2011 International Conference on Signal, Image Processing and Applications
With workshop of ICEEA 2011
IPCSIT vol.21 (2011) © (2011) IACSIT Press, Singapore

Survey on Multimedia Data Security

K.Kalaivani[1] and R.Sivakumar[2]

[1] Dept of EIE, Easwari engineering College, Chennai,kvani2007@gmail.com

[2] Dept of ECE, R.M.K Engineering College, Chennai,hod.ece@rmkec.ac.in

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.

Keywords: Multimedia medical data, PACS, DICOM, Telemedicine, Cryptography, and Watermarking.

1. 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. 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].

2. Techniques to Enhance the Security of Multimedia Data

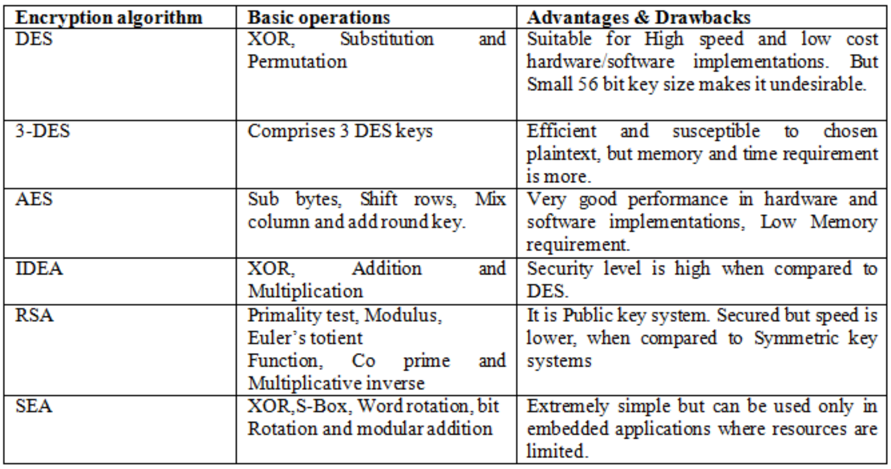
Information security has traditionally been ensured with Encryption techniques. Generally encryption techniques, such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the Rivest, Shamir and Adelman (RSA) algorithm, the Triple DES (3DES), and the International Data Encryption 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.

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.

2.1. 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.

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.

2.1.1 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].

2.1.2 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.

- 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.
- 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.
- 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.
- 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

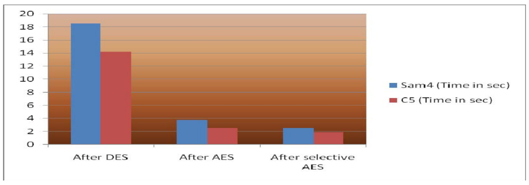
to be perfectly secure. The speed of this algorithm is roughly a half of the speed of naive algorithm, but that is arguably still the large amount of computation for high quality real-time video applications that have high bit rates.

2.2. Audio and Speech encryption techniques

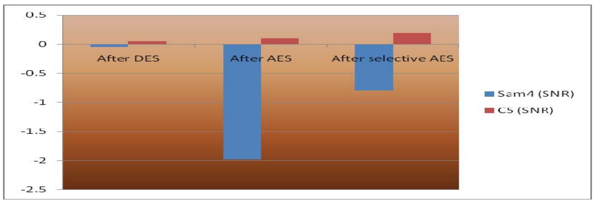
Secure voice (alternatively secure speech or ciphony) is a term in cryptography for the encryption of voice communication over a range of communication types such as radio, telephone or IP. It is enough to apply the naive approach, but in many instances this is too computationally expensive in the case 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.

- Selective Encryption Algorithm for G.723.1 Speech Codec: 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. 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 [9], 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.

Time consumption in sec



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.

- Perception-Based Partial Encryption Algorithm: This algorithm [10] 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.

2.3. 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.

- Partial Encryption Schemes for Images: Partial encryption methods [11] that are suitable for images, compressed with two specific classes of compression algorithms. They are quad tree compression algorithms, and wavelet compression algorithms based on zero trees. Partial encryption scheme encrypts only the significance information related to pixels.

- 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 ,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.

3. Techniques to Enhance the Security of Medical Data

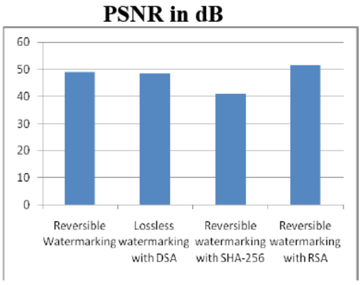
Data security in medical information system has become a priority for citizens and for government. The need to accumulate, share and analyze personal data is to improve the quality of care through electronic medical record. Data security has three main properties: confidentiality, integrity and availability. 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.

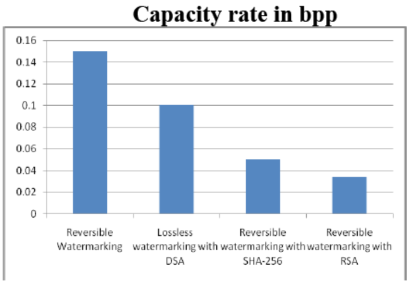
- Content-based Watermarking Technique: In this technique , Patient's information are encrypted and inserted in an image associated to it. This method implemented a security architecture using watermarking and encryption techniques in addition to the security provided by database management system.
- Digital Watermarking of Medical Image: Recently, the medical image has been digitized by the development of computer science and digitization of the medical devices. his 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.
- A Lossless Data Embedding Scheme for Medical Images : This method 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.
- Data Hiding Scheme for Medical Images:This scheme 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.
- Reversible Watermarking of Medical Image: The goals of lossless watermarking are to protect the copyrights and can recover the original image . 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 following table 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.

Table 2: 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





Finally reversible watermarking with RSA approach having best capacity rate and maximum PSNR value when compared to another algorithm.

4. 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.

5. References

[1] Hyung-Kvo Lee, Hee-Jung Kim, Ki-Ryong Kwon, Jong-Keuk Lee. Digital Watermarking of Medical image using ROI information, 2005, IEEE.

[2] Guillermo A. Francia III, Ming Yang, Monica Trifas .Applied Image Processing to Multimedia Information Security,2009, IEEE.

[3] Borko Furht, Daniel Socek, Ahmet M. Eskicioglu. Fundamentals of Multimedia Encryption Techniques, 2004, CRC Press.

[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, 2003, Orlando, FL.

[5] Borko Furht and Darko Kirovski. Multimedia Encryption and authentication Techniques and applications, 2006, Auerbach Publications Pages 91–128.

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

[7] L. Tang. Methods for Encrypting and Decrypting MPEG Video Data Efficiently, Proceedings of the 4th ACM International Multimedia Conference, 1996, Boston, MA.

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

[9] 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.

[10] A. Servetti and J.C. De Martin .Perception Based Partial Encryption of Compressed Speech, IEEE Transaction on Speech and Audio Processing, 2002,Vol. I, No. 8.

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