International Journal of Engineering Innovation & Research
Volume 1, Issue 1, ISSN : 2277 – 5668

A Proficient Manner to Transmit a Medical Image Using Triple Enhanced Data Encryption Standard (EHDES) Over Teeming Channel

Ramveer Singh
Associate Professor & Head,
Deptt. of I.T.,
R. K .G. Institute of Technology, Gzb. U.P.(India)
ramveersingh_rana@yahoo.co.in

Deo Brat Ojha
Professor
Deptt. of Mathematics,
Mewar University, Rajasthan (India),
deobratojha@rediffmail.com

***Abstract* — This paper proposed an efficient and effective architecture to transmit a medical image. The proposed arrangement provides the solution of protecting the transmission of medical image. With the security of medical image, we also emphasis on the channel capacity. The combination of Encryption with Triple EHDES and Lossless compression gives the better solution for protection and efficient use of communication channel. If any error occurred during the transmission due to teeming, that also measured and encountered from error correction code.**

***Key Words* — Encryption, EHDES, Compression, Channel Capacity, Error Correction Code.**

I. INTRODUCTION

For secure image transmission, two different approaches have been developed. The first approach is based on content protection through encryption [4], [5]. In this approach, proper decryption of data requires a key. The second approach bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. In the current era the transmission of Image over internet is so much challenging over the internet. In this manner, the better way to transmit the image over internet is encryption. Using the cryptography we secure the image as well as also better utilize the communication channel through compression technique.

Cryptography is a branch of applied mathematics that aims to add security in the cipher of any kind of messages. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document. [6]

We store information in computer system in the form of files. File is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is word wide accepted fact that securing file data is very important, in today's computing environment [3]. There are n numbers of approaches available to persuade image file data security, but due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data [3] and other chaos based encryption application for image, but each one has its own disadvantage, rendering them being less frequently used [1, 2].

In this article, we propose a new technique for secure image transmission of reduced image over teeming channel.

II. PRELIMINARIES

A. Triple EHDES

Triple EHDES uses the cascading or chain of Enhanced Data Encryption Standard (EHDES) [7, 8].

Let EK(P.T.) and DK(P.T.) represent the EHDES encryption and decryption of P.T. using EHDES key K respectively. Each EHDES encryption/decryption operation is a compound operation of EHDES encryption and decryption operations. The following operations are used:

1) EHDES encryption operation: the transformation of a 64-bit block P.T. into a 64-bit block C.T. that is defined as follows:

C.T = EK3(DK2(EK1(P.T.))).

2) EHDES decryption operation: the transformation of a 64-bit block P.T into a 64-bit block C.T. that is defined as follows:

C.T. = DK1(EK2(DK3(P.T.))).

The standard specifies the following keying options for bundle (K1, K2, K3).

1) Keying Option 1: K1, K2 and K3 are independent keys.

2) Keying Option 2: K1 and K2 are independent keys and K3 = K1.

3) Keying Option 3: K1 = K2 = K3.

B. Compression

A compression scheme can be employed what is known as lossless compression on secrete message to increase the amount of hiding secrete data, a scheme that allows the software to exactly reconstruct the original message [9].

The transmission of numerical images often needs an important number of bits. This number is again more consequent when it concerns medical images. If we want to

transmit these images by network, reducing the image size is important. The goal of the compression is to decrease this initial weight. This reduction strongly depends of the used compression method, as well as of the intrinsic nature of the image. Therefore the problem is the following:

1. To compress without lossy, but with low factor compression. If you want to transmit only one image, it is satisfactory. But in the medical area these are often sequences that the doctor waits to emit a diagnostic.

2. To compress with losses with the risk to lose information. The question that puts then is what the relevant information is's to preserve and those that can be neglected without altering the quality of the diagnosis or the analysis. The human visual system is one of the means of appreciation, although subjective and being able to vary from an individual to another. However, this system is still important to judge the possible causes of degradation and the quality of the compression [10].

The SEQUITUR Algorithm [11]

The SEQUITUR algorithm represents a finite sequence as a context free grammar whose language is the singleton set {σ}. It reads symbols one-by-one from the input sequence and restructures the rules of the grammar to maintain the following invariants:

(A) No pair of adjacent symbols appear more than once in the grammar, and

(B) Every rule (except the rule defining the start symbol) is used more than once. To intuitively understand the algorithm, we briefly describe how it works on a sequence 123123. As usual, we use capital letters to denote non-terminal symbols. After reading the first four symbols of the sequence 123123, the grammar consists of the single production rule S ➔ 1, 2, 3, 1 where S is the start symbol. On reading the fifth symbol, it becomes S ➔ 1, 2, 3, 1, 2 Since the adjacent symbols 1, 2 appear twice in this rule (violating the first invariant), SEQUITUR introduces a non-terminal A to get

S ➔ A, 3,A
A ➔1, 2

Note that here the rule defining non-terminal A is used twice. Finally, on reading the last symbol of the sequence 123123 the above grammar becomes

S ➔ A, 3, A, 3
A ➔ 1, 2

This grammar needs to be restructured since the symbols A, 3 appear twice. SEQUITUR introduces another non-terminal to solve the problem. We get the rules

S ➔ B,B
B ➔ A 3
A➔ 1 2

However, now the rule defining non-terminal A is used only once. So, this rule is eliminated to produce the final result.

S ➔ B, B
B ➔ 1, 2, 3

Note that the above grammar accepts only the sequence 123123.

C. Error Correction Code

A metric space is a set C with a distance function dist : $C \times C \to R^{+} = [0, \infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points)[12,13].

Definition : Let $C\{0,1\}^{n}$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by

$$dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right| \qquad c_i, c_j \in C$$

This is known as Hamming distance [14].

Definition : An error correction function f for a code C is defined as $f(c_i) = \{c_j / dist(c_i, c_j) \text{ is the minimum, over } C - \{c_i\}\}$. Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i [12].

Definition : The measurement of nearness between two code words c and c' is defined by $\text{nearness}\ (c, c') = dist(c, c') / n$, it is obvious that $0 \le \text{nearness}\ (c, c') \le 1$ [14].

Definition : The fuzzy membership function for a code word c' to be equal to a given c is defined as[14]

$FUZZ(c') = 0$ if $\text{nearness}(c, c') = z \le z_0 < 1$

$= z$ otherwise

III. OUR SCHEME

1. Input Image: Input an image, which has been transmit over teeming channel.

Input Medical Image ⟶

2. Generating $n \times n$ blocks: In RGB space the image is split up into red, blue and green images. The image is then divided into 8×8 blocks of pixels and accordingly the image of $w \times h$ pixels will contain $W \times H$ blocks. Where, $W = w/8, H = h/8$.

Medical Image ⟶

3. Discrete Cosine Transforms (DCT): All values are level shifted by subtracting 128 from each value. The Forward Discrete Cosine Transform of the block is then computed. The mathematical formula for calculating the DCT is:

$$T(u,v) = \sum_{x=0}^{n} \sum_{y=0}^{n} f(x,y), g(x,y,u,v)$$

Where,

$$g(x, y, u, v)$$

$$\frac{1}{4}\alpha(u)\alpha(v)\cos\left[\frac{(2x+1)u\pi}{2n}\right]\cos\left[\frac{(2y+1)v\pi}{2n}\right]$$

Where

$$\alpha(u) =$$

$$\begin{cases} \frac{1}{\sqrt{2}} \text{..... } for.u = 0 \\ 1 \text{..... } for.u = 1,2,...N-1 \end{cases}$$

4. Quantization: Quantization is the step where the most of the compression takes place. DCT really does not compress the image, as it is almost lossless. Quantization makes use of the fact that, the high frequency components are less important than the low frequency components. The Quantization output is

$$Q_{DCT} = round\left(\frac{T(u,v)}{Z(u,v)}\right)$$

The $Z(u, v)$ matrix could be anything, but the JPEG committee suggests some matrices which work well with image compression.

5. Compression using SEQUITUR:

After quantization, the scheme uses a filter to pass only the string of non-zero coefficients. By the end of this process we will have a list of non-zero tokens for each block preceded by their count. DCT based image compression using blocks of size 8x8 is considered. After this, the quantization of DCT coefficients of image blocks is carried out. The SEQUITER compression is then applied to the quantized DCT coefficients.

6. Encryption using Triple EHDES:

In this step of our manner, we use the cascading of EHDES or three times. In single EHDES, Message breaks in 64 Bit n blocks of plain text.

IV. Security Analysis

The Compression scheme used in this paper is lossless and provide less compression ratio, which is main requirement. We are transmitting a medical image here, then we have not compromise about the originality of Image.

Cryptographic scheme is always based on key and the strength of scheme is depend on breaking of key. EHDES uses 56 bit, Cracking 56- bit algorithm with a single key search might take around a week on a very powerful computer.

But Now in EHDES,

At time t, the generated key is, K_{newX}

At time t + 1, the generated key is $K_{newY,}$

And At time t + n, the generated key is K_{newZ}

Here,

$$K_{newX} \neq K_{newY} \neq K_{newZ}$$

It might be possible that $K_{newX,}$ $K_{newY,}$ K_{newZ} are equal if and only if the generated no. N_{RNG} at time t, t + 1, t + n are same. Here, we use triple EHDES, which make the system three times more strong and secure.

The encoded message *c* is transmitted. It is possible that during the transmission some bits of c are changed. The receiver receives the incorrect message *c'*. He calculates that *dist*(*x, y*) is minimum. If the error is not too big, that is $dist(c,c) < \frac{1}{2d}$, where d is the minimum distance of any two distinct code words, then *c'* is equal to the original message *c*.

Conclusion

Section 3 and 4 itself shows the strength and security of A Proficient Manner to Transmit a Medical Image Using Triple Enhanced Data Encryption Standard (EHDES) over teeming Channel. The attraction and usability of this manner is, it's also having the feature of error detection and correction using error correction code.

References

[1] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.

[2] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, Vol. 3 No. 4, April 2008.

[3] Rajesh Kumar Pal and Indranil Sengupta, "Enhancing File Data Security In Linux Operating System by Integrating Secure File System" June 2009.

[4] G. Lo-varco,W. Puech, and M. Dumas. "Dct-based watermarking method using error correction codes", In ICAPR'03, International Conference on Advances in Pattern Recognition, Calcutta, India, pages 347–350, 2003.

[5] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. "Confidential storage and transmission of medical image data", Computers in Biology and Medicine, 33:277–292, 2003.

[6] Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and Rudinei Goularte, "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control" , University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department, Maringa, PR, Brazil.

[7] Ramveer Singh , Awakash Mishra and D.B.Ojha "An Instinctive Approach for Secure Communication – Enhanced Data Encryption Standard (EHDES)" International journal of computer science and Information technology, Vol. 1 (4), 2010, 264-267.

[8] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati Garg "An Innovative Approach to Enhance the Security of

Data Encryption Scheme" International Journal of Computer Theory and Engineering, Vol. 2,No. 3, June, 2010,1793-8201.

[9] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan.

[10] Borie J., Puech W., and Dumas M., "Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.

[11] N.Walkinshaw, S.Afshan, P.McMinn "Using Compression Algorithms to Support the Comprehension of Program Traces" Proceedings of the International Workshop on Dynamic Analysis (WODA 2010) Trento, Italy, July 2010.

[12] J.P.Pandey, D.B.Ojha, Ajay Sharma, "Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem", in Journal of Applied and Theoretical Information Technology, (pp 16-19) Vol. 9, No. 1, Nov. 2009.

[13] V.Pless, "Introduction to theory of Error Correcting Codes", Wiley , New York 1982.

[14] A.A.Al-saggaf, H.S.Acharya, "A Fuzzy Commitment Scheme" IEEE International Conference on Advances in Computer Vision and Information Technology 28-30 November 2007 – India

AUTHOR'S PROFILE

Ramveer Singh, Bachelor of Engineering from Dr. B.R. Ambedkar University, Agra (U.P.), INDIA in 2003. Master of Technology from V.M.R.F. Deemed University, Salem (T.N.), INDIA in 2007. Ph.D. (Submitted) from Singhania University, Jhunjhunu, Rajsthan, INDIA. The major field of study is Cryptography and network security. He has more than nine year experience in teaching and research. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network security. Mr. Singh is the life-time member of Computer Society of India and Computer Science Teacher Association.

Dr. Deo Brat Ojha, Ph.D. from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varanasi (U.P.), INDIA in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. . He is working as a Professor at Mewar University, Rajasthan, INDIA. He is the author/co-author of more than 50 publications in International/National journals and conferences.