A Reversible Crypto-Watermarking System for Secure Medical Image Transmission

Anna Babu
Computer Science & Engineering,
SCMS School of Engineering & Technology,
Ernakulam, Kerala, India
Email: annababu123@gmail.com

Sonal Ayyappan
Computer Science & Engineering,
SCMS School of Engineering & Technology,
Ernakulam, Kerala, India
Email: sonalayyappan@yahoo.com

***Abstract*—Health care institution demands exchange of medical images of number of patients to sought opinions from different experts. In order to reduce storage and secure transmission of the medical images, the paper presents a reversible crypto-watermarking technique. The system is based on stream cipher encryption of the image using a secret key and the secret key ciphering is done by public-private key crypto system- ELGamal. The secret key which is encrypted using ELGamal and is watermarked in Discrete Cosine Transform (DCT) domain using the spread spectrum coding algorithm. The Digital Watermarking is the process of embedding data to multimedia content. This can be done in spatial as well as frequency domain of the cover image to be transmitted. The robustness against attacks is ensured while embedding the encrypted secret key in transform domain. But if capacity is the major concern then spatial pixel manipulations based on prediction errors can be effective media for transferring the data. The experimental results reveals and analyzes the reversible crypto-watermarking method in terms of PSNR value, entropy requirements and histogram analysis.**

***Index Terms*—Stream cipher, crypto-watermarking, encryption, Discrete Cosine Transform, ELGamal.**

I. Introduction

Crypto-Watermarking is an evident area of research especially with the advent of medical related technologies. In applications related to telemedicine, medical images require security and confidentiality to be ensured as the opinions are sought based on the information provided by these images. Since the exchange of medical images between hospitals and also among different experts is common practice, the security and confidentiality of medical images is demanded. Crypto-watermarking helps in providing the appropriate informations embedded in the medical images without creating an opportunity to defame an institution by rightful delivery of medical images to intended owner. Digital watermarking is the process of embedding data into multimedia content. The data hiding can be done in two domains - spatial and frequency domain. The robustness against attack is possible when the embedding is done in frequency domain and if capacity is of major concern spatial domain can be of great help.

Privacy protection can be ensured with encryption and embedding the symmetric key in the encrypted domain. Encryption is the key for confidentiality and authentication of medical images transmitted. Encryption converts a data into unintelligible form. When a image with some secrecy need to be transmitted are encrypted, the provider unknown of the secret data tries to compress the encrypted image. With lossy compression method given by the authors of paper [13], an encrypted gray image can be efficiently be compressed by removing excessively fine and coarse coefficients information obtained from frequency domain transform. Irrespective of image format or size, watermarking is a technique that embeds the data into the cover signal imperceptibly [2].

This paper proposes a scheme for reversible crypto-watermarking for safe transfer of medical images. In proposed scheme, the original image is encrypted and the secret key is embedded into the encrypted image using the spread spectrum coding algorithm. The recipient on receiving the medical image extracts the secret key embedded and uses it to decrypt the cover image and finally gets to view the image information. Due to the security concerns the secret key is encrypted using public-private cryptosystem using ELGamal.

The reminder of the paper is sectioned as follows. Section II of the paper, we review the related works done in this area. The proposed mechanism is described in Section III in which a detailed explanation of the feature selection method been used is explained. Section IV of the paper discusses about the details of experiments and the results of the study. Finally, Section V presents the conclusion of the study.

II. Related Works

The method recognized by Zhenxing Qian, Xinpeng Zhang in [1] is one of the scheme of crypto-watermarking in which data hiding is done in encrypted images. The stream cipher technique for encryption followed by data hiding in which selected bits are taken from the encrypted image to embed the secret data.

Zhang et al. [21] had advised a scheme in which certain pixels are selected for estimating the errors and data hiding is done into these estimated errors. Standard stream cipher algorithm AES is used to encrypt the pixels of the image and special scheme is used to encrypt the estimation errors. The efficiency and feasibility of the scheme is computed by PSNR and embedding rate.

978-1-4673-6540-6/15/$31.00 ©2015 IEEE

Koushik Pal et al. [2] had embedded the patient record including patients name, diagnostic and region of interest into the cover image by the use of discrete cosine transform in frequency domain and RSA public-private key algorithm The infected region to be the ROI is detected through a amalgamation of contour detection algorithm and region growing. The embedded information is found to be obtained with exact similarity even from several attacked image.

The scheme described in [3] is based on the arrangement of encryption algorithms using secret keys and public-private keys including watermarking. The algorithm for image encryption is done using stream cipher technique with secret key encrypted with an asymmetric cipher technique. The watermarking algorithm is used to insert this encrypted secret key into the encrypted image.

The system explained by D.Bouslimi et al. [4] move towards a watermarking algorithm which is substitutive, with the quantization index modulation (QIM) applied and an encryption algorithm employed which was stream or block cipher technique or both. In Joint Watermarking/Encryption scheme watermark is embedded during the encryption process. It allows verifying the image reliability in both encrypted and spatial domains. Here encryption and data embedding is conducted together at the stage for protection, decryption and data extraction can be applied in parallel.

The Medical image watermarking preserves image quality that is mandatory for medical diagnosis and treatment. The authors of [6] highlights needs that are essential for medical image watermarking with a go over of developments since 2000 and simulated experiments to exhibit the significance of watermarking in management of medical information.

William Puesh et al. [8] described the system with encryption or data hiding algorithms, the protection of multimedia data. The transmission time can be reduced by the use of the data compression. This work, provide solutions to combine image encryption and compression. Application of reversible data hiding algorithms on encrypted images wish to remove the embedded information before the decryption of image. The use of bit substitution- data hiding method aids for this purpose. In order to remove the watermarked data during the decryption step, local standard deviation analysis of the watermarked encrypted images is done.

Sharing of medical image in applications such as remote diagnosis aid or e-learning values a lot,Thus Coatrieux et al. [9] proposes to make the image more usable while watermarking it with associated knowledge digest. Watermarking is used to push in the Knowledge Digest (KD) into the gray-scale pixel values of the related images. When it is shared through internet, watermarking helps to transmit reliability proofs of an image and its KD.

III. Proposed Methodology

The proposed method systematically does the encryption and watermarking of medical images efficiently with confidentiality assured. A medical image is selected for transmission in scenario of practioner and medical specialist. Before transmission following steps are done systematically. This constitutes encryption of image based on secret key using stream cipher method RC4. Then the encrypted image is watermarked using DCT watermarking after the key itself being encrypted using public-private crypto-system. The encrypted and watermarked image is finally transmitted. The proposed methodology is depicted in Fig. 1.

Encrypting images using asymmetric methods are not suitable because they are computationally complex. So a conventional symmetric key encryption, with channel to transfer the key is used [3]. The projected method combines a algorithm for symmetric image encryption, secret key encryption using asymmetric public-private scheme and spread spectrum coding algorithm in discrete cosine transform for watermarking. RSA being the traditional asymmetric method based on public-private keys and being probe to several security issues, the secret key is encrypted using ELGamal public-private cryptosystem. Suppose a Medical Practioner M wish to send an image securely to another specialist S. M will use a symmetric algorithm to encrypt the image. First, M generates his secret key to encrypt the image with it, then this secret key will be encrypted with a ELGamal public key to obtain an encrypted secret key k" which will be then inserted in the encrypted image using discrete cosine transform (DCT) based on spread spectrum technique to get at the end an encrypted watermarked image. Finally, M sends the image to S. S then receives the image, extracted the watermark (the encrypted secret key k") and decrypted it using his ELGamal private key, So he can decrypt the image that M send it to him and view it.

Basically, four steps are basically involved in the proposed crypto-watermarking technique.

1) Image encryption
2) Secret key encryption
3) Watermarking the encrypted key.
4) Transmission and reception of encrypted image.

After the reception of image the watermark extraction is done followed by decryption of key using the private key and image decryption is the final step to get the output.

A. Image Encryption

The utilization of internet for information transmissions has created the basic call for security. Several robust encryption techniques for plain messages have been developed to supply this demand. The encryption practice can be asymmetric, symmetric or hybrid. It can be functional to blocks or streams. The block encryption scheme applied to images, can meet with basically three inconveniences. The first and foremost one is when there is encryption of identical zones, they are found to be similar. The problem that is found next is that block encryption schemes are not vigorous to noise. The data integrity preservation is the third problem [8]. The combination of encryption and watermarking can solve these types of problems. The encryption function is based on following equation shown in 1. The encryption function can differ based on the algorithm used. The proposed work is done based on

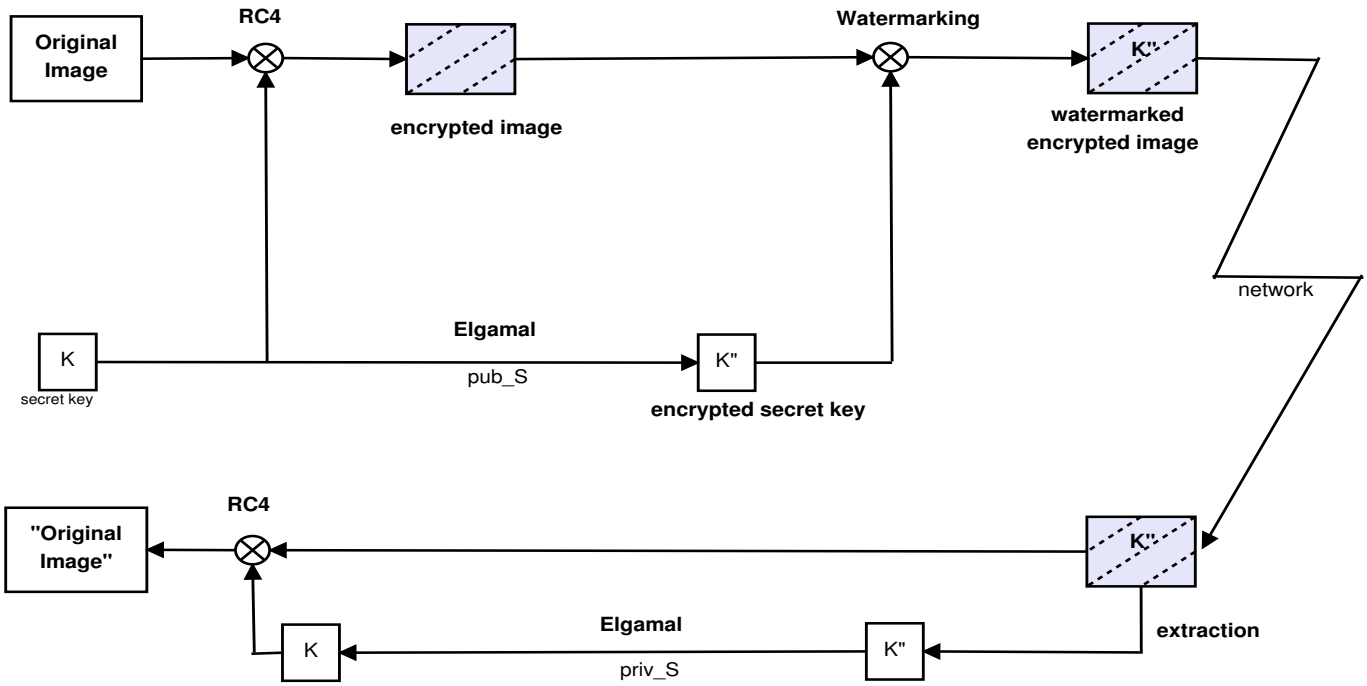

Fig. 1. Proposed Methodology

RC4 algorithm and the encryption of key is done based on public-private key algorithm- ELGamal.

$$Y = E_k(X) \tag{1}$$

where $E_k()$ is the function for encryption with k as the secret key and Y is the corresponding cipher-text to X. The RC4 stream cipher method used is explained in following section especially the key generation and XOR operation.

1) Stream Cipher - RC4: RC4 is a symmetric cipher designed for RSA Security in 1987 by Ron Rivest. The specificity of such stream cipher algorithm resides in how the bit/byte key stream is generated by the PRNG. The RC4 PRNG is based on two steps:- Initialization and byte key stream generation. This algorithm produces a stream of pseudo-random values. The input stream is XOR ed with these values. The encryption and decryption process is the same as the data stream is simply XOR ed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plain text message, it will produce the encrypted version [14].

The encryption key selected before the initialization step is 16 random values based on image pixels in the input image i.e. between 0 and 255. As the proposed work is done using python-opencv. This key is given as input to the encrypt function of python's RC4 module. The input image to be encrypted is taken as plain text and is appended to the list for encryption. The byte stream generation is accomplished by elements in the table combined by permutations and addition operation to generate the stream. In RC4 module each value of k is generated based on RC4 key stream generation algorithm and the entries in S box are once again permuted. Encryption is done by XORing the key value k with the bytes of plain text in the appended list of plain text image pixels. Decryption is done again by XORing the key value k cipher text rounding based on bytes.

B. Key Encryption

The secret key taken based on PRNG is the key to decrypt the medical image sent to the specialist so that he can view the image for diagnosis or further processing, so there is a great need to secure this key at the same time the key needs to be obtained by the specialist fast. The security is guaranteed through public-private key algorithm. In order to increase the security the proposed method use a strong algorithm known as ELGamal which increases the randomization involved in the cipher text also it is difficult against cryptanalysis. The Practioner M takes the public key of Specialist S and encrypts the secret key and embeds the encrypted secret key in image using either watermarking or steganography principles. The basics of ELGamal crypto-system is explained in detail in following subsection.

1) ELGamal Cryptosystem: An ELGamal crypto-system operates in a finite cyclic group [27] [26]. An ELGamal crypto-system can be described by a 4-tuple (p, g,x, y), where p is a large prime and describes which group Z_p^* is used, g is an element of order n in Z_p^*, x is a random integer with $1 \leq x \leq n-1$, and $y = g^x$. The steps in the ELGamal crypto-system are as follows:

1) **Key generation**: Pick a large prime p, generator g of Z_p^*, private key is a random x such that $1 \leq x \leq p-2$ and public key is 4 tuple (p, g, y = g^x mod p).

2) **Encryption**: Pick random k such that, $1 \leq k \leq p-2$ and encryption function is defined as

$$E(m) = (g^k \mod p, my^k \mod p) = (\gamma, \delta) \quad (2)$$

3) **Decryption**: Given cipher text (γ,δ), compute $\gamma^{-x} \mod p$ and recover m such that

$$m = \delta\gamma^{-x} \mod p \quad (3)$$

In the experiment the chosen key is variable length. If the 8 pixels are chosen randomly using a PRNG. It can be encrypted using ELGamal crypto-system using the public key of the specialist S say is 4 tuple (p, g, y = g^x mod p) and the encrypted key to be watermarked is obtained basically 2 ciphers which are joined and embedded in the encrypted image. The key chosen is 104101125130945616157 then this secret key is encrypted with public key of S.

C. Digital Watermarking

Watermarking is the process of embedding a signal into a multimedia content of text, image, audio or video types; and signal used as watermark can be of any format- text, image or audio signal. It can be viewed as a data hiding technique. In case of digital images, information embedded can be either invisible or visible from the user perspective. The watermarking is based on spatial and frequency domain [24]. The frequency domain being more robust to attacks, the work is done on Discrete Cosine Transform. The encrypted secret key is embedded in DCT domain using spread spectrum approach an traditional method discussed by [13] as the basic watermarking principle. The work can be categorized to the following methods based on watermarking done on the image:

- The insertion and extraction of watermark using DCT transform.
- Embedding of encrypted secret key using spread spectrum technique in this transform domain at middle frequency coefficients.
- Computing PSNR function (peak signal-to-noise ratio) of the watermarked image after the application of DCT.

1) Discrete Cosine Transform(DCT): The transformation of a signal from the pixel-intensity domain to the frequency domain is done using discrete cosine transform and vice versa, is done with inverse discrete cosine transform (IDCT). The information similarity is verified to be same in both domain [24]. The Discrete Cosine Transform (DCT) is widely deliberate due to the fact that watermarks embedded in the DCT domain are often more robust to JPEG and MPEG compression, but as in general both the DCT and DWT transforms have been extensively used in many digital signal processing applications [25].

The General Methodology:

The discrete cosine transform (DCT) is an orthogonal transform that can convert a image pixel levels into elementary frequency coefficients. For an input image, the DCT frequency components are computed using 4 shown below:

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}C_u C_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n) \; cos\frac{(2m+1)u\pi}{2M} cos\frac{(2n+1)v\pi}{2N} \quad (4)$$

In the equation, with size of N x M pixels, x(m, n) is the spatial intensity at corresponding position of the image, and y(u, v) is the DCT frequency coefficient at corresponding point of the DCT matrix.

The inverse DCT operation is done for watermarked image to restore the image to cover image extracting the watermark information applying the 5 shown below.

$$x(m,n) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}C_u C_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} y(u,v) \; cos\frac{(2m+1)u\pi}{2M} cos\frac{(2n+1)v\pi}{2N} \quad (5)$$

Low-frequencies sub band contains the important visual details of the image and high frequency coefficients of the image are easily eliminated through geometrical modification - basically compression. The watermark is embedded by altering the frequency elements of the middle frequency sub band so that the visual quality of the image will not be distorted and the watermark can not be removed by geometrical changes.

2) Spread Spectrum Watermarking: The proposed watermarking algorithm in the transform domain i.e. DCT domain is spread spectrum technique. First, the best place for insert the watermark bits is found by index sorting for getting the first n high frequency coefficients. The watermark is spread over to many bins accumulating frequency so that the energy in any bin is negligible and cannot be detected. The watermark should not be placed in regions of insignificance. Watermark is known as a signal trasmitted through the frequency domain of the image.

Watermark Insertion:

The robustness and security of watermark is ensured by, placing the watermark explicitly in the most significant coefficients of the image perceptually. In order to place watermark of length n into an NxN image, coefficients are computed for the NxN image using DCT and placing the watermark into magnitude coefficients with high values. Create a watermark where each value x_i is chosen independently according to N (0, 1). The extracted from host digital image, a sequence of values V_i , into which a watermark x_i is inserted to obtain an adjusted sequence of values W_i.

- Inserting and Extracting the Watermark: Watermark insertion results in watermarked image W, with a scaling parameter α used to specify, the extent to which watermark alters the cover image. Formula for computing watermarked signal is shown in 6. A large value of α will cause perceptual degradation in the watermarked image.

$$W_i = V_i + \alpha x_i \quad (6)$$

where V_i is DCT coefficient value of the image and α is scaling factor denotes the imperceptability degree. The extraction is reverse of the process of insertion including deviation analysis. For each watermarked cipher text Y_i, applying the decoding function for two possible values (0 or 1) while analyzing the local standard deviation. The bit value is selected where local standard deviation is least.

IV. Experimental Setup and Results

The reversible crypto-watermarking system has been implemented using OpenCV python on a Ubuntu 14.04 operating system and 4GB RAM. The performance of combined crypto-watermarking techniques: (i) RC4 image encryption (ii) DCT-Spread spectrum coding and (iii) key encryption using EL-Gamal cryptosystem; is tested and evaluated using the dataset described in next section.

A. Dataset

The method is applied on more than 30 gray level images. The proposed method being applied on a chest image (396 x 400 pixels) and the medical image (512 x 512 pixels) with its result illustrated in Figure 2 and is illustrated in Figure 3 is shown. Different sets of medical images are tested on proposed method [16] [17]. The watermark data is encrypted key data which is variable length ranging to up to 126bits. The results are evaluated using mean-square-error(MSE), peak-signal-to-noise-ratio (PSNR), entropy for encryption efficiency.

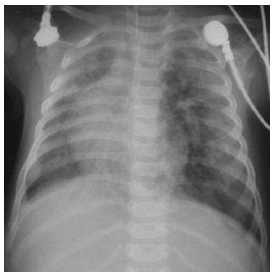

Fig. 2. Input Image 1

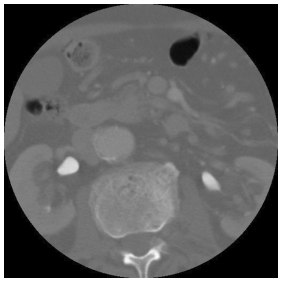

Fig. 3. Input Image 2

B. Evaluation

Stream cipher method is applied to encrypt the input image. The encryption of the original image Fig. 2 is done by using the RC4 algorithm to get the encrypted image illustrated in Fig. 4. In this encrypted image bits of encrypted key is embedded to get the watermarked encrypted image illustrated in Fig. 5. The pixels where the substituted one bit with the message. On reception of image by the specialist the watermark is extracted from the image which is embedded secret key k' and this secret key is used to decrypt the image to view the initial image. The watermark extracted image and corresponding decrypted image is shown in Fig. 6 and 7 respectively.

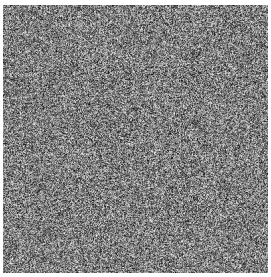

Fig. 4. Encrypted Image

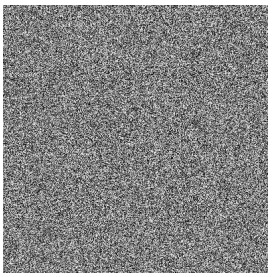

Fig. 5. Watermarked Image

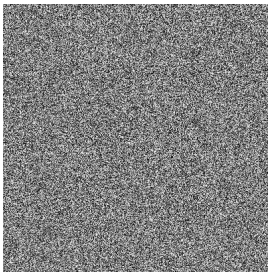

Fig. 6. Key Extracted Image

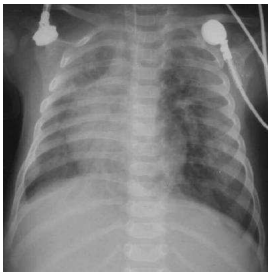

Fig. 7. Decrypted Image

C. Results

Inorder to interpret the results obtained, it is important to develop tools to measure the error between decrypted and original image. Among these methods histogram analysis,and the degree of imperceptability between two images are used based on histogram and PSNR values respectively. Entropy is other factor to understand the security and robustness involved in the encryption process for images. Entropy for encrypted image is near 7.9bits/pixel. Table I shows the entropy of input image and encrypted image respectively.

TABLE I
Entropy description for medical image and its encryption

IMAGE	ENTROPY(bits/pixel)
chest_image	7.21
encrypted_image	7.99

D. Histogram Analysis

A histogram is a graphical representation of a continuous variable distribution. So the difference difference can be noted clearly between the histogram of original image before encryption in Fig. 2 and the histogram of the image after encryption is shown in Fig. 4, where uniform distribution of pixels are done, which can resist attacks. So, efficiency of algorithm is ensured due to the security it guarantees with secure transmission of confidential information.

By the comparison of both histograms that of the initial image, and that of the image encrypted, with remark that the probabilities of occurance of gray levels in the image are equally distributed also shown respectively.

E. Quality Analysis

The proposed crypto-watermarking system is applied to chest image. Quality Metrics used is Peak Signal to Noise Ratio and to evaluate the similarity between the Decrypted image and original image. Bigger is PSNR, better is quality of image. PSNR for image with size M x N is given by 7:

$$PSNR = 10\log_{10}\left(\frac{\sum_{x=1}^{M}\sum_{y=1}^{N} E_{max}^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}(f(x,y) - f'(x,y))^2}\right) \quad (7)$$

Where, f(x, y) is pixel gray values of original image. f'(x, y) is pixel gray values of watermarked image. M and N are image pixel dimensions. PSNR value obtained for the decrypted image is infinity. These results show a great improvement in the performance of the combined Crypto-Watermarking technique when assigned with encryption.

V. Conclusion

The method combining encryption and watermarking is proposed and evaluated for safe transmission. Advantage of both encryption algorithm with secret key and public-private keys are used based on ELGamal. Being robust to moderate noise stream cipher algorithm is efficient with high quality factor. Spread Spectrum watermarking in DCT domain is used to embed the encrypted key due to its imperceptability and robustness to geometric distortions. Finally result is presented on medical images.

References

[1] Zhenxing Qian, Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image with Distributed Source Encoding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 39, no. 1, pp. 1-46, August 2015.

[2] Koushik Pal, Subhajit Koley, Goutam Ghosh, Mahua Bhattacharya, "A New Combined Crypto-Watermarking Technique using RSA Algorithm and Discrete Cosine Transform to Retrieve Embedded EPR from Noisy Bio-Medical Images", *IEEE 1st International Conference on Condition Assessment Techniques in Electrical Systems (CATCON)*, pp. 368-373, December 2013.

[3] LAKRISSI, Youssra, Mohammed ERRITALI, and Mohammed FAKIR, "A Joint Encryption/Watermarking Algorithm for Secure Image Transfer,"*International journal of Computer Networking and Communication (IJCNAC)*, vol. 1, no. 1, August 2013.

[4] Bouslimi, Dalel, Gouenou Coatrieux, Michel Cozic, and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, pp. 891 - 899 July 2012.

[5] Shahid, Zafar, Marc Chaumont, and William Puech, "Fast Protection of H.264/AVC by Selective Encryption of CAVLC and CABAC for I and P Frames", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 5, pp. 565 - 576, March 2011.

[6] Rao, N. V., and V. Meena Kumari, "Watermarking in Medical Imaging for Security and Authentication," *International Journal of Information Security* vol. 20, no. 3, pp. 148-155, May 2011.

[7] Luis Prez-Freire and Fernando Prez-Gonzlez, "Spread-Spectrum Watermarking Security", *IEEE Transactions on Information Forensics and Security* , vol. 4, no. 1, pp. 2 - 24, February 2009.

[8] W.Puesh and J.M.Rodrigues, "A Reversible Data Hiding Method for Encrypted Images", *Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents* 2008.

[9] Coatrieux, Gouenou, Clara Le Guillou, J-M. Cauvin, and Christian Roux , "Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images", *IEEE Transactions on Information Technology in Biomedicine*, vol.13, no.2, pp. 158 - 165, October 2008.

[10] W.Puesh and J.M.Rodrigues, "A New Crypto-Watermarking Method For Medical Images Safe Transfer", *12th Eurasip Signal Processing Conference,* pp. 1481-1484, June 2006.

[11] D. Stinson, "Cryptography - Theory and Practice", CRC Press, Boca Raton, Florida, USA, 1995.

[12] B. Schneier, "Applied cryptography", Wiley, New-York, USA, 1995.

[13] Cox, I. J., Kilian, J., Leighton, F. T. and Shamoon, T. "Secure spread spectrum watermarking for multimedia", *Image Processing, IEEE Transactions on,* vol. 6, no. 12, pp. 1673-1687, 1997

[14] William Stallings, "Cryptography and network security: Principles and practice", Prentice Hall, Upper Saddle River, New Jersey, 2003.

[15] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging,*in Proc. IEEE Int. Conf.*, ITAB, Arlington, VA, pp. 250255, 2000 .

[16] Candemir S, Jaeger S, Musco J, Xue Z, Karargyris A, Antani SK, Thoma GR, Palaniappan K., "Lung segmentation in chest radiographs using anatomical atlases with nonrigid registration.", *IEEE Trans Med Imaging.* vol. 33, no. 2, pp. 577 doi: 10.1109/TMI.2013.2290491, PMID: 24239990, Feb 2014

[17] Jaeger S, Karargyris A, Candemir S, Folio L, Siegelman J, Callaghan FM, Xue Z, Palaniappan K, Singh RK, Antani SK. "Automatic tuberculosis screening using chest radiographs.", *IEEE Trans Med Imaging.*, vol. 33, no. 2, pp. 233-45, doi: 10.1109/TMI.2013.2284099, PMID:24108713,Feb 2014

[18] Zhang, Xinpeng. "Reversible data hiding in encrypted image."Signal Processing Letters, IEEE18.4 (2011): 255-258.

[19] Acharya, Rajendra, et al. "Transmission and storage of medical images with patient information."Computers in Biology and Medicine33.4 (2003): 303-310.

[20] Khan, Asifullah, Ayesha Siddiqa, Summuyya Munib, and Sana Ambreen Malik. "A recent survey of reversible watermarking techniques."Information Sciences, 279 (2014): 251-272.

[21] Zhang, Weiming, Kede Ma, and Nenghai Yu. "Reversibility improved data hiding in encrypted images."Signal Processing94 (2014): 118-127.

[22] Fernndez-Alemn, Jos Luis, Inmaculada Carrin Seor, Pedro ngel Oliver Lozoya, and Ambrosio Toval. "Security and privacy in electronic health records: A systematic literature review."Journal of biomedical informatics46, no. 3 (2013): 541-562.

[23] Prez-Freire, Luis, Pedro Comesana, and Fernando Prez-Gonzlez, "Information-theoretic analysis of security in side-informed data hiding." In Information Hiding, pp. 131-145, Springer Berlin Heidelberg, 2005.

[24] Cox, Ingemar J., Matthew L. Miller, Jeffrey A. Bloom, and Chris Honsinger, "Digital watermarking", vol. 53, San Francisco: Morgan Kaufmann, 2002.

[25] Cox, Ingemar, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker, "Digital watermarking and steganography". Morgan Kaufmann, 2007.

[26] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory,* vol. 22 , no. 6, pp. 644 - 654, 1976.

[27] B. Schneier, "Applied cryptography", Wiley, New-York, USA, 1996.