Survey on Multimedia Data Security

K. Kalaivani and B. R. Sivakumar

***Abstract*—This Paper, deals with the various techniques related to security aspect of Multimedia data, especially the Medical data, their advantages and disadvantages. The First Part describes the Introduction of Multimedia data and its use in Medical field. The Second part describes various techniques that can be applied for General Multimedia data. The third Part describes various techniques that can be applied to Medical images. The Fourth part describes necessity to improve the security of Medical data and the requirement of new algorithm for improving the security and quality of medical data captured by different image capturing devices like ultra-sonography (US), positron emission tomography (PET), single-photon emission computed tomography (SPECT), optical imaging (OI), computed tomography (CT), X-ray, ultrasound, MRI etc.**

***Index Terms*—Multimedia medical data, PACS, DICOM, telemedicine, cryptography, and watermarking.**

I. Introduction

Due to the recent developments in computer networking technology, distribution of digital multimedia content through the internet is enormous. However, the increased number of digital documents, multimedia processing tools, and the worldwide availability of Internet access has created a very suitable medium for copyright fraud and uncontrollable distribution of multimedia content. A major requirement now is to protect the intellectual property of multimedia content in multimedia networks. There are number of data types that can be characterized as multimedia data types. These are typically the elements for the building blocks of generalized multimedia environments, platforms, or integrating tools. The basic types can be described as text, images, audio, video and Graphic objects. Multimedia finds its application in various areas including, but not limited to, advertisements, art, education, entertainment, engineering, medicine, mathematics, business, scientific research and spatial temporal applications. Particularly in Medicine, doctors can get trained by looking at a virtual surgery or they can simulate how the human body is affected by diseases spread by viruses and bacteria and then develop techniques to prevent it. So with the development of information communication and computer technology, there has been the growth of Digital hospital, Telemedicine in network by database of digital medical image.

HIS (Hospital information system) and PACS (Picture archiving and communication system) based on DICOM (Digital imaging and communications in Medicine) pave the way to store medical images and search for database and give remote medical treatment[1].

Manuscript received December 22, 2011; revised February 13, 2012.

The authors are form Easwari engineering college, R.M.K Engineering college. (e-mail id:kvani2007@gmail.com; hod.ece@rmkec.ac.in)

II. Techniques to Enhance the Security of Multimedia Data

Information security has traditionally been ensured with Encryption techniques. Generally encryption techniques, such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the Rivest, Shamir and Adelman (RSA) algorithm, the Triple DES (3DES), and the International Data Encryption Algorithm (IDEA) and Scalable encryption algorithm(SEA), work on bit stream of data input without regard to their nature of application. In other Words, the encryption proceeds without distinguishing the input data as either: audio, video, text, or graphics.

TABLE1. Classification of Standard Encryption Methods, Adapted From [2]

Encryption algorithm	Basic operations	Advantages & Drawbacks
DES	XOR, Substitution and Permutation	Suitable for High speed and low cost hardware/software implementations. But Small 56 bit key size makes it undesirable.
3-DES	Comprises 3 DES keys	Efficient and susceptible to chosen plaintext, but memory and time requirement is more.
AES	Sub bytes, Shift rows, Mix column and add round key.	Very good performance in hardware and software implementations, Low Memory requirement.
IDEA	XOR, Addition and Multiplication	Security level is high when compared to DES.
RSA	Primality test, Modulus, Euler's totient Function, Co prime and Multiplicative inverse	It is Public key system. Secured but speed is lower, when compared to Symmetric key systems
SEA	XOR,S-Box, Word rotation, bit Rotation and modular addition	Extremely simple but can be used only in embedded applications where resources are limited.

When the Multimedia data is not a real time data, it can be treated as a regular binary stream and above mentioned conventional techniques can be applied. When varieties of constraints are present, it is difficult to accomplish security for multimedia data.

A. Video Encryption

Symmetric key cryptography algorithms can be used to

encrypt the multimedia data. But the fastest algorithm, such as AES, is computationally very costly for many of the real-time multimedia data.

1) Video scrambling

This method uses filter banks or frequency converters and it is performing permutation of the signal in time domain or distortion of the signal in the frequency domain. However, this scheme is offering less security, and this method can be easily cracked by advanced computers [3].

2) Selective Video encryption

Selective encryption technique is combining compression with encryption. And this technique can handle real-time audio and video data efficiently [4].This method is selecting only the very important coefficients from final or intermediate steps of a compression process and encrypt those coefficients. Coefficients which are less important not encrypted.

a) Secure MPEG (SECMPEG)

The SECMPEG contains four different levels of security. At the first level, SECMPEG encrypts the headers from the sequence layer to the slice layer, while the motion vectors and DCT blocks are unencrypted. At the second Level, most relevant parts of the I-blocks are additionally encrypted (upper left corner of the block). At the third level, SECMPEG encrypts all I-frames and all I-blocks. Finally, at the fourth level, SECMPEG encrypts the whole MPEG-1 sequence (the naive approach)[5]. This is the first technique to realize the benefits of encrypting only selected bits in a video bit stream. But speed is reduced and special encoder and decoder is required to handle SECMPEG streams.

b) Aegis

Aegis was initially designed for MPEG-1 and MPEG-2 video standards. Aegis method [6] encrypts I-frames of all MPEG groups of frames in an MPEG video stream, while B- and P frames are left unencrypted. In addition, Aegis also encrypts the MPEG video sequence header, which contains all of the decoding initialization parameters that include the picture width, height, frame rate, bit rate, buffer size, etc. This method provides sufficient security for the entertainment videos, such as the pay TV broadcast, but not satisfying the applications where the security is one of the top priorities.

c) Zigzag Permutation Algorithm

This algorithm is based on embedding the encryption into the MPEG compression process. The JPEG images and the I-frames of MPEG video undergo a zigzag reordering of the 8x8 blocks[7]. The zigzag pattern forms a sequence of 64 entries that is ready to enter entropy-encoding stage. The main idea of this approach is to use a random permutation list to map the individual 8x8 blocks to a 1x64 vector. Zig zag permutation cipher seriously lacks the desired level of security.

d) Qiao-Nahrstedt Video Encryption Algorithm

Qiao and Nahrstedt have proposed an MPEG video encryption algorithm [8] based on the statistical analysis of the MPEG video stream. This algorithm first divides a chunk of the MPEG video stream into two byte lists: an odd list and an even list. Then it performs the XOR operation to encrypt the odd list, and uses another encryption function to encrypt the even list to get the cipher text. Since this chunk of data is a non-repeated pattern, it is considered to be perfectly secure. The speed of this algorithm is roughly a half of the speed of naive algorithm, but that is arguably still the large amount of computation for high quality real-time video applications that have high bit rates.

e) Shi - Wang - Bhargava Video Encryption Algorithms

Shi, Wang and Bhargava have classified their work into four different Video encryption algorithms [9].

e.1) Algorithm I

This algorithm uses the permutation of Huffman code words in the I-frames. And incorporates encryption and compression in one step. The secret part of the algorithm is a permutation p, which is used to permute standard JPEG/MPEG Huffman codeword list. In order to save compression ratio, the permutation p must be such that it only permutes the code words with the same number of bits. But this algorithm is highly vulnerable to known-plaintext attack, and cipher text-only attack.

e.2) Algorithm II (VEA)

This algorithm encrypts only the sign bits of the DCT coefficients in an MPEG video. The Algorithm II simply xors the sign bits of the DCT coefficients with a secret m-bit binary key $k = k1k2...km$. The security of this algorithm depends on length of the key. If the key is as long as the video stream and it is unique and used only once which is known to be absolutely secure. But this is highly impractical for mass applications such as VOD (Video on Demand) and similar. On the other hand, if the key is too short, many attacks can be developed.

e.3) Algorithm III (MVEA)

Modified Video encryption algorithm (MVEA) is an improvement over VEA. It includes the following additions: the sign bits of differential values of motion vectors in P- and Bframes can also be randomly changed. This type of improvement makes the video playback more random and more non-viewable. When the sign bits of differential values of motion vectors are changed, the directions of motion vectors change as well. In addition, the magnitudes of motion vectors change, making the whole video very chaotic. Still, this algorithm is also having security issues.

e.4) Algorithm IV (RVEA)

Real-time Video encryption algorithm (RVEA), which uses conventional symmetric key cryptography to encrypt the sign bits of DCT coefficients and the sign bits of motion vectors. The selective approach significantly speeds up the process of conventional encryption by only encrypting certain sign bits in the MPEG stream. The sign bits of DCT coefficients and motion vectors are simply extracted from the MPEG video sequence, encrypted using a fast conventional cryptosystem such as AES, and then restored back to their original position in the encrypted form. So this algorithm is much better than previous three algorithms in terms of security.

B. Audio and Speech Encryption Techniques

Secure voice (alternatively secure speech or ciphony) is a term in cryptography for the encryption of voice communication over a range of communication types such as radio, telephone or IP. It is enough to apply the naive

approach, but in many instances this is too computationally expensive in the case of small mobile devices. As far as the security is concerned, perhaps the most important type of audio data is speech. Unlike in the case of music files and similar entertainment audio sequences, in many applications, speech requires substantial level of security.

1) Encryption of compressed speech

Speech signals are encrypted simply by permutation of speech segments in the time domain or distort the signal in the frequency domain by applying inverters and filter banks. But this method is insecure.

a) Selective Encryption Algorithm for G.723.1 Speech Codec

G.723.1 is the most popular compression standard, which has a very low bit rate, and extremely suitable for voice communications over the packet-switching based networks. In this method [10], selective encryption is applied to most significant bits of all important G.723.1 coefficients. The total number of selected bits for encryption is 37 in each frame, which is less than 1/5 of the entire speech stream at the 6.3 Kbps rate, and less than 1/4 of the entire speech stream at the 5.3 Kbps rate. In this part, by taking a audio file, comparison is performed between total DES encryption, total AES encryption and selective AES encryption on the quantized audio data experimentally by considering time consumption and SNR values as parameters for the audio files Sam4 and C5 as shown in Fig. 1 and Fig. 2.

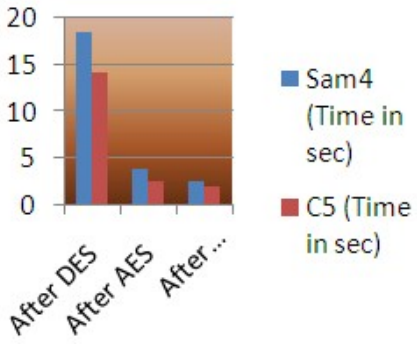

Fig. 1. Time consumption in sec.

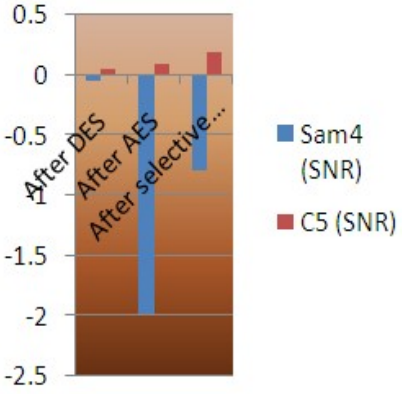

Fig. 2. SNR in dB.

Time consumption for selective AES encryption on MP3 compression is less than total AES and DES encryption techniques on MP3 compression. So, the selective encryption technique is better than total DES and AES encryption techniques as it takes less time with degradation of signal that is inaudible to the unauthorized users.

b) Perception-Based Partial Encryption Algorithm

This algorithm [11] is applied for partial encryption of telephone bandwidth speech and it is implemented for the ITU-T G.729 codec for a rate of 8 Kbps. Two partial-encryption techniques are developed, a low-protection scheme, aimed at preventing most kinds of eavesdropping and a high-protection scheme, based on the encryption of a larger share of perceptually important bits and meant to perform as well as full encryption of the compressed bit stream.

2) B. Encryption of compressed Audio

There are numerous applications where the general audio data needs to be protected, and the expensive naive approach might be infeasible. In the case of MP3 (MPEGI, Layer3), selective encryption [12] is implemented in which the MDCT (Modified cosine transform) coefficients are partitioned into several frequency regions during Huffman encoding. This spectral subdivision may be exploited to lower the perceptual quality of the compressed signal by low-pass filtering. Limiting the frequency content of audio material is an effective way to generate sample-mode quality, an attractive alternative to the simpler approach of introducing annoying artifacts, such as clicks and pops. The cut-off frequency, moreover, may be modified by increasing or decreasing the number of coefficients that the decoder may decompress, delivering the desired degrees of perceptual quality. This algorithm provides sufficient level of security.

C. Image Encryption Techniques

Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. However, there are number of applications for which the naive based encryption and decryption represents a major bottleneck in communication and processing. So in that cases selective image encryption techniques are used. Selective image encryption is based on encrypting only certain parts of the image, in order to reduce the amount of computation.

1) Partial Encryption Schemes for Images

Partial encryption methods [13] that are suitable for images, compressed with two specific classes of compression algorithms. They are quadtree compression algorithms, and wavelet compression algorithms based on zero trees. Partial encryption scheme encrypts only the significance information related to pixels.

2) Selective Encryption Methods for Raster and JPEG Images

An uncompressed (raster) grey level image defines 8 bit planes. The highest (most significant) Bit planes are highly correlated to the original gray level image. This selective encryption scheme [14] that is consisted of xoring the selected bit planes with a key that has the same number of bits as the bits that are to be encrypted. Encrypting only the bit planes that contain nearly uncorrelated values would decrease the vulnerability to the known-plaintext attacks.

The second method is designed to selectively encrypt the JPEG compressed images. In this selective encryption method, only the appended bits that correspond to the selected AC coefficients are encrypted. The DC coefficients are left unencrypted, since their values are highly predictable. On the other hand, the code words are left unencrypted for the

synchronization purposes.

III. Techniques to Enhance the Security of Medical Data

Data security in medical information system has become a priority for citizens and for government. The need to accumulate, share and analyze personal data is to improve the quality of care through electronic medical record. Data security has three main properties: confidentiality, integrity and availability. Overall, the property of confidentiality prevents illegal access. The property of integrity guarantees detection of any modification of data, whether accidental or malicious. Finally, the property of availability protects the system against the attacks of denial of service.

A. Content-based Watermarking Technique

In this technique [15], Patient's information are encrypted and inserted in an image associated to it. This method implemented a security architecture using watermarking and encryption techniques in addition to the security provided by database management system.

B. Digital Watermarking of Medical Image

Recently, the medical image has been digitized by the development **of** computer science and digitization **of** the medical devices. There are needs for database service of the medical image and long term storage because of the construction of PACS (Picture Archiving and Communication System) following DICOM (Digita1 Imaging Communications in Medicine) standards, telemedicine, and et al**.** Furthermore, authentication and copyright protection are required to protect the illegal distortion and reproduction of the medical information data [16]. So this technique propose digital watermarking technique for medical image that Prevents illegal forgery that can be caused after transmitting medical image data remotely. A wrong diagnosis may be occurred if the watermark is embedded into the whole area of image. Therefore, watermark is embedded into some area of medical image, except the decision area that makes a diagnosis so called region of interest (ROI) area to increase invisibility.

C. Lossless Watermarking Method Based on Haar Wavelet Transform

This method [17] identifies parts of the image that can be reversibly watermarked and conducts message embedding in the conventional Haar wavelet transform coefficients and this approach makes use of an approximation of the image signal that is invariant to the watermark addition for classifying the image in order to avoid over/underflows. The method has been tested on different sets of medical images and it is one of the most competitive existing lossless watermarking schemes in terms of high capacity and low distortion.

D. Watermarking Techniques for Medical Imaging

Three kinds of watermarking methods [18] were identified for medical images. A first class regroups methods that embed information within region of non-interest (RONI) in order not to compromise the diagnosis capability and in this method changing the black background in a salt and pepper like noisy pattern may annoy the physician. Consequently, the watermark signal amplitude has to be correctly selected. The second approach corresponds to reversible watermarking. Once the embedded content is read, the watermark can be removed from the image allowing retrieval of the original image which provides robustness and sometimes it introduces in the image a highly visible salt-and-pepper noise. The third approach consists in using classical watermarking methods while minimizing the distortion. In that case, the watermark replaces some image details such as the least significant bit of the image or details lost after lossy image compression and provides robustness.

E. A Lossless Data Embedding Scheme for Medical Images

This method [19] is embedding to medical images with patient information such as patient personal data, history, test and diagnosis result before transmitting and storing, and recovering the embedded information and the original images exactly after receiving is an efficient way to execute correct medical practice and reduce storage, memory requirement and transmission time. It provides integrity of medical images and corresponding documentations, and protection of information.

F. Approaches to Medical Image Integrity and Authenticity

There are two major approaches to provide authenticity and integrity: the use of metadata (e.g., header) and the use of watermarking [20].

1) **Metadata*:*** Metadata are data attached to the information. For image security, usually the digital signature is the metadata, which is stored along with the medical image. The best known approach DICOM standard, where the digital signature information is stored in its header. The metadata approach has also been used to introduce confidentiality, using DICOM header data to encrypt the images.

2) **Watermarking:** Watermarking is a technique that embeds information into its own data, widely used for purposes like digital rights management (DRM).

G. Multiple Digital Watermarking Applied to Medical Imaging

This technique is wavelet-based multiple watermarking scheme [21] and simultaneously embeds four types of watermarks into medical images, aiming to enhance protection of sensitive data, provide source and data authentication capability, and allow efficient image archiving and retrieval. In order to increase robustness of the watermarks conveying signature, index, and caption data, a combination of repetition and BCH coding is performed during the embedding procedure. The experimental results demonstrate the efficiency of the scheme in terms of robustness, imperceptibility, and integrity control capability, thus illuminating its potential to act as a value-added tool in medical information management.

H. Medical Image Watermarking with Tamper Detection and Recovery

It is a fragile watermarking scheme which could detect tamper and subsequently recover the image. This scheme [22] required a secret key and a public chaotic mixing algorithm to embed and recover a tampered image. The scheme was also

resilient to VQ (Vector quantization) attack. The purpose of this technique is to verify the integrity and authenticity of medical images.

I. Integration of Medical data

There are certain special problems in the field of medicine have not yet been solved. These problems include integration of data from different sources and provision of multiple levels of access control to protect the privacy of patients. So this method provides data integration and security by mixing medical waveforms and images with encrypted patient identifiers and unencrypted associative data, such as acquisition parameters, diagnostic images, and notes and comments in textual, pictorial, and voice forms [23]. The sampling rate of the data is varied according to their local smoothness. Then, redundant samples (or pixels) are eliminated and replaced by associative data which are labeled using a status string encoded based on the Huffman and run-length techniques. This method achieves both data compression and integration simultaneously.

J. Data Hiding Scheme for Medical Images

This scheme [24] is embedding patient information into a medical image through data hiding could improve the level of security and confidentiality that is essential for diffusion of medical information system. Such security provides integrity of medical images and corresponding documentations, along with protection of confidential information. The scheme imperceptibly embeds in medical images patient's personal information like name and unique identification number. The objective was to have a simple model which uses minimal resources and hence a strong candidate for use in mobile healthcare applications where the resources of memory, computation and connectivity are extremely limited.

K. Reversible Watermarking of Medical Image.

TABLE II: CAPACITY RATE AND PSNR VALUES FOR VARIOUS REVERSIBLE WATERMARKING ALGORITHMS.

Algorithm used	Capacity Rate in bpp	PSNR in dB
Reversible Watermarking	0.15	49.11
Lossless watermarking with DSA Approach	0.10	48.51
Reversible watermarking with SHA-256	0.05	41.00
Reversible watermarking with RSA approach	0.034	51.5

The goals of lossless watermarking are to protect the copyrights and can recover the original image [25]. There are mainly two schemes in reversible or lossless watermarking. In the case of additive insertion, the watermark to be embedded is embedded in to the original image. In Substitutive insertion the basic LSB scheme removes the pixels least significant bits by bits of the message to be embedded. The Table II shows that capacity rate and PSNR values of medical images with various algorithms implemented by using MAT lab. From the following table, discussion can be done, that the capacity rate and PSNR values for various medical images by using reversible watermarking algorithms.

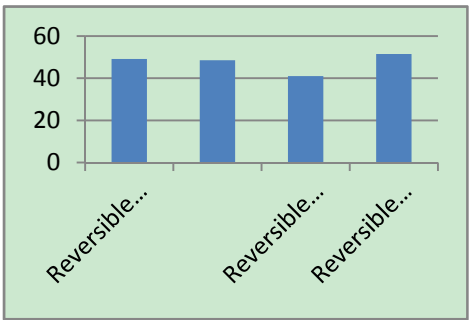

Fig. 3. PSNR in dB

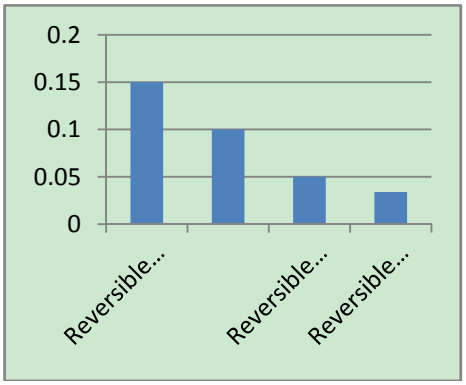

Fig. 4. Capacity rate in bpp

Finally reversible watermarking with RSA approach having best capacity rate and maximum PSNR value when compared to another algorithm as shown in Fig. 3 and Fig. 4.

L. Medical Image Security in a PACS Environment

Medical image security is an important issue when digital images and their pertinent patient information are transmitted across public networks. Here it is proposed that a dedicated PACS security server that will act as an image authority to check and certify the image origin and integrity upon request by a user [26]. The public key (asymmetric) cryptography technology is an effective tool for a secure data communication. The method has been utilized recently in DICOM Security Profiles for secure communication of DICOM images. Medical image security in a PACS environment has become a pressing issue as communications of images increasingly extends over open networks, and hospitals are hard pushed by government mandates, and security guidelines to ensure health data security. However, there has not been an infrastructure or systematic method to implement and deploy these standards in a PACS environment.

IV. CONCLUSION

This paper has presented a literature review of the state-of-the technology of Multimedia medical information security. It is clear that, in the case of existing security schemes there are some drawbacks. Major problem with watermarking scheme is that they are not very robust against different types of image manipulations or attacks. These techniques are quite complicated to implement in real time

and Criminals can use encryption to secure communications, or to store incriminating material on electronic devices. Medical images are sensitive. So it is necessary to protect them. Based on the limitations of different techniques seen that, there is a need of special technique for medical image communication which will takes care of security aspects.

REFERENCES

[1] H.-K. Lee, H.-J. Kim, K.-R. Kwon, and J.-K. Lee, "Digital Watermarking of Medical image using ROI information," *IEEE*, 2009.

[2] G. A. Francia III, M. Yang, and M. Trifas "Applied Image.Processing to Multimedia Information Security," *IEEE*, 2009.

[3] B. Furht, D. Socek, and A. M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques," *CRC Press*, 2004.

[4] T. Lookabaugh, D. C. Sicker, D. M. Keaton, W. Y. Guo, and I. Vedula, "Security Analysis of Selectively Encrypted MPEG-2 Streams," *Multimedia Systems and Applications VI Conference*, Orlando, FL, 2004.

[5] B. Furht and D. Kirovski, "Multimedia Encryption and Authentication Techniques and Applications," *Auerbach Publications* pp.91–128, 2006.

[6] T. B. Maples and G. A. Spanos, "Performance study of selective encryption scheme for the security of networked real-time video," in *Proceedings of the 4th International Conference on Computer and Communications*, Las Vegas, NV,1995.

[7] L. Tang," Methods for Encrypting and Decrypting MPEG Video Data Efficiently," in *Proceedings of the 4th ACM International Multimedia Conference*, Boston, MA, 2006.

[8] L. Qiao and K. Nahrstedt, "A New Algorithm for MPEG Video Encryption," in Proceedings *of the 1st International Conference on Imaging Science, Systems and Technology (CISST '97)*, Las Vegas, NV, pp. 21-29,1997.

[9] B. Bhargava, C. Shi, and Y. Wang, "MEPG Video Encryption Algorithms", 2002, Available: http://raidlab.cs.purdue.edu/papers/mm.ps

[10] C.-P. Wu and C.-C. J. Kuo, "Fast Encryption Methods for Audiovisual Data Confidentiality," *SPIE International Symposia on Information Technologies 2000*, Boston, MA, pp. 284-295, 2002.

[11] A. Servetti and J. C. De Martin, "Perception Based Partial Encryption of Compressed Speech," *IEEE Transaction on Speech and Audio Processing*, vol. 1, no. 8, 2002.

[12] N. J. Thorwirth, P. Horvatic, R. Weis and J. Zhao ," Security methods for MP3 music delivery," Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers, vol. 2, pp 1831-1835,2000.

[13] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Video," *IEEE Transactions on Signal Processing*, pp. 2439-2451, 2000.

[14] M. Van Droogenbroeck and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images," Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) Ghent, Belgium. 2002.

[15] Mustapha Machkour, Youness Idrissi Khamlichi, and Karim Afdel, "Data security in medical information system," *IEEE*, 2009.

[16] H.-K. Lee. H.-J. Kim. K.-R. Kwon, and J.-K. Lee, "Digital Watermarking of Medical Image Using R0I Information," *IEEE*, 2005.

[17] W. Pan, G. Coatrieux, N. Cuppens, and F. Cuppens, "An Additive and Lossless Watermarking Method Based on Invariant Image Approximation and Haar Wavelet Transform," *32nd Annual International Conference of the IEEE EMBS Buenos Aires*, Argentina, 2010.

[18] G. Coatrieux and L. Lecornu, "A Review of Image Watermarking Applications in Healthcare," *IEEE*.

[19] X. Luo, Qiang Cheng, and J. Tan," A Lossless Data Embedding Scheme for Medical Images in Application of e- Diagnosis," *in Proceedings of the 25th Annual Intemational Conference of the IEEE EMBS Cancun*, Mexico,2003.

[20] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto, "Providing Integrity and Authenticity in DICOM Images: A Novel Approach," *IEEE transactions on information technology in Biomedicine*, vol.13, no.4, 2009.

[21] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Digital Watermarking Applied to Medical Imaging," in *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China, 2005.

[22] J. M. Zain and A. R. M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery," in *Proceedings of the 28th IEEE EMBS Annual International Conference*, New York City, USA, 2006.

[23] M. Sun, Y.-Q. Shi, Q. Liu, and R. J. Sclabassi, "Sample Domain Integration of Medical Data for Multimedia Diagnosis," *IEEE*, 2002.

[24] V. N. Kumar, M. Rochan, S. Hariharan, and K. Rajamani, "Data Hiding Scheme for Medical Images using Lossless Code for Mobile HIMS," *IEEE*, 2011.

[25] A. Umamageswari, M. F. Ukrit, and G. R. Suresh," A Survey on Security in Medical Image Communication," *International Journal of Computer Applications*, vol. 30, no. 3, 2011.

[26] F. Cao, H. K. Huang, and X.Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Computerized Medical Imaging and Graphics*, vol. 27, pp. 185–196, 2003.

K. Kalaivani received the B.E degree in Electronics and communication engineering from Bharathiar university, Coimbatore,India in 1999. She received the M.E degree in Embedded systems from college of engineering, Guindy,Chennai, India in 2008. From 2001 to 2011 she was employed as a Assistant professor in Electronics and communication engineering department of R.M.K engineering college. In 2011 July onwards working as a Assistant Professor in Easwari engineering college. She is a research scholar doing Ph.D under the supervision of Dr.R.Sivakumar , R.M.K Engineering college. Her interest in research includes Multimedia Medical image processing and Neural networks. She is a member of IACSIT.