Volume 1, No. 2, September 2010
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

An Approach to Compress & Secure Image Transmission over a Noisy Channel

Ramveer Singh[1] ,Awakash Mishra[2], Sanjive Tyagi [3]and Deo Brat Ojha[4]
[1] Mr. Ramveer Singh, R. K .G. Institute of Technology, Gzb. U.P.(India)
& Research Scholar Singhania University, jhunjhunu, Rajsthan, INDIA.
e-mail: ramveersingh_rana@yahoo.co.in. .
[2](Research Scholar Singhania University, Jhunjhunu, Rajsthan)
Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P.,INDIA
e-mail: awakashmishra@gmail.com
[3] Mr.Sanjive Tyagi, Radha Govind Engineering College, Meerut, U.P.(India),
(Research Scholar Singhania University, jhunjhunu, Rajsthan)
E-mail: tosanjive@gmail.com
[4] Dr. Deo Brat Ojha, Deptt. Of mathematics, R. K. G. Institute of Technology, Gzb., U.P.(India),
e-mail: deobratojha@rediffmail.com

Abstract:In our day to day life, requires more secure transmission whereas the transmission channel is too noisy. Transmission image in various field i.e. medical field (Telemedicine) with complete efficiency for saving human life, secrecy of communication between secret agents and their relative government, to maintain the confidentiality in military operations, etc. In our approach, we introduced a new scheme to transmit an image over noisy transmission channel. Our approach is suitable combination of cryptography and compression with removal of transmission error. Cryptography provides secure transmission, Compression increases the capacity of transmission channel and Fuzzy is used for error which gets during transmission of image.

Key Words: Image, Compression, Encryption, Decryption, Secure Communication, Error Detection & Correction.

INTRODUCTION

The amount of image has increased rapidly on the Internet. Image Two different approach of technologies have been developed for this purpose. The first approach is based on content protection through encryption [1], [2].
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 addition, to avoid sending files of the enormous size, 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 [4].
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 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 [5].
In this scheme, we introduce effective approach to transmit an secure and compressed image over noisy transmission channel.

PRELIMINERIES

Enhanced Data Encryption Standard (EHDES)

Enhanced Data Encryption Standard (EHDES) [6] , [7], uses the block of data and a symmetric key. As traditional Data Encryption Standard (DES), it also breaks data string into 64-Bit blocks and follows three phases:
1. Key Generation. 2. Encryption on Input Data. 3. Decryption on Input Cipher.

Key Generation

In this phase of EHDES moderate the initial 56 Bit key using Random Number Generator (RNG) for every block of message (M_1, M_2, $M_{3\ ...Mn}$). The new generated 56 Bit keys ($K_{new1,}$ $K_{new2,}$ $K_{new3.....}$ $K_{new\ n.}$ For every M_i EHDES

generate $K_{new\ i}$, applying F on generated random number (N_{RNG}) and the initial key K.

Encryption on Input Data

Message breaks in 64 Bit n blocks of plain text.

M = {M_1, M_2, M_3,.. M_n}

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

C={C_1, C_2, C_3,..... C_n}.

Decryption on Input Cipher

Decryption is the reverse process of encryption and also used the same key which is used in encryption.

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:

- no pair of adjacent symbols appear more than once in the grammar, and
- 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.

Block Error Rate

The application's block error rate can be computed from the bit error rate using the following equation [10]:

$$BLER = \binom{N}{E} * P^E * (1-P)^{N-E}$$

Where:

N is the number of bits in a block, E is the number of errors in a block and p is the probability of a bit error (bit error rate)

This equation basically states that the block error rate is dependent on three factors:

• The number of statistical combinations of failing bit patterns (E combinations of N),

• The probability of E errors occurring (*p* raised to the E power), and

• The probability of N-E correct data bits ((1-*p*) raised to the N-E power).

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)[11,12].

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 [13].

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 [11].

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 $0 \le \text{nearness}\ (c, c') \le 1$ [13].

Definition : The fuzzy membership function for a codeword c' to be equal to a given c is defined as[13]

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

OUR SCHEME

A complete transmission process includes the following steps:

Step 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, $W = w/8, H = h/8$.

Step 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

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

Step 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

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

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

Step 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.

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

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

Step 5: Encryption using EHDES: In encryption phase, EHDES take output of compression phase as a message block M_n and a new generated key $K_{new\,n}$ implement encryption process as per traditional DES.

In this process, New key is also make 16 different key for every round of EHDES using shifting property as per traditional DES. For every block of message M, new key $K_{new\,n}$ makes a new key block for every round of DES to implement in the encryption process.

Decryption Process is the inverse step of encryption process. In decryption, we also use the same key which is used in encryption.

$$Ci = E_{K_{new\,n}}\{mi\} \text{ and } mi = D_{K_{new\,n)}}\{Ci\},$$

where $1 \le i \le n$.

Step 6, 7: Error Correction:

Receiver check that $dist(t(c)c') > 0$, he will realize that there is an error occurs during the transmission. Receiver apply the error correction function f to c' : $f(c)$.

Then receiver will compute nearness

$(t(c), f(c')) = dist(t(c)f(c'))/n$

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

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. From our view point of compressed pattern matching, compression time is not a serious matter, while the decompression time is critical. In the original program of Sequitur, decompression routine borrows the same data structures, such as doubly linked list, that are unnecessary for decompression only. Thus we simply rewrote the decompression routine using a standard array.

Cryptographic scheme strength is often described by the bit length of encryption key. The more bits in the key, the harder it is to decrypt data simply by all possible key. DES uses 56 bit, Cracking 56- bit algorithm with a single key search might take around a week on a very powerful computer.

Now,

At time t, the generated key is, $K_{new\,X}$

At time t + 1, the generated key is $K_{new\,Y}$,

And At time t + n, the generated key is $K_{new\,Z}$

Here,

$$K_{new\,X} \neq K_{new\,Y} \neq K_{new\,Z}$$

It might be possible that $K_{new\,X}$, $K_{new\,Y}$, $K_{new\,Z}$ are equal if and only if the generated no. N_{RNG} at time t, t + 1, t + n are same.

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 $\text{dist}(c,c') < \frac{1}{2d}$, where d is the minimum distance of any two distinct code words, then *c'* is equal to the original message *c*.

CONCLUSION

Our scheme provides the complete security and compressed form of image, which provide the maximum efficiency to transmission channel. If some error is produced by channel, the fuzzy error correction code remove the error and provide to user more perfect image.

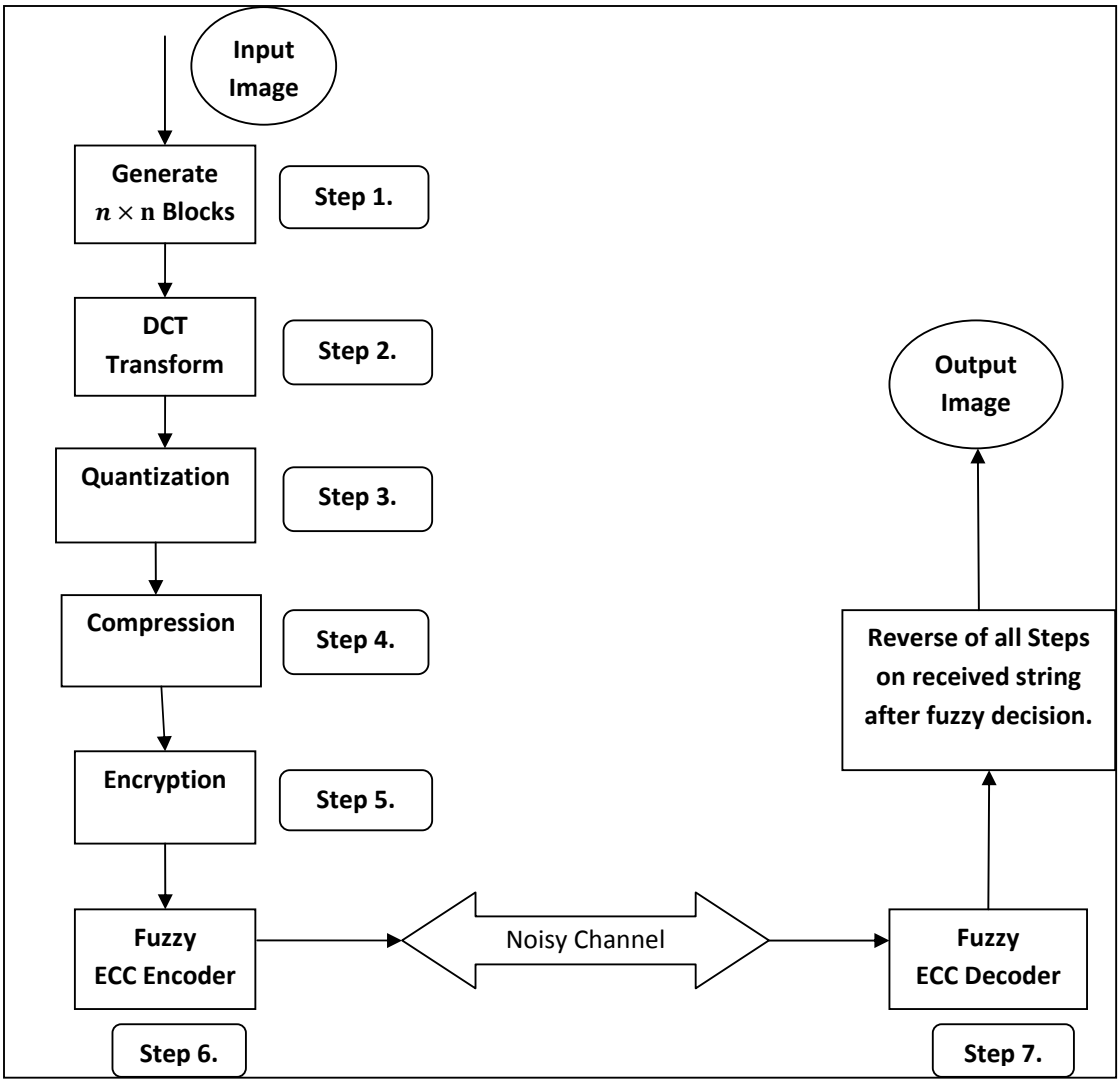

Figure 1: Architecture of Proposed Scheme.

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.] 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

[5] 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.

[6] 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)

[7] 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

[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.

[9]http://www.fcet.staffs.ac.uk/alg1/2004_5/Semester_1/Communications,%20COMMS%20(CE00038-2)/word%20notes/Block%20Error%20Rate.doc

[10] 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.

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

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

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.

Sanjive Tyagi, 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. He has more than ten year experience in teaching and research as Assistant professor . He is working at Radha Govind Engineering College, Meerut (U.P.), INDIA. The current research area is Image hiding using Stegnography.

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