Volume 2, No. 1, January 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

A Proficient mode to Transmit Secure Large Size Data with Authentication & Integrity using Double –EHDES over Teeming Channel

Ramveer Singh*[1], Sanjive Tyagi [2], Awakash Mishra[3], Akshay Tyagi[4], Deo Brat Ojha[5]
[*1]Deptt. of Information Technology, R.K.G.Institute of Technology, Gzb., U.P.(India),
(Research Scholar Singhania University, jhunjhunu, Rajsthan)
E-mail: ramveersingh_rana@yahoo.co.in
[2]Deptt. of M.C.A., Radha Govind Engineering College, Meerut, U.P. (India),
(Research Scholar Singhania University, jhunjhunu, Rajsthan)
E-mail: tosanjive@gmail.com
[3](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
[4](Research Scholar Mewar University, Chittorgarh, Rajasthan))
Gradute School of Business & Administration, Greater Noida, U.P., INDIA
e-mail: akshaytyagi@airtelmail.in
[5]Deptt. Of mathematics, R. K. G. Institute of Technology, Gzb., U.P.(India),
e-mail: deobratojha@rediffmail.com

Abstract – In this paper, we presents a Proficient mode to Transmit Secure Large Size Data with Authentication & Integrity using Double – EHDES over Teeming Channel. This approach really enhances the capability and maximum utilization of busy channel. A complete transmission is always based upon correctness and delivery on time and the massage transmission is too much sensitive and crucial. In this paper, we establish the complete arrangement of combination of encryption and compression with double EHDES while transmitting over media.A lossless compression provides us integrity. Fuzzy error correction provides error less message over noisy channel.
Keywords— Double - EHDES, Cryptography, Stegnography, Compression, Image File, Error Correction Code.

INTRODUCTION

Steganalysis is a technology which determines the presence of a hidden message or image in cover image and attempt to disclose the actual contents of this message [1].A more erudite method of steganography is by merging the two techniques to produce more security to secure data transmission such that if intruders detect the presence of data even then message cannot be decode without the knowledge of key.

The most common stegno method is the LSB approach, or Least Significant Bit. As we know digital pixels are represented by three colors: red, green and blue. These colors together form digital pictures or video. Each color of every pixel requires 1 byte or 8 bits of information. Since the first bit is the "least significant" or carries the least amount of importance in the byte, this steganographic technique chooses to overwrite the first bit of successive bytes until the entire secret message is embedded into the original source file, or the cover data. Since we have only modified the least significant bits of a portion of the source file, the human eye should not be able to detect the degradation in the picture or video [2].

PRELIMINARIES

1. Stegnography:

Steganography is a technique used to embed secret information into non-secret information, preventing the message from being detected by non-authorized people.[3]

The purpose of steganography is to hide the very presence of communication by embedding messages into innocuous-looking cover objects, such as digital images. To accommodate a secret message, the original cover image is slightly modified by the embedding algorithm to obtain the stego image. The embedding process usually

incorporates a secret stego-key that governs the embedding process and it is also needed for the extraction of the hidden message [4].

There are three basic views behind hiding information. The first is capacity, which is the amount of information that can be embedded within the cover file. An information-hiding algorithm has to be able to compactly store a message within a file. Next is security, which refers to how a third-party can detect

hidden information within a file. Intuitively, if a message is to be hidden, an ideal algorithm would store information in a way that was very hard to notice. High security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too. Various encryption techniques like cryptography, digital watermarking, steganography etc have already been introduced in attempt to address these growing concerns [5].

Steganography have four application areas:

- Copyright Protection. It has security, invisibility and robustness requirements. Watermark techniques fit in this area.
- Authentication. It has security and invisibility requirements. Digital signature fits in this area.
- Secret and Invisible Communication. It has requirements for security, invisibility and insertion of high volumes of secret data. [6]

2. Cryptography

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. [7]

DEFINITION:

A cryptosystem is a five -tuple (M, C, K, E, D), where the following conditions are satisfied:

1. M is a finite set of possible plain texts.
2. C is a finite set of possible ciphertexts.
3. K, the keyspace, is a finite set of possible keys.
4. For each K ε k, there is an encryption rule eK ε E. and a corresponding decryption rule dK ε D. Each eK : M →C and dK : C → M are functions such that dK(eK(x)) = x for every plaintext x ε M.

The main property is property 4. It says that if a plaintext x is encrypted using eK, and the resulting ciphertext is subsequently decrypted using dK, then the original plaintext x results.

2.1 EHDES

In Enhanced Data Encryption Standard (EHDES), we use the block ciphering of data and a symmetric key. As traditional Data Encryption Standard (DES), we also break our data into 64-Bit blocks and use a symmetric key of 56-Bit.

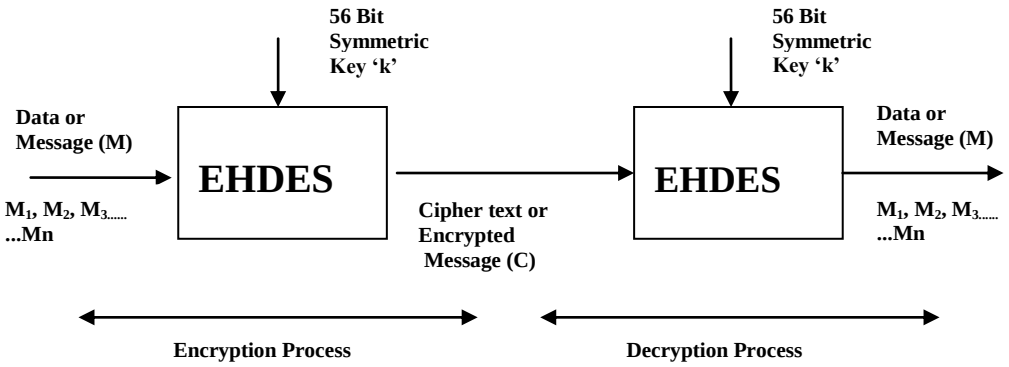

Figure 2: Encryption and Decryption process of EHDES.

3.1 Enhanced Data Encryption Standard (EHDES)

Enhanced Data Encryption Standard (EHDES) having three phases.

1. Key Generation. 2. Encryption on Input Data. 3. Decryption on Input Cipher.

3.1.1 Key Generation

In this phase of EHDES, We 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 ($K_{new1,}$ $K_{new2,}$ $K_{new3.....}$ $K_{new\ n}$) from initial key K is used for encryption and decryption for each block of data. For new keys, we generate a random number and implement a function F on generated random number (N_{RNG}) and the initial key K.

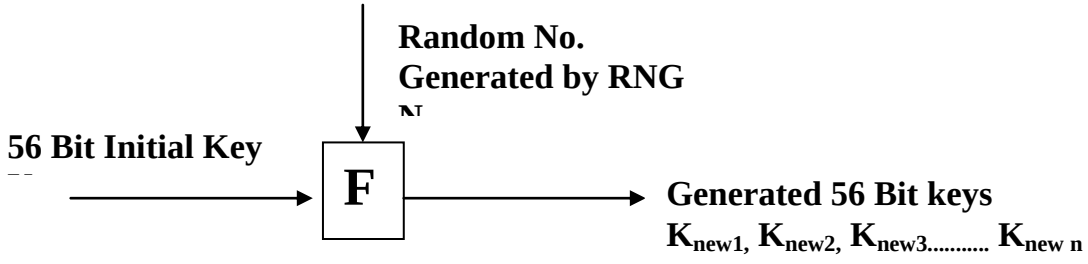

Figure 3: Process of new generated key ($K_{new\ i}$) of EHDES.

3.1.2. Encryption on Input Data.

As we know Data Encryption Standard (DES) is based on block cipher scheme. 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,....., M_n} blocks by each new generated key K_{new1}, K_{new2}, K_{new3}..... $K_{new\ n}$.

3.1.3. Decryption on Input Cipher

Decryption is the reverse process of encryption. For decryption, we also used the same key which is used in encryption. On the receiver side, the user also generate the same new key $K_{new\ i}$ for each block of cipher and generate plain text through decryption process of data encryption standard.

2.1.1 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) [8, 9], we breaks block of message and follow these three phases:

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

1). Key Generation

In this phase, EHDES generates the n different keys (Knew1, Knew2, Knew3..... Knew n) to apply a function F on Initial key k and a random number (NRNG), for every block of message (M1, M2, M3 ...Mn).

2). Encryption on Input Data.

Message breaks in 64 Bit n blocks of plain text.

M = {M1, M2, M3,....., Mn}

Now, we encrypt our message {M1, M2, M3,....., Mn} blocks by each new generated key Knew1, Knew2, Knew3..... Knew n.

3). Decryption on Input Cipher

Decryption is the reverse process of encryption.

3. Data 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 [10].

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 [11].

3.1 The SEQUITUR Algorithm [12]

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.

4. 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)[13,14].

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 [15].

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 [13].

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 $0 \le \text{nearness } (c, c') \le 1$ [15].

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 APPROACH

In our new concept, we encrypt the original text message letter by letter applying a function, which involves certain mathematical operation using corresponding letters and also numbers from the original image, then we use highly secure encryption using Double - EHDES algorithm to encrypt the message. For encryption we need to use secret key for plain text M and Double - EHDES encryption function.

Cipher Text: $C = E_{K(EHDES)}$(Message).

Then using sequitur compression algorithm on secrete data file (c) to hide a large amount of data with high security.

Then Hide compressed and encrypted text into cover image using Stegnography algorithm i.e List Significant Bit (LSB) coding is the way to embed information in cover image file. In this LSB technique is applied on compressed encrypted message. It is really appreciable method to provide high security to the high confidential image.

The proposed method is enhanced or characterized by robustness, larger amount of secrete data, less time complexity and especially high security.

Proposed work deals with the security of text message by applying symmetric key cryptography algorithm Double - EHDES in which we use generated secret key which are calculated using Double - EHDES key generation process. Secret key is used at both sender side and receiver side. Secret key are always different using Double - EHDES algorithm with modification that a mathematical function F. This function using a value depends on the decimal value of the R array of each pixel of cover image. The first letter corresponding to the first pixel and next to the second pixel and so on .

A mathematical function F is using R array of each pixel of cover image and initial key K for generating the Secret key $K_{new\ i}$.The encrypted code is taken digit by digit. This approach constitutes the phase one security in our work.

Now in the second phase of work, we have used Sequitur loss less compression technique to compress the encrypted text so that we can hide large amount of data in cover image.

In next phase, we have introduced the hiding of encrypted and compressed text file into any cover image.

In our work secret key are always different because we are generating randomly number based on the confidential message text and original cover image. This method is a unique to generate random number such that no one can guess the random number to crack the secret key.

A. Algorithm for encrypting the confidential message

Step 1:
Convert the text to number system, which are ASCII number of character.

Step 2:
A mathematical function fis used which gives the number of randomnumbers below given number say R.

Step 3:
Here, the value of R depends on the decimal value of character of cipher text.

Step 4:
The F function is then applied on the random number R by checking the parity of decimal value of character of cipher text.

X =ASCII Converted Character numbers of confidential Message.

R =Decimal value of the R array of the pixels the original cover image.

$K_{new\ i}$ = F(R)=Result value after applying the F function

Step 5:
Now using random number R, generate secret key

Calculate, $K_{new\ i}$ = F(R and K)

Where R is a random number.

Step 6:
Encryption using secret key and Double- EHDES

Plain Text M

Cipher Text: $C = E_{K(EHDES)}(X)$.

B. Algorithm for compress the confidential message

Step:
Perform the lossless compression technique (sequitur) on cipher text to increase the amount of hiding secrete data.

C. Process for convert cover image file

Step 1: Generating n × 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

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

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

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

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.

C. Algorithm to embed confidential message into cover image file.

Algorithm to embed confidential message into cover image file named inFile generate new file with embedded message file named outFile.

Encoded-Message (msg,inFile on input-mode,outFile on output-mode)
Step 1:
Read offset bytes from input inFile and writes to output File outFile
Step 2:
Calculate message length and write it into output file by embedding using XOR function it in last two bits for every byte. Suppose, Message length being 16 bits, will be stored in 8 pairs of 2 bits.
Step 3:
Embed each byte of message in 4 pairs of 2 bits each is embedded in 4 byte of input file and written into output file named outFile.
Step 4:
Write the remaining bytes of the input file into output file.

D. Algorithm for generate of message from Image

The picture is received at receive side. This function decode message from a file named outFile open on output mode.Decode Message (outFile on Input-mode)
Step 1:
Read offset bytes from the input file and apply again XOR function, Generate message bit.
Step 2:
Read last 2 bits of consecutive 8 bytes and concatenate them to get the message length.
Step 3:
Read last 2 bits from input file in pairs of 4 and concatenate them to get message of 1 byte.
Step 4:
Repeat step 3 until the message is extracted of calculated length.
Step 5:
Decompress & Decrypt the message.

E. Procedure for detecting and correcting error

If any error occurred during the transmission of message, we can detect and correct using fuzzy error correcting code.

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

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

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

I. CONCLUSIONS

In this paper, we propose an effectivescheme by using the LSB matching method to embed secure data into the stegno-image. This approach uses stegnography, Cryptography – Double EHDES, Lossless Compression

– Sequitur and Error Correction Code – Fuzzy error correction code.

REFERENCES

[1.] 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

[2] Alain C. Brainos, A Study Of Steganography And The Art Of Hiding Information, East Carolina University, http://www.infosecwriters.com/text_resources/pdf/steganographyDTEC6823.pdf

[3] Niels Provos, Peter Honeyman, *Hide and Seek: Introduction to Steganography*,IEEE Security and Privacy,Volume 1 , Issue 3 (May 2003), Pages: 32 - 44

[4] Jessica Fridrich and Miroslav Goljan, *Digital image steganography using stochastic modulation*, Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY, 13902-6000, USA.

[5] Swarnendu Mukherjee, Swarnendu Bhattacharya, Amlan Chaudhury *Triple Layer Data Security* ACM Ubiquity, Volume 9, Issue 17, April 29-May 5 ,2008

[6] Zhao, J. *In business today and tomorrow,* ACM Communications of the ACM, p. 7, 1998.

[7] 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.

[8] 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)

[9] 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

[10] 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

[11] 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.

[12]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.

[13] 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.

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

[15].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

AUTHOR,

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.

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.

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.

Akshay Tyagi, Persuing Ph.D from Mewar University, Chittorgarh, Rajsthan, INDIA. He has more than five year experience in teaching and research as LECTURER. He is working at Gradute School of Business & Administration, Greater Noida, U.P., INDIA. The current research area is Cryptography& fuzzy commitment scheme.

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.Dr. Ojha is the member of Mathematical Society Banaras Hindu University, LMIAENG, LMIACSIT. He is the author/co-author of more than 50 publications in International/National journals and conferences.

