RESEARCH ARTICLE OPEN ACCESS

A Review on Trending Cryptography Approaches for Security In Images

Simrat Kaur [1], Rupinder Kaur [2]
Department of Computer science
Baba Banda Singh Bahadur Engineering College
Fatehgarh Sahib
India

ABSTRACT

As the whole world is revolutionized with the advent of internet services and improved communication facilities. Now people prefer to consult their doctor by using the internet facilities. To communicate with the doctor for diagnosis and treatment of patient from the distant location by using the telecommunication services is known as telemedicine. In telemedicine technique the information related to patient is transmitted over the open network. This information is generally comprised of images, audio, video etc. Now in the open network this information can be easily accessed and altered by the malicious users. Therefore it is required to protect the sensitive data transferred over the network. In this paper the medical image encryption techniques are discussed. Cryptography in medical images may be described as encoding and decoding methods implemented on the medical images to hide the information in cover image so that only authorized user will able to access it. Various types of cryptography methods are explained in this paper along with different goals of cryptography.

***Keywords* :—** Cryptography, encryption, decryption, telemedicine, medical images, image security .

I. INTRODUCTION

In medical field it is required to transmit the data quickly and in secured manner. In present scenario image transmission becomes very important in medical applications therefore it is important to develop an optimum way to transmit the images over the internet [1]. Telemedicine may be described as a new technique that helps in implementation of communication system in the field of healthcare system. Telemedicine has improved the medical field system. Various types of benefits are associated with the telemedicine like remote diagnosis of disease and consultation from doctors, remote-distance learning. But this technique is associated with the risk because the data is transmitted over the open networks, and therefore can be easily accessed by the malicious users. Hence people working in medical field demand for techniques to transmit the medical images in secure way so that the safe transmission of record can take place.

As telemedicine has revolutionized the whole medical system therefore the requirement for secured medical images and record transmission has triggered the healthcare organizations at international level to create the standards for medical data transmission. Example of international standard is digital imaging and communication in medicine (DICOM). Standards generated by the international organizations provide the specific strategy and mechanism to acquire three types of telemedicine security services: confidentiality, authenticity and integrity. When these standards are applied on the medical images while transmission, the illegal access will not occur. To avoid the tampering of sensitive data and validate the ownership, the authenticity services will be helpful. At present, various techniques like cryptography, digital watermarking is implemented to obtain the desired security services in the medical field. The cryptography technique applied in applications of telemedicine has been derived from the cryptographic functions like symmetric encryption, hashing and digital signatures. With the help of symmetric encryption the confidentiality of image transmitted over the network is maintained by implementing block coding techniques and stream coding method. On the other hand the hashing technique and digital signatures verify the authenticity of received medical images. Now in the digital image watermarking technique, the sensitive data is hided into digital medical images. In this technique the patient’s medical record is embedded as watermark. On the other hand the authenticity is acquired by hiding watermarks into the medical images. The watermarks hided in the images are not perceptible by human eye. The technique of watermark embedding reduces the quality of medical image therefore this technique is not widely accepted by the medical standards [2].

II. NECESSITY FOR IMAGE SECURITY

With the advancement in information and communication system various new issues related to security and privacy of data has been raised. Therefore using the secure form of transmission system for images is very important in present scenario and also its related matter must be handled carefully. As it is highly important to secure the medical image while transmitting it over the internet, therefore various encoding schemes to encrypt the digital images have been introduced. Generally implemented security techniques are: DFT, DCT, DWT, etc. transmission of medical image over the open network will lead to two types of attack on the image that are as follow:

1) ***Active attacks:*** This consists of few data stream modification or false data stream creation.
2) ***Passive attacks:*** This attack uses the data but not affect the system resources.

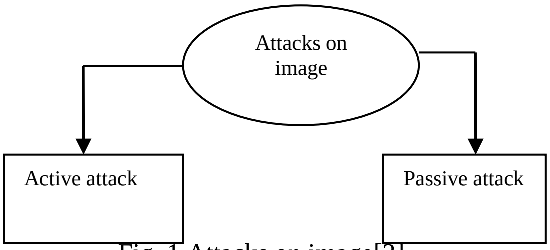

Fig. 1 Attacks on image[3]

III. PERFORMANCE PARAMETERS OF ENCRYPTION TECHNIQUE

Various parameters that help in determining the efficiency of image encryption technique are as follow: [3]

a. Encryption Ratio (ER): It analyses the amount of information need to be encoded. Therefore the value of encryption ratio should be least so that the computational complexity will reduce.

b. Speed (S): In real time applications, encoding and decoding speed plays vital role.

c. Visual Degradation (VD): It analyzes the perceptual distortion on images. In various applications this parameter plays important role. By obtaining the optimum value of VD the image data can be protected from the illegal attacks. For sensitive data, optimum value of VD will disguise the malicious users.

d. Format Compliance (FC): Encoded data stream must be in compliance with compressor and the standard decrypting device must decode the data without any decryption.

e. Cryptographic Security (CS): It describes about the necessity of encoding scheme to protect the data from malicious attacks. For sensitive multimedia applications it is really important to implement the data encoding schemes.

f. Compression Friendliness (CF): Mostly the encoding techniques are considered as compression friendly but some of the encoding techniques affect the data compression efficiency or add on more data bits. It is required that length of encoded data stream should not increase [4].

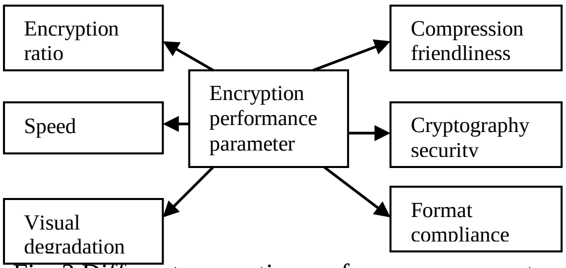

Fig. 2 Different encryption performance parameters [3]

VI. DIFFERENT IMAGE ENCRYPTION METHODS

Various image encoding techniques are described below:

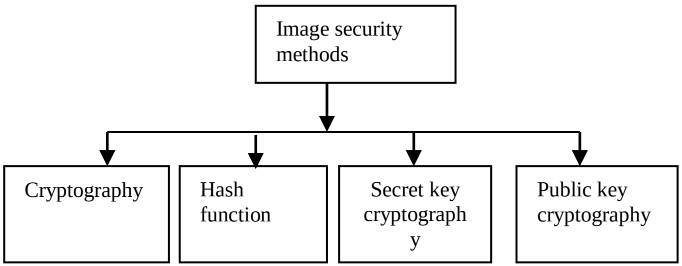

Fig. 3 Image encryption methods [3]

a. ***Cryptography:*** It may be described as a technique implemented for hiding the data stream by using the encryption and decryption methods. This technique is also referred as "public key cryptography". The key used for encoding must be known at both ends

either transmitter or receiver. Therefore the intermediate people cannot easily access the data stream shared between transmitter and receiver end. [5] The word "Cryptography" has been derived from Greek letters. These Greek words are "Krypto" that means hidden and "graphene" that means writing. Therefore cryptography is considered as technique used to hide the written message. The systems that are used for encryption and decryption of data bits in cryptography technique are referred as "cryptosystems". Cryptography system may be described as group of cryptographic mechanism and that is comprised of:

- Paradigm implemented for encoding and decoding.
- Procedure to check Integrity.
- Digital signature technique.

Image encoding paradigm has ability to transform the real image to another form of image so that it is not easy to determine the image in order to make the image information confidential. Technique used for encoding and conversion of plain text with the help of specific key into a format that cannot be easily recognized is known as encryption. On the other hand the technique used for decoding the encoded data so that it can be transformed into readable form of text is known as decryption. In image encryption the plain text may be described as an image which sender wants to transmit towards the receiver end. Here the cipher text may be described as the encoded form of data by using a particular paradigm.

b. Secret Key Cryptography: In this kind of cryptography, single encryption key is used. With the help of this single key the information is encoded at transmitter end and decoded at receiver end.

c. Public Key Cryptography (PKC): In this kind of cryptography technique, two types of encoding key cryptosystems are implemented in order to ensure the secured form of data transmission between sender and receiver unit over the open network. [6] In the public key cryptography system different types of keys are used to encode the information and therefore it is also known as asymmetric cryptosystem. In this encoding system both public and private keys are used to establish both private as well as public form of communication.

d. *Hash Functions (HFs):* In this encryption technique the message integrity is validated to ensure that the message is in its original state and has not altered after implementation of encryption technique. As in telemedicine the image transmission plays an important role therefore it is also required to protect the image from the illegal access.

V. CRYPTOGRAPHY METHODS

The cryptography technique used for encryption of message can be further classified into different groups as shown below:

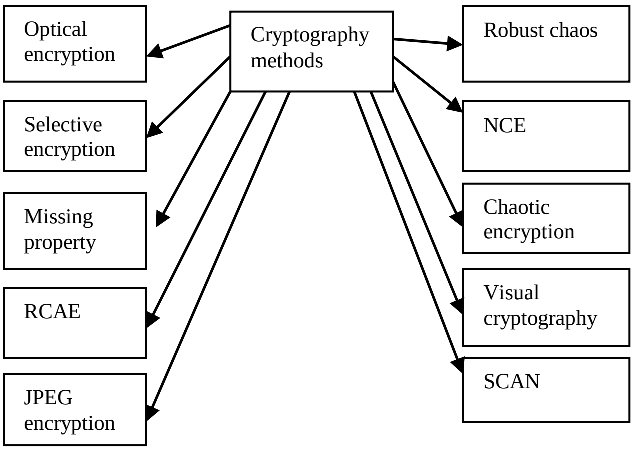

Fig. 4 cryptography methods [3]

a. Optical Encryption: In this type of cryptography technique, optical devices are used to acquire the image encoding by making the components of image random.

b. Selective Encryption: In this type of encryption technique the whole bits in data stream are not encoded. In this only specific bits are used to encode the data stream.

c. Mixing property: It represents the diffusion property. The group of plain texts or data to be encoded has initial region in phase space of map. After this, the mixing property implemented so that the single plain text is obtained over the multiple encoded text digits.

d. Reversible Cellular Automata Based Encryption (RCAE): In this type of cryptography technique, the cellular automat has been design specially in order to get the reversible usage. Size of key used in this type of encryption paradigm is 224 bit.

e. Robust chaos: It is an optimum type of encoding paradigm that has great significance for single key digits on encoded data digits. In robust chaos the encryption keys will exhibit the encoding paradigm factors, therefore it is required that these parameters should be handle with care along with the other variables use in it.

f. JPEG Encryption: The encoding technique was initially introduced for JPEG 2000 format images. This technique obtains multilevel encoding and hence the complexities in computation will reduce [7].

g. Non-chaotic Encryption (NCE): In this encoding technique the Sudoku based matrix is used. The Sudoku matrix used here must be represented in the form of rows and columns. This Sudoku matrix is used for scrambling or encoding the plaintext. In addition to this it is also used for changing the intensity of image pixel. At last, the mapping technique was implemented to shuffle the position of pixels.

h. Chaotic Encryption (CE): Chaotic encryption technique may be described as highly sensitive encryption method. This includes highly sensitive initial values along with the mixing property. This encoding technique also provides the periodic form of encryption.

i. Visual Cryptography: The visual cryptography is a type of encoding technique that implements the human vision to determine the real image and or for decryption process. Therefore in this method no decryption algorithms are required to decode the images. This cryptography technique offers the security to the data so that malicious user cannot easily access the information.

***j. SCAN pattern (SCANP) based encryption*:** This is type of encoding technique was offered for the gray scale images. This also provides the lossless form of compression. In SCAN based encryption method the 2D spatial accessing technique is used [8].

VI. CRYPTOGRAPHY GOALS

There are basically five major goals of cryptography which are described below:

a. Authentication: cryptography technique ensures that the data transmit over the channel is the same that it claims to be. So it can be said that the data transmitted over the channel will not be altered and at the receiver end the original data can be easily accessed [9].

b. Secrecy or Confidentiality: The Confidentiality may be described as connection between two or many people in such a way that the information is just shared between them only. Therefore it can be said that only valid users will access the information and no illegal user can interpret it.

c. Integrity: with the help of cryptography it can be assured that the information is appropriate, precise and prevented from the illegal access from the unauthorized users.

d. ***Non-Repudiation:*** This offers the guarantee that the data transmitted over the network is protected against any rejection by various entities included in transmission process [10].

e. Availability and Service Reliability: The term availability may be described as the capability of the end user to obtain the information in a particular location and also in the appropriate format. The secured form of systems generally attacked by malicious users and that leads to the violation in the information availability and different services to authenticated users. In cryptography the systems are expected to provide the good quality of service to users.

VII. CONCLUSIONS

With the advancement in telecommunication services the telemedicine technique has been widely used. In this technique the medical images are shared over the internet where the unauthorized user can easily extract the sensitive data. Therefore to prevent the images from illegal access the cryptography technique can be implemented. In this the original image and patient's related data is embedded and encoded and after that it is transmitted over the network and finally interpreted by the intended receiver only.

ACKNOWLEDGMENT

I would like to thank Baba Banda Singh Bahadur Engineering College for providing me best infrastructure for preceding my research work.

REFERENCES

[1] Vinay Pandey, Manish Shrivastava "Medical Image Protection using steganography by crypto image as cover Image", International Journal of Advanced computer Research, VOL 2, Issue 5, 2012.

[2] Ali Al-Haj, Gheith Abandah, Noor Hussein, "Crypto-based algorithms for secured medical image transmission", IET, Vol 9, Issue 6, Pp 365-373, 2015.

[3] Madhu B., Ganga Holi, Srikant Murthy K. "An Overview of Image Security Techniques", International Journal of Computer Applications, Vol 154, 2016.

[4] Fahad bin Muhaya, Muhammad Usama and Fahim Akhter "Chaos based Secure Storage and Transmission of Digital Medical Images" Applied Mathematics & Information Sciences An international Journal, Vol 8, Pp27-33, 2014.

[5] Naina Gaharwar Reena Gunjan "Reversible watermarking for digital Images using Visual cryptography and Pixel histogram shifting" IJCSMC, Vol. 4, Issue. 7, Pp 185-193, 2015.

[6] D.R.Denslin Brabin et al, "Reversible Data Hiding: A Survey", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 3, May 2013

[7] C.Anuradha, "Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013,

[8] Rini.J, "Study on Separable Reversible Data Hiding in Encrypted Images", International Journal of Advancements in Research & Technology, Volume 2, Issue 12, December-2013,

[9] Yojna Chandel, "A Review on Reversible Data Hiding", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 9, September 2015,

[10] Dr. J. Jagadeesan, "Reversible Data Hiding In Encrypted Images Using AES Data Encryption Technique", International Journal of Emerging Research in Management &Technology, Volume-3, Issue-4, April 2014,

[11] Sukhdeep Kaur, "Reversible Data Hiding and its Methods: A Survey", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 821-826,

[12] Bhattacharjee, T., Nov. 2014 "Progressive quality access through secret sharing and data hiding scheme"Pp 5-7,2014

[13] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[14] Zhicheng Ni , "Reversible data hiding", IEEE, Volume: 16 Issue: 3,

[15] YUN-QING SH, "Reversible Data Hiding: Advances in the Past Two Decades", IEEE, VOLUME 4,

[16] Haishan Chen et al., "High-Fidelity Reversible Data Hiding Using Directionally-Enclosed Prediction", IEEE Signal Processing Letters, vol. 24, no. 5, pp.574 – 578, 2017.

[17] AuliaArham et al., "Combination Schemes Reversible Data Hiding for Medical Images", 2016 2nd International Conference on Science and Technology-Computer (ICST), pp.44 – 49, 2016.

[18] Tanwi Biswas et al., "A New Method of Reversible Data Hiding Based on Compressed Gray Level Histogram Shifting", 2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), pp.1 – 6, 2016.

[19] Shuang Yi et al., "Improved Reversible Data Hiding in Encrypted Images using Histogram Modification", 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp.004819 – 004823, 2016.

[20] Siren Cai et al., "A New Reversible Data Hiding Scheme Based On High-Dimensional Pixel-Intensity-Histogram Modification", 2016 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), pp.1 – 6, 2016.