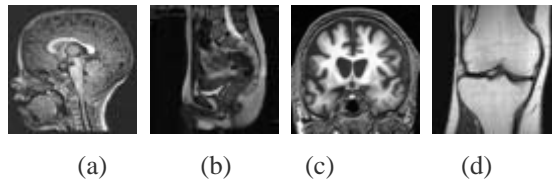


Figure 1: Secret Image

<b>GOOD HEALTH HOSPITAL</b>	
<u>Patient personal details</u>	
Patient Name	: Pranav
Date of Birth	: 23-09-1983
Patient Age	: 46
Patient Address	: Mount baton
<u>Patient Health details</u>	
Patient Weight	: 54Kg
Patient Height	: 173cm
Blood Group	: 0-ve
visual of eyes	: Normal
Blood Pressure	: Normal
HB content in Blood	:: Normal
Blood Sugar	: slightly increased
urine sugar	: Normal
Cause for Admission	: stomatiitics
Left Kidney	: Normal
right Kidney	: Normal
heart	: Normal
<u>Clinical Findings:</u>	
Everything normal, low blood HB content, Follow the doctor's advice.	

Figure 2: Corresponding Electronic Patient Record

The secret image shown in Figure 1(a) and the corresponding EPR information shown in Figure 2(a) are encoded using DNA coding rule 4. The encoded medical image and the encoded EPR are sequentially divided using the random seed  $k$  and  $r$ . Each segment of the encoded EPR is inserted before each segment of the encoded secret image. The resulting sequence is transformed using the DNA coding rule 6 resulting in DNA encoded secret image is shown in Figure 3. The size of the DNA encoded secret is twice that of the original secret. The size depends upon the number of EPR characters and the pixels present in the secret image. Since the size is greater than the original secret, Huffman encoding used to compress which results in smaller sized secret shown in Figure 4. The shadows generated result in smaller size images compared to the original secret.

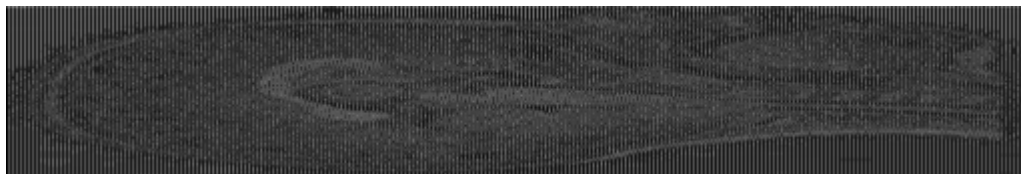


Figure 3: DNA Encoded Secret Image

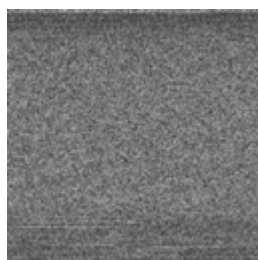


Figure 4: Compressed Secret Image (424x 424)

A (3, 4) threshold secret sharing scheme is performed on the images of Figure 4 and the corresponding shadows are shown in Figure 5. The generated shadows are embedded into the host images shown in Figure 6. Figure 7 shows the generated stego images. These meaningful shadows are distributed to four clinicians.

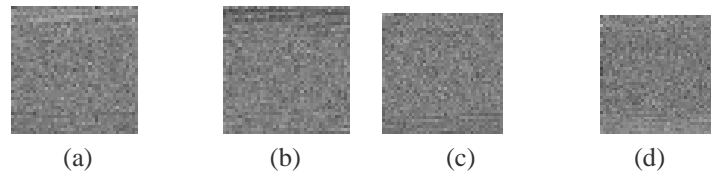


Figure 5: Generated Shadows (245x 245)

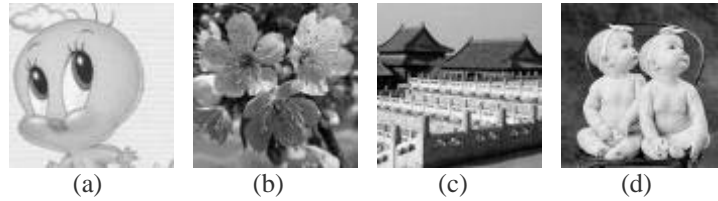


Figure 6: (a)-(d) Various host images (490x 490)

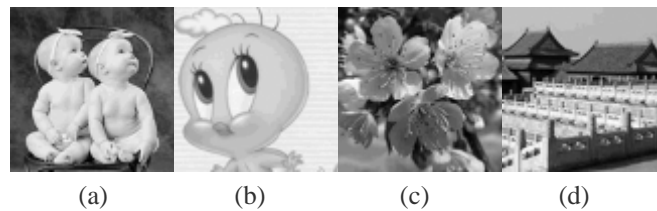


Figure 7: (a)-(d) Generated Shadows (490x 490)

The distortions in the stego image are computed, using the Peak to Signal Noise Ratio.

$$PSNR = 10 \times 10 \log \left[ \frac{255^2}{MSE} \right] dB \tag{7}$$

where MSE is the Mean Square Error between the original cover image and the stego image. For a cover image of size  $M \times N$ , the MSE is given below;

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (C_{ij} - S_{ij})^2 \tag{8}$$

$C_{ij}$  is the pixel value of the original cover image and  $S_{ij}$  is the pixel values of the stego image, respectively. A higher PSNR value means that the quality of the stego image is similar to that of the original cover image. A PSNR value of less than 35 dB denotes that some of the important signal characteristics are lost. A PSNR value less than 30 dB is an unacceptable quality. Good quality is implied by a PSNR value greater than 35 dB. The embedding of shadow was tested with various host images shown in Figure 6 and obtained PSNR value between 46.8 and 47. The result implies stego images of a better quality.

During reconstruction images from Figure 7(a), (b), (c) are pooled together in order to retrieve the medical image and the EPR as discussed in section 3.2. Retrieved EPR and the secret image are given Figure 8..Ulutas *et al.* (2011) determined that the number of EPR characters that are embedded using secret sharing depends upon threshold value, size of the image and bit depth of the image. So, the number of characters (NOC) is calculated using the following equation.

$$NOC = \frac{(NM)}{k} \times (k - \lceil \log_{251} 2^b \rceil) \tag{9}$$

**GOOD HEALTH HOSPITAL**

Patient personal details

Patient Name : Pranav  
 Date of Birth : 23-09-1983  
 Patient Age : 46  
 Patient Address : Mount baton

Patient Health details

Patient Weight : 54Kg  
 Patient Height : 173cm  
 Blood Group : 0-ve  
 visual of eyes : Normal  
 Blood Pressure : Normal  
 HB content in Blood :: Normal  
 Blood Sugar : slightly increased  
 urine sugar : Normal  
 Cause for Admission : stomatitits  
 Left Kidney : Normal  
 right Kidney : Normal  
 heart : Normal

Clinical Findings:

Everything normal, low blood HB content, Follow the doctor's advice.




Figure 8: (a) Secret Image

(b) Electronic Patient Record

So, the NOC computed by Ulutas for a 12-bit medical image of size 256 x 256 is 21,845. Whereas Nayak et al. (2009)[21] method can hide maximum of 14,510 bytes, similarly the embedding capacity of Lou et al. (2009) [17] scheme is approximately 14,863 bytes. Table 2 shows the embedding capacity of the proposed scheme for various sized images are higher than others in literature.

TABLE 2.  
Embedding capacity of EPR of different size

S. No	Image Size (MXN)	EPR size (in bytes)	Enlarged size after hiding	Share size after Huffman compression	Actual size of shares in %	Reduced size of shares in %
1.	32X32	32X32	32X64	22X22	69%	31%
		32X64	32X96	24X24	75%	25%
		32X96	32X128	27X27	84%	16%
		32X128	32X160	30X30	93%	7%
		32X160	32X192	32X32	100%	0%
2.	64X64	64X64	64X128	41X41	64%	36%
		64X128	64X192	47X47	73%	27%
		64X192	64X256	53X53	83%	17%
		64X256	64X320	58X58	91%	9%
		64X320	64X384	62X62	97%	3%
3.	128X128	128X128	128X256	81X81	63%	37%
		128X256	128X384	92X92	72%	28%
		128X384	128X512	105X105	82%	18%
		128X512	128X640	114X114	89%	11%
		128X640	128X768	123X123	96%	4%
4.	256X256	256X256	256X512	160X160	63%	37%
		256X512	256X768	182X182	71%	29%
		256X768	256X1024	209X209	82%	18%
		256X1024	256X1280	227X227	89%	11%
		256X1280	256X1536	244X244	95%	5%
5.	512X512	512X512	512X1024	318X318	62%	38%
		512X1024	512X1536	364X364	71%	29%
		512X1536	512X2048	416X416	81%	19%
		512X2048	512X2560	460X460	90%	10%
		512X2560	512X3072	503X503	98%	02%



## V. SECURITY ANALYSIS

### A. Correlation Analysis

To resist a statistical attack, less correlation among two adjacent pixels is very essential and critical. In this section, the correlation coefficient of two adjacent horizontal and diagonal pixels in the original image and encrypted image is examined. In order to test the correlation between two adjacent pixels, 3000 pairs (horizontal and vertical) of adjacent pixels were selected in a random manner from the original secret and encrypted images. Using the following formulae, the correlation coefficient is calculated which are given in Tables 3.

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (10)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (11)$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (12)$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad (13)$$

where x and y are the grey values of two adjacent pixels in the image, cov(x, y) is the covariance, D(x) is the variance, and E(x) is the mean. The result shows that the correlations of adjacent pixels in the encrypted image are greatly reduced, when using the DNA confusion.

TABLE 3  
Correlation analysis

Secrets Name	Secret		Share 1		Share 2		Share 3		Share 4	
	HC	VC	HC	VC	HC	VC	HC	VC	HC	VC
Medical1	0.9658	0.9696	0.0235	0.0226	0.0709	0.0010	0.0057	0.0081	0.0325	0.0213
Medical2	0.9418	0.9525	0.0135	0.0230	0.0751	0.0145	0.0766	0.0197	0.0561	0.0320
Medical3	0.9759	0.9811	0.0111	0.0201	0.0238	0.0215	0.0635	0.0132	0.0305	0.0309
Medical4	0.9734	0.9787	0.0612	0.0354	0.0510	0.0409	0.0486	0.0428	0.0367	0.0410
Medical5	0.9777	0.9881	0.0370	0.0989	0.0236	0.0617	0.0120	0.0530	0.0173	0.0920
Medical6	0.9715	0.9830	0.0584	0.0246	0.0471	0.0388	0.0156	0.0234	0.0268	0.0153
Medical7	0.9591	0.9776	0.0139	0.0274	0.0164	0.0300	0.0191	0.0116	0.0704	0.0245
Medical8	0.9373	0.9372	0.0942	0.0419	0.0825	0.0438	0.0199	0.0504	0.0804	0.0285
Medical9	0.8718	0.8844	0.0782	0.0316	0.0947	0.0292	0.0291	0.0314	0.0745	0.0250
Medical10	0.9884	0.9955	0.0520	0.0197	0.0097	0.0077	0.0015	0.0142	0.0268	0.0153
Medical11	0.9754	0.9870	0.0285	0.0348	0.0312	0.0067	0.0156	0.0254	0.0134	0.0147

### B. Information Entropy

Information entropy is defined to express the degree of uncertainties in the system. The same is used to express the uncertainties in the image information. Information entropy can measure the distribution of the grey value in the image; the results show that the greater the information entropy, the more uniform is the distribution of the grey value. Information entropy is defined as follows:

$$H(m) = -\sum_{i=1}^L P(m_i) \log_2 P(m_i) \quad (14)$$

where  $m_i$  is the  $i$ th grey value for the  $L$  level grey image,  $P(m_i)$  is the emergence probability of  $m_i$ , so,  $\sum_{i=0}^L P(m_i) = 1$ . For an ideally random image, the value of the information entropy is 8. An effective encryption algorithm should make the information entropy tend to 8. The information entropies of the encrypted shares are shown in Table 4, all of which are very close to 8. It can be seen that the proposed algorithm is very effective.

TABLE4  
Information Entropy of various shares

Secrets Name	Secret	Share 1	Share 2	Share 3	Share 4
Medical1	6.4691	7.9371	7.9380	7.9411	7.9373
Medical2	6.9618	7.9007	7.9030	7.9105	7.9018
Medical3	5.9680	7.9630	7.9643	7.9591	7.9588
Medical4	6.7178	7.9501	7.9508	7.9521	7.9539
Medical5	6.3921	7.9685	7.9876	7.9826	7.9876
Medical6	6.4137	7.9790	7.9555	7.9450	7.9794
Medical7	6.5072	7.9676	7.9734	7.9707	7.9689
Medical8	5.5344	7.9783	7.9888	7.9758	7.9999
Medical9	6.9369	7.9451	7.9424	7.9455	7.9464
Medical10	5.1719	7.9596	7.9567	7.9402	7.9588

## VI. CONCLUSION

This paper proposed a method that hides an EPR into a medical image using DNA cryptography which is then securely distributed among  $n$  clinicians based on Shamir secret sharing. This method avoids the disclosure of the information to those who are not supposed to access it. Embedding capacity for EPR is higher than various other methodologies in research. The secret medical image and the EPR are reconstructed without loss. Better PSNR is achieved which shows the pleasing nature of the host image. The proposed method provides EPR hiding along with confidentiality and authenticity

## REFERENCES

- [1] R.U.Acharya, P.S.Bhat, S.Kumar, and L.C.Min, "Transmission and storage of medical images with patient information," *Computers in Biology and Medicine*, vol.33, pp. 303–310,2003.
- [2] R.Acharya, U.C. Niranjan, S.S Iyengar, N.Kannathal, and L.C.Min, " Simultaneous storage of patient information with medical images in the frequency domain," *Computer Methods and Programs in Biomedicine*, vol.76, pp. 13–19,2004.
- [3] Adleman, "Molecular computation of solutions of combinational problems," *Science*, vol. 266, pp. 1021–1024,1994.
- [4] G.R.Blakley, " Safeguarding cryptography keys," in *Proc. AFIPS'79*, vol. 48, pp. 313–317.
- [5] C.G.Boncellet, " The NTMAC for authentication of noisy messages," *IEEE Trans. on Information Forensics and Security*, vol. 1, pp.320–323,2004.
- [6] C.T.Celland, V. Risca, and C. Bancroft, " Hiding messages in DNA microdots," *Nature*, vol. 399, pp.533-534,1994.
- [7] Chang, C.C.Hsieh, and C.P. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol.41, pp.3130-313,2008.
- [8] H.M.Chao, C.M.Hsu, and S.G.Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 6, pp. 46–53,2002.
- [9] S.Cheng, Q.Wu, and K.R. Castleman, " Non-ubiquitous digital watermarking for record indexing and integrity protection of medical images," in *Proc. ICIP*, vol. 2, p. 1062–1065.
- [10] C.G.Coatrieux, L.Roux, and B. Sankur, " A review of image watermarking applications in healthcare," in *Proc. IEEE Int. Conference on Engineering in Medicine and Biology*, vol. 1, pp. 4691–4694.
- [11] G.Coatrieux, C.Quantin, J.Montagner, M. Fassa, F.Allaert, and C.Roux, "Watermarking medical images with anonymous patient identification to verify authenticity," *Studies in Health Technology and Informatics*, vol. 136, pp. 667–672,2008.
- [12] A.Gehani, T.H. LaBean, and J.H.Reif, "DNA-based cryptography," *Dimacs Series in Discrete Mathematics and Theoretical Computer Science*, vol.54, pp.233-249,2000.
- [13] A.Giakoumaki, S.Pavlopoulos, and D.Koutsouris, "A medical image watermarking scheme based on wavelet transform," in *Proc. of 25th Annual Int. Conf. of the IEEE EMBS*. vol. 1, pp. 856–859,2003.
- [14] J.Hu, and F.Han, "A pixel based scrambling scheme for digital medical images protection," *Journal of Network and Computer Applications*, vol.32, pp.788–794, 2009.
- [15] P.Y.Lin, and C.S.Chan, "Invertible secret image sharing with steganography," *Pattern Recogn. Lett*, vol.31, pp. 1887–1893,2010.
- [16] C.C.Lin., and W.H. Tsai, "Secret Image sharing with steganography and authentication," *J.Syst. Software*, vol. 73, pp. 405-414, 2004.
- [17] D.C.Lou, M.C. Hu, and J.L.Liu, "Multiple layer data hiding scheme for medical images," *Computer Standards and Interfaces*, vol.31, pp.329–335,2009.
- [18] X.Luo, Q.Cheng, and J.Tan, "A lossless data embedding scheme for medical images in application of e-diagnosis," in *Procs of 25th Annual Int. Conf. of the IEEE EMB*., vol. 1, pp. 852–855,2003.
- [19] N.A.Memon, S.A.M. Gilani, and A. Ali, "Watermarking of chest CT scan medical images for content authentication," in *Proc. of International Conference on Information and Communication Technologie*., pp. 175–180,2009.
- [20] M. Ulutas, G. Ulutas, and V. V. Nabyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *The journal of System and Software*, vol.84, pp.341-353,2011.
- [21] J.Nayak, P.S.Bhat, U. Rajendra Acharya, and M. Sathish Kumar, "Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes," *Journal of Medical Systems*, vol. 33, pp.163–171,2009.
- [22] M.Osamah, Al-Qershi, and Bee Ee Khoo, "ROI-based tamper detection and recovery for medical images using reversible Watermarking Technique," in *Proc. of IEEE International Conference on Computer Research and Development*,2010.
- [23] A.Shamir, " How to share a secret?," in *Comm. ACM*, vol. 22 .pp. 612–613,1979.
- [24] F.Y.Shih, and Y.Ta Wu, "Robust watermarking and compression for medical images based on genetic algorithms," *Journal of Information Sciences*, vol.175 .pp. 200–216,2005.
- [25] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, and C.H Huang, "Data hiding methods based upon DNA sequences," *Information Sciences*, vol.180 , pp. 2196–2208,2010.

- [26] C.C.Thien, and J.C. Lin, " Secret image sharing," Computers & Graphics, vol.26,pp.765–770,2002.
- [27] V.Jagannathan, A.Mahadevan, Hariharan, and Srinivasan, "Number Theory Based Image compression Encryption and Application to Image Multiplexing," in IEEE - ICSCN, pp.59-64,2007.
- [28] P.Viswanathan, and P.Venkata Krishna, "Text fusion watermarking in Medical image with semi-reversible for secure transfer and authentication," in Proc. of International Conference on Advances in Recent Technologies in Communication and Computing IEEE, pp. 585-589,2009.
- [29] R.Z.Wang, " Secret image sharing with smaller shadow images," Pattern Recognition Letters, vol.27, pp.551-555,2006.
- [30] J.D.Watson, and F.H.C.Crick, "A structure for deoxyribose nucleic acid," Nature, vol.171 pp.737–738,1953.
- [31] C.S.Woo,J.Du, and B.Pham, "Multiple watermark method for privacy control and tamper detection in medical images," in Proc. of APRS Workshop on Digital Image Computing, pp. 59–64,2005.
- [32] H.C.Wu, and C.C.Chang, " Sharing visual multi-secrets using circle shares," Comput. Stand. Interfaces, vol.134, pp.123–135,2005.
- [33] G.Z.Xiao, M.X.Lu, L. Qin, and X.J. Lai, " New field of cryptography: DNA cryptography," Chinese Science Bulletin, vol.51 , pp.1413-1420,2006.
- [34] X.Q.Zhou, H.K. Huang, and S.L.Lou, " Authenticity and integrity of digital mammography images," IEEE Transaction on Medical Imaging, vol.20 , pp.784–791,2001.