1st International Conference on Applied Soft Computing Techniques
22 & 23.04.2017
In association with
International Journal of Scientific Research in Science and Technology

A Survey on Medical Image Encryption

P. K. Kavitha*[1], P. Vidhya Saraswathi[2]
*[1]Research Scholar, Department of Computer Applications, Kalasalingam University, Krishnankoil, Tamil Nadu, India
pkkavitha78@gmail.com[1]
[2]Assistant Professor, Department of Computer Applications, Kalasalingam University, Krishnankoil, Tamil Nadu, India
vidhyasaraswathi.p@gmail.com[2]

ABSTRACT

In healthcare industry Medical images or information is transmitted from source to destination using wired or wireless medium. The transmission of this information requires more security. To transfer the Image information from one place to another encryption and decryption process is used. Encryption means converting data or information from its original form into converting form that hides the information in it. The Image data need to be protected from unauthorized access. Encryption is used to increase the data security. The encrypted Image is secured from any kind cryptanalysis. This paper provides Literature survey of various Image Encryption and Decryption Techniques, methods and algorithms for Medical images.

Keywords: Encryption, Decryption, Cryptanalysis

I. INTRODUCTION

Nowadays Internet is used for faster transmission of valuable information. These information may be text, image, video anything . The Internet has many types of attacks. So the valuable information needs to be protected from the eavesdroppers. Medical Images are used in various fields such as Medical Science, Military communications, Biometric field, Medical Imaging, Telemedicine, Online photograph album, etc. The security of the medical images is based on (i) Confidentiality (ii) Integrity (iii) Availability.

Confidentiality: The protection of data from unauthorized user. The sender and receiver understand the contents of the message which is transmitted.

Integrity: The content of their communication is not changed in transmission.

Availability: Timely accessibility of data to authorized entities.

To exchange the image securely over the network, the image encryption is used. Unauthorized user can't able to decrypt the image. Text Encryption varied from Image Encryption. The characteristics of image are big functionality, high redundancy and correlation between the pixels. Images are vast in size, already existing encryption methods are difficult to apply and sluggish in manner. To transfer digital data into a cipher code encryption process of mathematical algorithms and keys used. To get back the original image or text from converted form that is cipher data, decryption with the mathematical algorithms and keys used.

In image encryption method, we first study the differences between implementations for image data and text data. There are a number of differences between the image data and text data as follows. Text data are sequences of words. Text data can be encrypted directly by using block or stream ciphers. When the cipher text is produced, it must be decrypted to the plaintext in a lossless way. The cipher image can be decrypted to the plain image in some lossy manner. Digital images are represented as 2D arrays. To protect stored 2D data, they must be converted into a 1D array before using encryption techniques. Encryption and Decryption are used by image compression for reducing its storage space and transmission time.

II. CRYPTOGRAPHY TERMINOLOGY

Plaintext: The source message.

Cipher text: The distorted message.
Key: Critical statistics utilized by the Cipher, Only the Sender and Receiver recognizes the key.
Cipher: An algorithmic rule for remodelling Plaintext to Cipher text.
Code: An algorithmic rule for translating an understandable message into an meaningless message.
Encipher: (Encrypt) Converting Plaintext to Ciphertext the usage of a Cipher and a Key.
Decipher: (Decrypt) Converting Ciphertext into Plaintext the usage of a Cipher and a Key.
Cryptology: The combination of Cryptography and Cryptanalysis.
Cryptography: Study of Encryption Principles and strategies.
Cryptanalysis: (Code Breaking) The look at of standards and techniques of deciphering Ciphertext without knowing a key.
Hash algorithm: An algorithmic rule that converts textual content into a string of fixed length.
Secret Key Cryptography (SKC): Single key used for both enciphering and deciphering.
Public Key Cryptography (PKC): Two Keys used. One key for Encipher and some other for Decipher.
Public Key Infrastructure (PKI): PKI is a Certificate authority.

III. CRYPTOGRAPHIC ALGORITHMS

Depending upon the number of keys used, cryptographic algorithms can be categorized into two types :

- Symmetric algorithms (Secret Key)
- Asymmetric algorithms (Public Key)

Symmetric : It is also known as Secret key or Private key. Sender and Receiver used a single key for enciphering and deciphering. Examples : Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard (AES).
Asymmetric : Two different keys (public and private keys) are used for enciphering and deciphering. For Encipher, Public key is used. For Decipher, Private key is used. Examples : Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptosystem (ECC).
Encryption Algorithm : Encipher message created as output. Enciphered data depends on the plaintext and the secret key. It performs various transformations and substitutions on the plaintext.
Decryption Algorithm : Reverse manner of Encipher. It takes the Cipher and the Secret Key as input and gives the plaintext as output.
An encryption algorithm for multimedia data based on arithmetic modulo 2. Both plaintext and ciphertext are of block size 64. Secret key is also of 64 bit length. The structure of this block cipher provide confusion and diffusion.

IV. LITERATURE SURVEY

A. **Q. N. Natsheh et. al [1]** have presented an algorithm using XOR Cipher with AES (Advanced Encryption Standard). DICOM is Digital Images and Communication in Medicine. This file contains Two Parts : Header Data and Client Data. Header Data(Textual Data) stores the Patient's Information. Clinical Data consists of Name, Scan Image Type, Pixel array attributes such as Pixel Depth etc. Pixel Data can be an image, short video or audio. DICOM offer confidentiality for header records. DICOM supports the huge kind of Digital Medical Images consisting of Computed Tomography, Magnetic Resonance Images (MRI). Encrypting Decrypting Medical images required greater computational time. In this paper, AES used for only one image is encrypted and XOR cipher for encrypting the remaining multi-frame DICOM images.

XOR Cipher : It is a symmetric encryption algorithm. XOR cipher is derived from Boolean Algebra XOR function that returns 'True' while two arguments have different values. XOR function can be applied to binary bits. In Enciphering, the strength of the XOR cipher depends on the Length and the nature of the Key. Lengthy Key achieves higher overall performance.

XOR-AES based Encryption:
First approach : First image in the Multi-frame DICOM images as XOR key to encrypt the rest of the images in the Multi-frames.
Second approach: To encrypt the key using AES with Counter(CTR) mode of operation.

This Algorithm is evaluated using computational time, normalized correlation, entropy, PSNR(Peak Signal to Noise Ratio) and Histogram analysis. Medical image confidentiality was achieved by using the XOR cipher. The XOR keys were generated randomly. The Encryption approach based on a random key that

provides better performance and shorter encryption, decryption time than Naive approach.

B. **Vratesh Kumar Kushwaha et. al [2]** have proposed a new technique that combines Encryption and Watermarking for protected transaction of medical image. In this scheme, ROI in the image as the watermark. Selected ROI portion is enciphered by linear feedback shift register totally stream ciphering. Again, this portion is encrypted with the public key. That key is derived from a Diffie-Hellman Algorithm. Region of Interest is embedded into the Medical Image by Spread Spectrum scheme.

Bit Plane Slicing : For analyze the image, keeping apart a digital image into bit planes. Every pixel is represented by using 8 bits. Suppose the image has eight 1-bit planes. It has the ranges from bit plane1 - 0(LSB) to bitplane7 (MSB). Bit Plane 0 includes all lowest order bits and Bit Plane 7 includes all high order bits. Bit-plane extraction for a 8-bit image, value of gray level transformation maps all levels between 0 and 127 to one level and maps all levels from 129 to 253 to another.

Diffie-Hellman : This is a way of exchanging cryptographic keys. It permits two persons that haven't any knowledge about each other. They shared their secret key through the Internet. That key is used to encrypt the Medical Image.

For Example, S and R are Sender and Receiver, then S and R agree a secret key. m and n are two large numbers m & n such that 1< n< m. S chooses random A and then computes $A=n^a$ mod m. R chooses random B and then computes $B=n^b$ mod m. S Computes Key1= n^a mod m. R Computes Key2= n^b mod m. Key1=Key2 =n^{ab} mod m.

Watermarking : The process of embedding digital statistics into another for copyright protection, authentication and authorized verification. For Encipher, Use the equation $E = \Sigma(h, m, k)$ where E is the Stego Image, h is the Host Image, m is the watermark image and k is a secret key. For Deciphering, use the equation D(E, k).

Encryption

- Using Bit plane slicing, pick the MSB plane from the Medical Image
- Then, select the ROI from the MSB plane.
- Generate a 64-bit Secret key the use of LFSR and added to each pixel of the image.
- Using Diffie-Hellman algorithm, the Public Key is generated.

Decryption

- Encrypted watermark image chosen for extraction.
- Watermarked image deciphered by Stream cipher.
- Using Diffie-Hellman algorithm, Public key is generated.
- Add it to extract pixel of the encrypted image.
- Finally, the ROI image is acquired.

The Scheme turned into tested for Different Medical Images. That image may be MRI (Magnetic Resonance Imaging), CT-Scan (Computed Tomography) and X-Ray Images. In this paper, MRI Image of size 256 x 256 was taken as Cover Image and ROI of the image is taken as Watermark. The Public key is generated via using a D-H algorithm by growing the Level of Security.

C. **Simranjeet Kau r et. al [3]** introduced a new Reversible Data Hiding Technique for Authentication and Data Hiding. In this paper, ROI(Region of Interest) and NROI (Non Region of Interest) is defined. ROI is protected and efforts embed data in NROI. Here, Semi-reversible Scheme is capable of hiding patient's data. The Fragile Watermarking Technique is used to verify authenticity of the image, to achieve image authentication.

Watermark: Using Hash Function, generate a fixed hexadecimal number message to a particular message defined by the sender. Read the Text file. It contains Patient's information and Converted character into integer values.

Embedding the Watermark in NROI Steps

1. Read Image into MATLAB environment.
2. Convert it into Gray Scale Image.
3. Separate ROI and NROI using the Cropping Tool.
4. Read Diagnosis Report.
5. Generate watermark by combining step 3 and 4.
6. Put the integer form of concatenated character string data into an array called TABLE.
7. Scan the host image from TABLE and match for minimum difference match in NROI.
8. Confirm its location in a Secret Key array.

9. Update the Encrypted image array according to this newly found pixel and update the secret key.
10. The Watermarked signal image will be produced.

Extraction Process

- Load the Watermarked Image
- Extract the pixels by using the secret key in the sequence provided by secret key and put it in an array.
- Decrypt the extracted watermark.
- Compute the MAC code
- Compare the extracted hashes to the computed hash.
- If both are same, then received image is authentic.
- If both are not same, then received image is unauthentic.

To evaluate the performance DICOM image of brain of patient was used. Fragile Data Hiding Technique preserves the record of Medical Image through embedding the medical diagnosis report and other records. This approach lets in the storing and transmission of Electronic Patient Record beside with image authentication codes. The original image can be recovered perfectly. The scheme is good at authentication.

D. **C. Deepak Naidu et. al [*4*]** have presented a new algorithm to combine LSB(Least Significant Bit) algorithm with Blowfish algorithm. This is also known as combination of Steganography and Cryptography. Blowfish Algorithm is used to encipher and decipher of the image. LSB Algorithm is used to embed the message into the image. This method consists of three phases. There are Image Steganography, Cryptography and Decryption.

Image Steganography - LSB Algorithm.

The inputted image and the cover image are both covered into their binary equivalents. Each bit of the message is embedded into each pixel's LSB. This method keeps till all the bits of the message are embedded into the cover image. Then acquiring the Stego-Image.

Cryptography - Blowfish Algorithm.

Blowfish is a symmetric block cipher. It has a P-array and S-boxes. The P-array has 18 32-bit boxes such as P1,P2,P3,....,P18. S-boxes has 4 32-bit arrays such as S1,S2,S3,S4 with 256 entries each. This algorithm have 16 rounds.

Decryption

Encrypted image first decrypted using the Blowfish algorithm and then the hidden message can be obtained from the Stego-Image.

This paper mainly concentrates on the confidentiality of patient information during the transfer of Medical Images over the Internet. This algorithm is more efficient than many other algorithms. This method offers High quality images and the MSE (Mean Square Error) value is very less.

E. **A. Umamageshwari et.al [*5*]** affords a Novel Algorithms AHF (Additive Hash Function) and RSA. DS (Digital Signature) is used right here to attain high Confidentiality and Authentication. First, using JPEG2000 Medical Image is compressed. Then shared through open network.

JPEG2000 Image Compression : Four Steps in this process are the following

1. Pre-processing
2. Transformation
3. Quantization
4. Entropy Encoding

- **Pre-processing :** Input Medical Image is decomposed into components of most of 256. These additives are decomposed into rectangular tiles.
- **Transformation :** DWT(Discrete Wavelet Transform) used in JPEG2000. After pre-processing, each and every tile is decomposed into special resolution tiers. Resolution tiers are made from sub bands of coefficients.
- **Quantization :** Sub bands of coefficients are quantized. Also sub bands of coefficients are accrued as blocks.
- **Entropy Encoding :** Bit planes of the coefficients in code block are entropy encoded. ROI can be coded at a better pleasant than the historical past.

The Input image is an MRI image of size 512 x 512.

Additive Hash Function (AHF) : This accepts first row of the source image as input. To produce a constant length of output as a hash value (Message Digest), some confusion and diffusion methods applied mathematically. Output of hash value size may be 128 bits.

Procedure of AHF : Convert the image into 512 x 512 pixel. Then take the first row as another table. Divide 512 elements into 4 Divisions namely A1,A2,A3,A4. Each includes 128 elements.

Add Exchange Sets :

B1 = A1 + A3

B2 = A2 + A4

Subtract B1 and B2, M1024 = B2 - B1. Then Divide the M1024 into 8 elements. 16 Elements = 128 bits. c1,c2,c3,c4,c5,c6,c7,c8 are 8 elements.

Add Exchange values

M1 = c1 + c5 M2 = c2 + c6

M3 = c3 + c7 M4 = c4 + c8

Each value of M has 16 elements = 128 bits.

Add and Subtract interchange values of M.

HF1 = M3 – M1

HF2 = M4 + M2

Add HF1 and HF2 to get the hash value.

AHF = HF1 + HF2

Digital Signature using RSA Approach : Digital Signature is used for Authentication. DS is also used to verify the reliability of the source message. RSA method is used to generate the DS. Additive Hash Function accepts the Medical Image and gives 128 bit output of the hash value. The RSA algorithm is used to encrypt the hash value. Reversible watermarking used to extract the signature. Digital Signature is as compared with Extracted Signature. If they are equal, then original image isn't altered in some point of transmission.

Kerberos Algorithm : It is a secret key encryption scheme used for authentication. Tickets of authentication introduced to Kerberos. Medical professionals make use of a pair of keys for encipher. They used the system that contains no record of the username and password. The system launches a demand for the Kerberos Initial Ticketing Service for requesting a ticket yielding for the user. This request is unauthenticated. The Initial Ticketing Service creates an exclusive session key named Kusession and launch to the user.

Session key form :

| | Ttks.kusession| Ktks.Kusession|Kuser

The user decipher the TGT via his/her password as a key. If the decipher succeeds, the user is real.

Kerberos Ticket Form:

{TKT, {request, User ID, Time} Kusession}

where TGT = { Ttks,kusession} Ktks

Kerberos ticket yielding service uses its own secret key (Ktks) to decipher the demand it has expected. The session key (Kusession) deciphers the rest of the demand.

A strict authentication was achieved through Kerberos. This method successfully applied. Additive Hash Function and RSA method solves the dilemma of integrity, reliability and confirmation of Medical Image. A secret key is used for embedding and removal method. It provides further confirmation for Medical Images. It has high security.

F. **P. Antony Raj et.al [6]** have presented the JPEG Lossless algorithm for the purpose of compression and MD5 to compute the image to improve the authenticity hash value. Encryption process using Advanced Classical Cipher to shape the Digital Signature. First, DS and message are watermark. Then it is embedded in Digital image communication images.

Image Compression : Compression needed to avoid a collision between original image, watermark and Digital Signature. In this process, squashed representation of an image sinking the image storage and transmission requirements. Here, the compress Medical image before embedding JPEG Lossless using the DWT, so no need to block the image.

Digital Signature : Digital Signature computed using MD5 and ACC. Input Medical Image uses DS to verify the authentication. MD5 algorithm used to generate DS.

MD5 Algorithm : First accepts the input of any length and gives 128 bit stable output as the hash value. The hash value of the Medical Image is encrypted using ACC Algorithm. Patient details, Disease details and Digital Signature grouped as watermark. Sender side, using Reversible watermarking, watermark is fixed inside the image. Receiver side, Digital Signature and Patient, Disease details extracted from the image. The hash value of the input image is calculated.

Kerberos : Firewalls make a risky assumption that the attacker is coming from the outside for attacks frequently. Kerberos assumes that network connections are the weak link in network security. Using ACC, find the DS. Then the DS and extracted signature is

compared. If two signatures are equal, then no fluctuate in the image through transmission.
Authentication can be achieved from Web servers and Kerberos Technique. Secret key used for both Embedding and Extraction methods. It produces substantiation to Medical Images.

G. **Boukhatem Mohammed Belkaid [*7*]** presents a new Encryption method called as Hybrid Encryption for Secure transmission of Medical images. Encipher is done using AES - Advanced Encryption Standard and RSA - Rivest, Shamir and Leonard Adleman. AES is used for Data privacy. RSA is used for verification. AES is based on Substitution-Permutation network. RSA is a Public Key Cryptosystem. This is broadly used to protecting data transmitted. Here, Encryption key is public and Decryption key is set aside secret. Encryption generates a exclusive password to each newfangled session of encryption.

AES Algorithm : AES is also called as Rijndael. Substitution – Permutation network grouping is AES. It has a permanent block size of 128 bits and a key size of 128, 192 or 256 bits. Four steps in this algorithm are Substitute bytes, Shift Rows, MixColumns and AddRoundKey.

Block Cipher Operation : In Cryptography, mode of operation is an algorithm that uses a block cipher. A block cipher is appropriate for the safe communication of groups of bits called a block. Modes of operation is used for enhancing the Cryptographic algorithms. Five modes of operations are used are ECB(Electronic Code Book), CFB(Cipher Feedback), CBC(Cipher Block Chaining)and Counter(CTR). These modes are utilize with symmetric block cipher that is Triple DES and AES.

RSA Algorithm : RSA(Rivest Shamir Adleman) developed in 1977. RSA created by Ron Rivest, Adi Shamir and Leonard Adleman at MIT. The calligraphy RSA are the first letter of their surnames. It is a Public Key Cryptosystem. It is used for sheltered data broadcast. Here, Encryption Key is public. Decryption Key is set aside Secret. Keys based on two big prime numbers. The sender encrypts images using RSA algorithm. A public and private key ($Pub_E(b_x,n_x)$, $Priv_R(u_x,n_x)$) are used in emission. In reception, the public and private key ($Pub_R(b_y,n_y)$, $Priv_R(u_y,n_y)$) are used. The Sender encipher image using the key K with the RSA. The private key of the $Priv_E$ to get a signed key K' such that : $K' = K^{ux} \bmod(n_x)$. K' is encipher next time using the RSA public key. Receiver make the key K". $K'' = K'^{by} \bmod(n_y)$.

AES technique reveals good characteristics by declining the correlation of adjacent pixels. Integrity is guaranteed by the correlation between adjacent pixels in the image. Several parameters used for various tests for analysis.

H. **Amarit M*ambutdee et.al [8]*** proposes a new method of application to Medical Image Encryption and Watermarking to store Patient information using Scrambling Algorithm. Patient information is hidden. First, the most important detail of Patient will convert into Two-Dimension Barcode ECC200 standard. Then, Patients need to create six digit Password for Secure this image. The Patient's Password will be reused in Watermark Extraction step. For Watermarking, DCT - Discrete Cosine Transform and DWT - Discrete Wavelet Transform applied to block size of 8x8 pixels.

Discrete Wavelet Transform : It is a mathematical algorithm used for explaining the structure of signal by converting signals from time domain to frequency domain. DWT used in many areas like Digital Signal Processing, Image Processing, Image Compression, and also in researching of Digital Watermarking. It produces decomposes the given image into four groups of frequency sub-bands. That four groups are Low Resolution Approximation Component, Horizontal, Vertical and Diagonal. Embedding watermarking in low frequency sub-bands are more robust.

Discrete Cosine Transform : It is a very popular transform function. It is used to alter the signal from the spatial domain to frequency domain. DCT has used in Data Compression and Image Processing. Many researches transform images by DCT then divided into Non-overlapped m x m block.

Arnold Transform : It is a simple chaotic map. It is widely used for Image Scrambling by shifting the position of a pixel instead of change the value. To improve reliability of Scramble, Arnold Transform given a new parameters known as a, b. Here, a, b are real number call parameters. These both numbers are higher than 1 will increase stronger of chaotic.

Two Dimensional Bar Code(Data Matrix Barcode) : It was invented in mid of 1980s. It is used to eliminate the limit of the One-Dimension Barcode for data capacity and size. This is used for error checking and error correction algorithm. This is matrix barcode constructed as a square or rectangular symbol. The size or image depends on the amount of information. Data Matrix Barcode is composed of two separate parts : Finder Pattern and L Finding Pattern. Finding Pattern is used by the scanner to locate the symbol and the encoded data. The solid dark is called the " L Findig Pattern". It is used to determine the size, orientation and distortion of the symbol.

DWT, DCT coefficient values compared in each block for position identification of the embed message in Medical Image. This paper applies Scrambling process to increase high embed capacity with maintaining high PSNR(Peak Signal Noise Ratio value. For Security improvement, unique security key is used for patients.

I**. Li-bo Zhang et.al [9]** have offered a Medical image Encryption and Compression method. This is used for secure transmission of Medical image . New method encipher and compress the Medical Image by Compressive Sensing and Pixel Swapping based Permutation Technique. In Compressive Sensing, Source image is compressed and encrypted by Bernoulli measurement matrix.

CS with Cryptographic Features Embedded : It is worn for Sampling and Compression of signals. Take a Length L and signal S, it is said to be K-sparse if S can be approximated. In Compressive Sensing, the signal is measured through standard samples. Receiver side, Convex Optimization algorithms. Orthogonal Matching Pursuit (OMP) used for reconstruction. Compressive Sensing measurement Matrix uses Optimal Sensing Performance. This method gives Low Complexity and user friendliness.

Pixel Swapping Based Permutation : Medical images are tousled by a two-dimensional area preserving map. All pixels in that image is scanned from Upper Left Corner to Lower Right Corner to construct puzzled image. For shuffling the square image some maps used. There is an Arnold cat map, Standard map and Baker map. For shuffling non-square image, Pixel Swapping based Permutation Strategy(PSP) is urbanized. Here, Pixels of the Plaintext and the Ciphertext are represented commencing Top to bottom and Left to Right. Every pixel in the source image will be altered with other pixel. All pixels are swapping using Pixel Swapping based Permutation Strategy.

Process : First, CS with cryptographic features used to compress the plaintext. This is known as the first level Encryption. Chebyshev map is serving as the secret key. Pixel Swapping based Permutation Strategy is used for image permutation. Quantized dimensions are encrypted through Permutation-Diffusion type Chaotic cipher. This method gives extra security level and quality.

J. **Vinay pandey et.al [10]** presents an algorithm to defend the communication of Medical Images. This work based on Cryptography, Data Hiding and Steganography. Stream Cipher Algorithm is used for Encrypt the input image. Lossless Data Embedding used to Combine the encrypted image with patient information. Steganography is used to entrench image through the private key. Decrypt the image, inverse methods in reverse order to get the original image and patient information. Extract the image before the decryption of the message to remove the noise in Medical Image.

Stream Cipher : It is also called as Flux Ciphering. It is defined as Block cipher. It has a unitary dimension such as 1 bit, 1 byte. Also, it has a patchy length of 1 to 256 bytes. Stream cipher used for their speeds and ability to modify every sign of the original text. The content of the record is perplexed to the right position and XOR operation is applied.

Process : The original image is enciphered through stream cipher. Then, using the Lossless Data Embedding method, Embed the encrypted image with Patient information. Apply Reversible Data Hiding algorithm to eliminate the entrenched data on enciphering image. Apply Steganography in embedded image among the Private Key. Apply the contrary methods in reverse order to get the original image and Patient details. Apply extraction method to eliminate the noise before Decryption. Existing methods have Less security and more noise. Steganography gives more security. The

Reversible Data hiding method used to remove the noise. This method is Fast and Less Noisy Image retrieved.

V. CONCLUSION

In this Paper, I have surveyed various image encryption and decryption techniques. The Security of images is very important today. Many encryption techniques are studied and analyzed to endorse the recital of the encryption methods. In all methods, Original image is embedded and encrypted then send it to the Receiver. Each Algorithm, Method and Technique used are unique. Every day latest encryption technique is evolving. More secure encryption techniques with high rate of security will work out forever. We should find further secured and a reduced amount of noisy medical image.

VI.REFERENCES

[1] Q. N. Natsheh, B. Li, A. G. Gale, "Security of multi-frame DICOM images using XOR encryption approach", International Conference On Medical Imaging Understanding and Analysis 2016.

[2] Vratesh Kumar Kushwaha, K. Anusudha, "ROI Based Double Encryption Approach for Secure Transaction of Medical Images", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol.2, Issue 4, April 2013.

[3] Simranjeet Kau r , Sukhjinder Kaur, Birdevinder Singh, "Data Hiding Technique for Secure Transmission of Medical Images", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163, Volume 1 Issue 8 (September 2014).

[4] C. Deepak Naidu, Srinivas Koppu, V. Madhu Viswanatham, and S.L Aarthy, "Cryptography Based Medical Image Security with LSB Blowfish Algorithms," ARPN Journal of Engineering and Applied Sciences, VOL. 9, NO. 8, AUGUST 2014.

[5] A.Umamageswari, G.R.Suresh , "A New Cryptographic Digital Signature for Secure Medical Image Communication in Telemedicine," International Journal of Computer Applications (0975 – 8887) Volume 86 – No 11, January 2014.

[6] P. Antony raj, Mrs. A. Umamageswari, "Enhancing Security in Medical Image Communication using Digital Signature," International Journal of Computing Communication and Information System(IJCCIS) Vol 6. No.1 – Jan-March 2014 Pp. 29-34.

[7] Boukhatem Mohammed Belkaid, Lahdir Mourad, "Secure Transfer of Medical Images Using Hybrid Encryption",2015.

[8] Amarit Nambutdee, Surapan Airphaiboon, "Medical Image Encryption based on DCT-DWT Domain Combining 2D-DataMatrix Barcode",2015.

[9] Li-bo Zhang, Zhi-liang Zhu, Ben-qiang Yang, Wen-yuan Liu, Hong-feng Zhu and Ming-yu Zou,"Medical Image Encryption and Compression Scheme using compressive Sensing and Pixel Swapping Based Permutation Approach", Research Article, 13 July 2015.

[10] Vinay Pandey, Angad Singh, Manish Shrivastava, " Medical Image Protection by using Cryptography Data Hiding and Steganography ", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459), Volume 2, Issue 1, January 2012.

[11] P. Vidhya Saraswathi, M. Venkatesulu, " A Block Cipher based on Boolean Matrices using Bit level Operations", Proceedings of International Conference on Computer and Information Science, pp 59-63, 4th - 6th June 2014.

[12] P. Vidhya Saraswathi, M. Venkatesulu, "A Block cipher for Multimedia Encryption using Chaotics Maps for Key Generation", Proceedings of International Conference, " Advances in Information Technology and Mobile Computing (AIM-2013)", published by Elsevier Science and Technology,pp.277-282, 26th - 27th April 2013.

[13] P. Vidhya Saraswathi, M. Venkatesulu, "A Block cipher for Multimedia Content Protection with Random Substitution using Binary Tree Traversal", Journal of Computer Science, Vol.8, No 9,pp. 1541-1546, August 2012.

[14] P. Vidhya Saraswathi, M. Venkatesulu, " A Class of Boolean Matrices Possessing Inverses Under XOR and AND Operations", European Journal of Scientific Research", Vol.118, No.1, pp. 108-112, January 2014.

[15] P. Vidhya Saraswathi, M. Venkatesulu, "A Secure image Content Transmission using Discrete chaotic maps", Jokull Journal, Vol.63, No.9, pp.404-418, September 2013.

[16] P. Karthika, P. Vidhya Saraswathi, "A Survey of Content based Video Copy Detection using Big Data", International Journal of Scientific Research in Science and Technology, ICASCT2401 | ICASCT | March-April-2017.