ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Effective Scheme to Transmit Medical Image with Double EHDES

Mr. Ramveer Singh
R. K .G. Institute of Technology, Ghaziabad (U.P.) India
& Research Scholar Singhania University, jhunjhunu
Rajsthan, India
ramveersingh_rana@yahoo.co.in.

Awakash Mishra
Department of M.C.A, Raj Kumar Goel Engineering
College, Ghaziabad, (U.P.) India
&Research Scholar Singhania University, Jhunjhunu,
Rajsthan, India
awakashmishra@gmail.com

Deo Brat Ojha*
Department of mathematics, R. K. G. Institute of Technology
Ghaziabad, (U.P.) India
deobratojha@rediffmail.com

Abstract: In the field of medical and science, the image transmission plays a vital and more vital role for enhancement in the relative area. For improvement in various fields like Medical, Defence, Banking Sector etc., we introduce an innovative and effective scheme to transmit data with help of Compression and Encryption, which is either in the form of Image or in other form. Cryptography is a tool to provide high level security and Compression is a procedure to reduce the size of Image. We use EHDES for more security and Sequitur for lossless compression.

Keywords: Image, Enhance Data Encryption Standard (EHDES), Lossless Compression, Sequitur, Secure Transmission

I. INTRODUCTION

Image transmission increases rapidly over the internet. Two different approaches of technologies have been developed for this purpose. The first approach is based on content protection through encryption [1], [2]. 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 utilise the communication channel through compression technique.

Cryptography is a branch of applied mathematics that aims to add security in the ciphers 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. [3]

In this current article, we introduced effective and important scheme to transmit an image with high security and reduce size. EHDES, provide us to almost unbreakable security over data and Sequitur provides the lossless compression through dictionary. Two major things must be always on tips

1. Data security 2. Reduce Size

Double EHDES provides two times security to EHDES. And Sequitur generate lossless output with reduce in size.

II. PRELIMINERIES

A. Double EHDES

Double EHDES is an arrangement or cascading of EHDES and its working just like a EHDES but two times. In Enhanced Data Encryption Standard (EHDES) [4, 5,], we breaks block of message and follow these three phases:

1. Key Generation. 2. Encryption. 3. Decryption.

A.1 Key Generation

In this phase, EHDES generates the n different keys ($K_{new1,}$ $K_{new2,}$ K_{new3}..... $K_{new\ n}$) to apply a function F on Initial key k and a random number (N_{RNG}), for every block of message (M_1, M_2, M_3 ..M_n).

A.2. Encryption on Input Data.

Message breaks in 64 Bit n blocks of plain text.

$$\mathbf{M = \{M_1, M_2, M_3,\ldots\ldots\ldots\ldots, M_n\}}$$

Now, we encrypt our message $\{M_1, M_2, M_3,\ldots\ldots\ldots\ldots, M_n\}$ blocks by each new generated key $K_{new1,}$ $K_{new2,}$ K_{new3}..... $K_{new\ n}$.

A.3. Decryption on Input Cipher

Decryption is the reverse process of encryption.

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 [6].

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 [7].

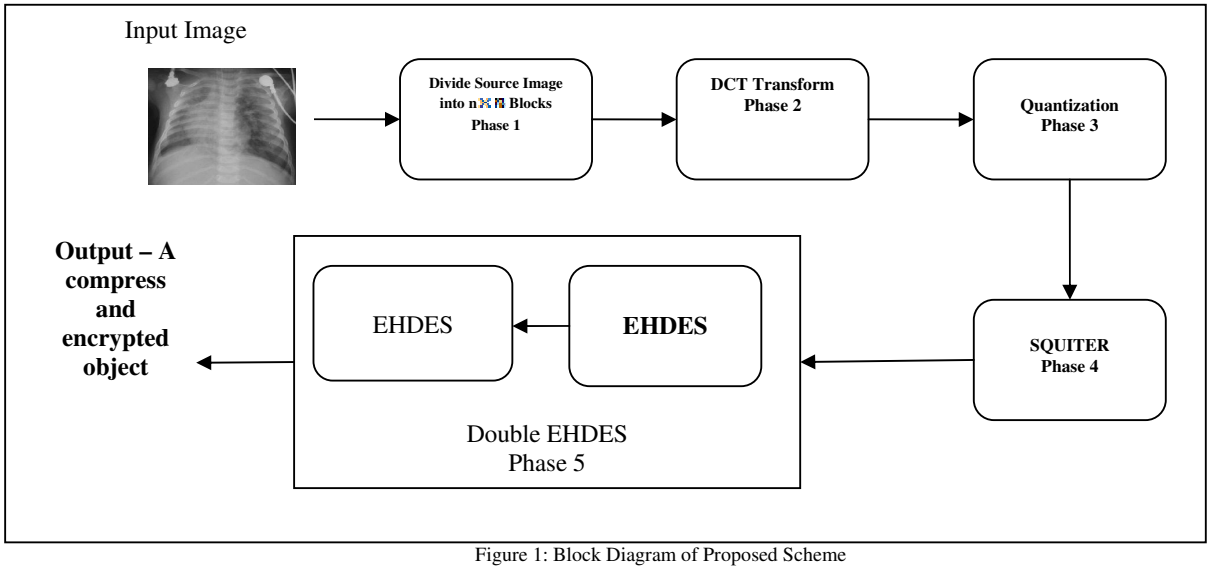

Figure 1: Block Diagram of Proposed Scheme

The SEQUITUR Algorithm [8]: 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.

III OUR SCHEME

Input an image and follows these phases:

Phase 1: 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, $W = w/8, H = h/8$.

Phase 2: 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 $\alpha(u) = \begin{cases} \frac{1}{\sqrt{2}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots for.\, u = 0 \\ 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots for.\, u = 1,2,\ldots.N-1 \end{cases}$

Phase 3: 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.

Phase 4: 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.

Phase 5: Encryption using Double EHDES: In encryption phase, We uses the cascading of EHDES and generate encrypted data.

IV SECURITY ANALYSIS

We verified that the compression ratio of Sequitur outperforms Gzip as well as Compress. On the other hand, however, the compression and decompression are very slow compared to Gzip and Compress, because Sequitur utilizes the arithmetic coding that is time consuming, and the program might not be fully optimized.

The compression achieved in this approach is evaluated based on the overall compression ratio (CR) which is defined as:

$$\text{C.R.} = \frac{size\ of\ the\ input\ or\ original\ image}{size of\ output\ or\ compressed\ image}$$

Cryptographic scheme EHDES itself an effective approach to achieve the result. When we implement EHDES two times, it's provided two times more security and complexity and also barricade to other user for Meet-in-Middle attack.

V. CONCLUSION

Our scheme provides a innovative concept to transmit an image over internet. In the current era security of transmitted image is very much crucial. With memorise this security we also worry about channel capacity, For the sake of capacity & security, we implement compression before encryption.

VI. REFERENCES

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

[2] 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.

[3] 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.

[4] 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, Sep. 2010 (Paper Acepted)

[5] 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

[6.] 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

[7] 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.

[8]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.

AUTHORS

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. Persuing Ph.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. The major field of study is Cryptography and network security. He has more than eight year experience in teaching and research as ASSOCIATE PROFESSOR. 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.

Awakash Mishra, Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), INDIA in 2007. Persuing Ph.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. He has more than four year experience in teaching and research as LECTURER. He is working at Raj Kumar Goel Engineering College, Ghaziabad (U.P.), INDIA. The current research area is Symmetric Key Cryptography.

Dr. Deo Brat Ojha, Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (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 Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. He is the author/co-author of more than 50 publications in International/National journals and conferences.