Improved Image Steganographic System by using Multiple Encryption and DWT

Manoj Kumar Ramaiya[1], Dr. Dinesh Goyal[2], Dr. Naveen Hemrajani[3]
Research Scholar, Computer Engineering, Suresh Gyan Vihar University, Jaipur, Rajasthan (India) [1]
Director, Center for Cloud Infrastructure & Security and Principal, Engineering, SGVU, Jaipur, Rajasthan (India) [2]
Head Computer Science Engineering, JECRC University, Rajasthan, Jaipur (India) [3]

Abstract— **The protection of data over unsecure transmission network has continually a key concern in the consideration of investigators or cyber professionals. With the fast promising practice of the internet in all personnel and professional drives, the distress for the unauthorized entrance by an intruder and the valuable information will be later exploitation, has further put pressure on the industry or researchers for developing methods and techniques to protect the information from intruders involves in unlawful activities or cybercrime.**

Cryptography is the art which deal with the transmuting a valuable and confidential information into inaudible forms. This unintelligible information might produce mistrustful in the observance of opponents when it transfers on open or unsafe communication networks and only legitimate receiver can only understand it meaning by decoding it. Conversely, Steganography embed confidential information or secrete message in to a cover image and hides its existence. As a common practice, hiding of secrete data into other media is apply in communication on text, image or multimedia contents for the purpose of digital signature, intellectual property protection and authentication.

Both Cryptographic and Steganographic methods delivers the adequate amount of security but are susceptible to intruder's attacks when information flow over unsafe communication channel. Efforts to combines these techniques i.e. Steganography and Cryptography, gives the ultimate results in security enhancement. The steganographic techniques currently used mainly emphasis on embedding mechanism with fewer attention to pre-processing of valuable information. Pre-processing of data offer robustness, high security level and flexibility. The suggested hybrid mechanism is exclusive method for image steganography based on multiple encryption using Triple Data Encryption Algorithm (TDEA) improving the security over unsecure transmission channel.

Index Terms— **Cryptography, Multiple encryption, TDEA, Digital Image Steganography, Discrete Wavelet Transforms.**

I. Introduction

Protection of secret information while transmitting it to legitimate receiver at a distance place has been in the considerations of despatchers since the ancient era, so very elementary to present day highly specific computer oriented techniques have been established. The former three to four decade led to the widespread transfer of information across every corner of the world. The remarkable evolution of the internet also produce and eased various E- Commerce applications. This demand the guarantee of safe keeping of data and any further misuse possible from this theft data. Further the communication between private parties demanding unconditional secrecy also demand the data transmission in improved or encoded mode.

In multimedia communication the requirement of secrecy and confidentiality increases additional significance primarily in open, unsecure communication channel like internet or intranet. Current age of worldwide connectivity, of viruses, intruders, eavesdropping and digital fraud or cyber-crime needs to safe-guard information from releasing into criminal hand.

Cryptographic systems [1,2] transforms a source message or secret information in to unintelligible form so it cannot be understand by intruders , while steganographic system hides the secret information in to other digital medium, so it cannot be apparent before the opponents. The term steganography [3, 4] derived from the Greek word *Steganos* which means *"covered"* and *Grafia* means *"writing"* i.e. Steganography means "covered writing" [5] . The secret information embed in to other media like cover image such that the resulting stego image should not diverge much from cover image. Cryptographic and Steganographic methods are widely used in the field of information hiding [7] and has acknowledged consideration from the commercial and academic world in the past. Former conceals the original data but latter conceal the very fact that data is hidden.

II. Related Works

Considering the strengths and weakness of cryptographic and steganographic, investigators tried to merging them, so that the new techniques would simultaneously retain the strength of steganography and cryptography while overcoming the respective deficiencies.

Manuscript received Aug, 2017.

Manoj Kumar Ramaiya*, Research Scholar, Computer Engineering, Suresh Gyan Vihar University Jaipur, Rajasthan (India), +919424062354.*

Dr. Dinesh Goyal*, Principal, School of Engineering, Suresh Gyan Vihar University, Jaipur, Rajasthan (India), +919887678379.*

Dr. Naveen Hemrajani*, Head, Computer Engineering, JECRC University, Jaipur, Rajasthan (India) +919829032657.*

The literature surveyed deal with methods involving only cryptographic methods or steganographic systems. Both of the methods have deficiency in terms of degree of safety and robustness against attacks. Effort to merging two methods to guarantee more secure encoding method will be made. In the most of the cases, methods involved works on plaintext and very fewer attempts been made to encode images.

Mostly suggested methods in literature survey involves cryptographic and steganographic, some of them related special domain while others is related to the transform domain. Shouchao Song et al. [7] suggested an algorithm by hybridization of cryptographic and steganographic methods based on Least Significant Bit toning method. The algorithm achieves the encryption and embedding in single stage which take less computation time as compare to existing methods. Another systems explain by Malik and Singh [8] encrypting the text using blowfish encryption algorithm and LSB technique of steganography which is non readable and secure further enhance the security.

Encryption of text using DES and data hiding using Least Significant Bit insertion, Seth Dhawal et al. [9] ensure more security over unsafe and open communication channel by hybridization of cryptographic and steganographic methods, they suggest the DES cryptographic algorithm used for text encryption and for embedding encrypted message in the cover image LSB substitution is used.

The techniques recommends compacting the signal before encrypting and employing steganographic techniques. Hikmat Farhat and Khalil Challita [10] offered multiple encryption. After Encryption the encrypted text secret message is embedding multiple cover images.

Ankit Uppal et al. [11] presented a new method by merging the RC5 enhance algorithm for encrypting the text message and Least Significant Bit method for embedding which result a highly secure communication method.

Dipti Kapoor Sarmah and Neha Bajpai[12] suggested an techniques by integrating AES encryption for secrete message. The resultant ciphertext is then embedded into the cover image by using Discrete Cosine Transform. The little modified techniques is offered by Pye Pye Aung and Tun Min Naing [13], using the same AES algorithm for encryption and this encrypted message is hide into cover image using DCT.

Literature reveals that a lot of research applying the idea of joining cryptographic and steganographic technique by first encrypting the secret information and then hiding it in the digital media are suggested. But they do the encryption and embedding is performed separately and no study employing them simultaneously have never been tried up until now.

Secondly most of the hybrid system uses cryptographic system to encrypt text message and hide the ciphertext by LSB steganography. To our information no techniques proposed cryptography for encrypting image (image encryption). Proposed system uses cryptographic techniques for encrypting secrete message i.e. image and then hiding this encrypted image is hide in to cover image by using LSB embedding.

III. Data Encryption Standard (DES) and Triple Data Encryption Standard (TDEA)

The DES Algorithm [14, 15, and 16] is designed to encryption and decryption blocks of data containing of 64 bits by using a 56-bit key. Decryption of block must be carried out using the identical key as used for encryption process, but ordered of using the key is reverse because the decryption method is the inverse of the encryption method. A block which is enciphered is inputted to an *IP* (initial permutation), then to special function based on permutation and substitution (*F*) and finally to an IP^{-1} (reverse initial permutation). The key based calculation termed as function f, also called the cipher function. The function K_S is called the key schedule. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions S_i and the permutation function *P*.

DES given the possible susceptibility to brute-force attack, there has been significant attention in finding an alternate to DES. One approach is to finding completely new algorithm and AES is example of that. Other alternative to use existing DES with multiple encryption and multiple keys. The initial standard that describes algorithm ANS X9.52 available in 1998 is “Triple Data Encryption Algorithm (TDEA)”. FIPS PUB 46-3 also describe 3-DES. Triple DES uses a key package that contain of three keys. K_1, K_2 and K_3 all of having 56 bits. These keys are applying in three different variant. The encryption of plaintext takes places as:

$$Ciphertext = EK_3\,(DK_2\,(EK_1\,(\,Plaintext)\,)\,)$$

Means DES first encrypt with K_1, secondly DES decrypt with K_2 and then DES encrypt with K_3. The plaintext will be recovered by decrypt with K_3 , encrypt with K_2 then decrypt with K1.

$$Plaintext = DK_1\,(EK_2\,(DK_3\,(\,Ciphertext)\,)\,)$$

Each triple DES encryption encrypt one block of 64 bits of data. The TDEA offer three different variants with respect to keys.

- All three Keys are independent
- K_1 and K_2 are independents and $K_3 = K_1$.
- All three keys are equal i.e. $K_1=K_2=K_3$.

Triple DES is beneficial because it has important sizes key length, which is longer than most key length associated with other encryption methods, i.e. 3×56=168 independent key bits ensuing in a dramatic increase in cryptographic strength and obvious to the meet-in-the-middle attack.

IV. Proposed Hybrid Model

Suggested steganographic method is based on TDEA (triple Data Encryption Algorithms) as depicted as follows:

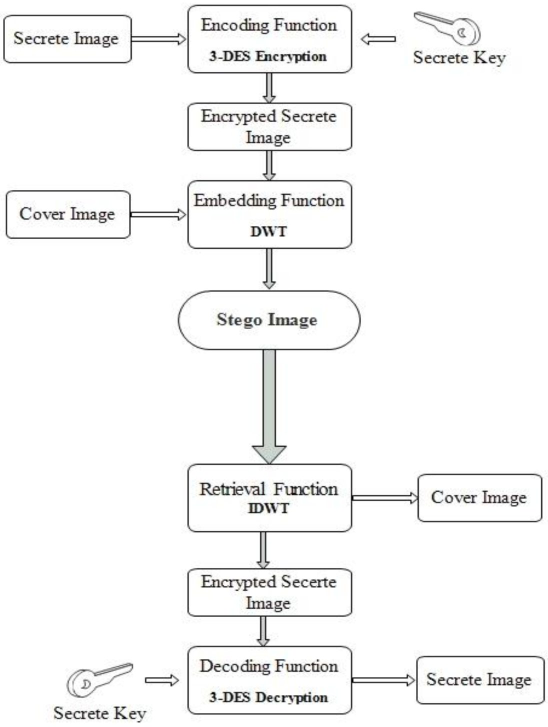

Figure 1. Proposed Steganographic Model

A. *Encoding Function using 3-DES Encryption*

Initially the secrete image is chosen for example (64×64). The intensity value of each pixel of secrete image is changed from decimal to binary. Now taking eight consecutive pixel values from secrete image, one block of 64 bits is formed. Input this block to triple DES encoding [18] function.

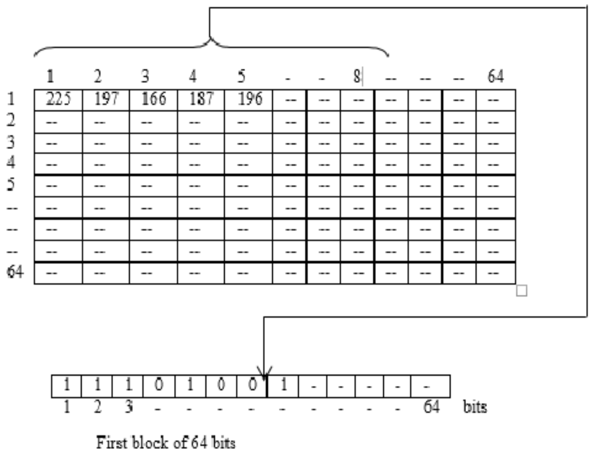

Figure 2. Formation of 64 Bit Block

One complete execution of Triple DES algorithm [17,18] with three keys gives eight pixel value of secrete image into respective pixel values of encrypted secrete image. Now taking next eight consecutive pixel next block of 64 bits is formed, again input this block to triple DES encoding function and get encrypted value of those pixels.

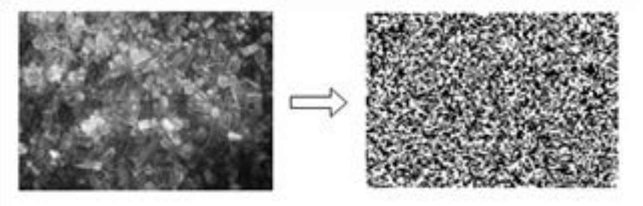

Figure 3. Output of Encoding function

B. *Embedding Function using one level DWT*

For embedding encrypted secrete image into cover image, 1- level DWT [19] of cover image is obtained. A two dimensional cover image is transferred into single level DWT. These decomposed HH, LH, LL and HL four bands are reorganized into column matrix representing the intensity of pixel value in decimal forms which in converted into respective binary for further use.

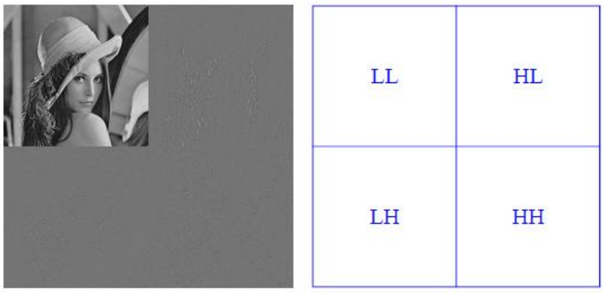

Figure 4. 1- Level DWT and Frequency Band

Now taking the encrypted image, the intensity values of every pixel are converted from decimal to binary. By taking the first pixel and divide this 8 bit value into 4 part taking 2 bits in each b1, b2, b3, b4 block.

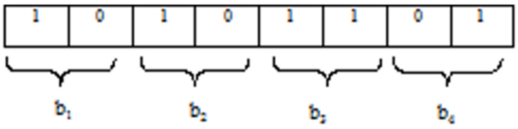

Figure 5. Bit Division

After receiving values of b_1, b_2, b_3, b_4 , these values are inserted into the four decomposed band of cover image as shown in figure. First two bits (b_1) are placed into the 2 bit LSB of the first pixel of LL band. Next two bit (b_2) are placed into the 2 bit LSB of the first pixel of HL band. Similarly b_3 and b_4 are placed into the 2 bit LSB of LH and HH band respectively.

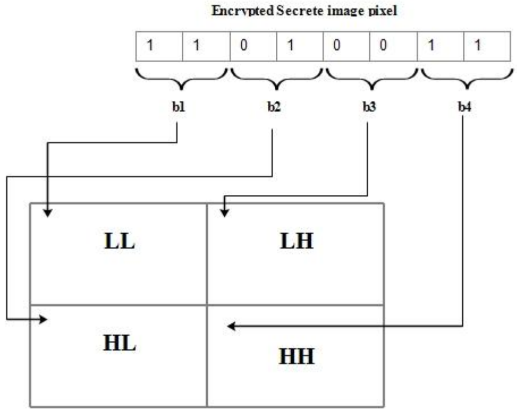

Figure 6. Block diagram of Bits Embedding

Likewise corresponding bits of secret image will be appended into the least significant bit of 1- level decomposed cover image. DWT decomposed cover image is represented with 8 bits in which MSBs are kept intact, only two bits lease significant bit are replaces by encrypted secrete image. Each pixel of secrete image is spread in cover image in such a way it provide more security and robustness.

Table 1: Encoding & Embedding Function

Input: A gray level Secrete Image (m × n), A gray Level Cover of size (2m × 2n);

Output: Stego Image of size (2m × 2n);

1. Input eight pixel value of the secrete image to form block of 64 bits to the image encoding Function (3- DES), which produces the encrypted secrete image.
2. Divide each pixel value of encrypted secrete image into 4 parts containing 2 bits each.
3. Decompose cover image by 1 – level Discrete Wavelet Transform (DWT) and append 2 bits of b1, b2, b3 and b4 in LL, HL, LH and HH band in respective pixel by replacing Least Significant Bit (LSB) of cover image taking pixel value one by one.
4. Reconstruct the processed image by using inverse discrete wavelet transform (IDVT) to produces stego image.
5. End.

C. Image Retrieval Function

At the receiving end, decoding of stego image perform the following process:

1. *Generate the 2 LSB bits from each band of the stego Image:* For extracting encrypted secrete image from stego image, 1- level DWT of stego image is obtained, which decompose the stego image into four band. These decomposed four bands are again reorganized into column matrix representing the intensity of pixel value in decimal value to respective binary value. The pixels value are handled one by one from the stego image and take 2 LSB bits from first pixel of each band.
2. *Concatenation of bits :* Now concatenating the input, the 8 bits of first pixel value of encrypted secrete image is acquired as

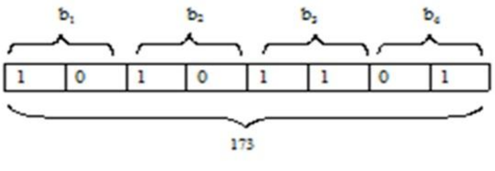

Figure 7. Concatenation of Bits

3. *Reformation of Encrypted Secrete Image:* Now the generated value is placed into first position. Similarly taking the next pixel value from each band of stego image, the process is repetitive and the whole encrypted secrete image is recovered.

D. TDEA Decoding Function for Creation of Secrete image

Now the eight successive pixel value from encrypted secrete image are again inputted to TDEA decoding function with same constraint and keys one by one (but used in reverse order) to obtained respective eight pixels value of original secrete image.

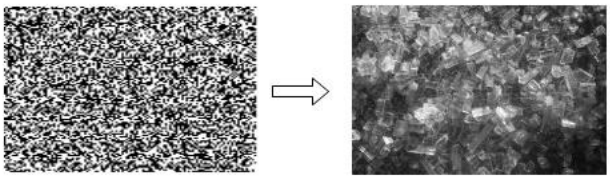

Figure 8. Output of Decoding Function

Table 2: Image Retrieval / Decoding Algorithm

Input: Stego Image of size (2m × 2n);

Output: A grey level Secrete Image (m × n);

1. Decompose stego image by 1 – level Discrete Wavelet Transform (DWT) and extract 2 bits LSB by taking first pixel value from each LL, HL, LH and HH band respectively.
2. Concatenated four 2bit (b1, b2, b3, b4) LSB to get 8 bits of each pixel of encrypted secrete image. Reconstruct encrypted secrete image.
3. By taking eight successive pixel value forming block of 64 bits are input to decoding Function (3DES) using keys value used in reverse order getting first eight pixel value of secrete image and so on.
4. End.

V. Results and Analysis

Proposed model is strong Steganography method because without knowing the secrete keys package the recovery of secrete image with the help of stego image is impossible. Furthermore cover image quality is also not degrading due to deviation in two LSB of each pixel which replicates only 0 – 3 difference in pixel value. Moreover the presented hybrid system is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

Table 3: Capacity and PSNR

Name of Image	**Size (Pixel)**	**Capacity**	**PSNR In DB**
Baboon.jpg	256 × 256	25 %	54.58
Cameraman.jpg	256 × 256	25 %	55.01
Lena.jpg	256 × 256	25 %	59.28
Pirate.jpg	256 × 256	25 %	56.32
Living_room.jpg	256 × 256	25 %	54.39

VI. Conclusion

The model of merging cryptographic and steganographic systems to achieve additional secure and robust data in employed. As a precursor, pre-processing is sustained to enhance security feature. The secret image to be transmitted is encrypted using well known encryption algorithms. The encrypted image is then hides into a cover image using steganographic techniques.

In order to improve the security during transmission over unsafe communication channel, pre-processing of secrete image proposes. The pre-processing encrypt the secrete image before being uses as input to be inserted into cover image maintaining the quality of the stego image as near as undistorted. This ensure that even if the steganographic technique fails and attacks to counter the embedding are employed, the extracted image is still in the encrypted shape. The time for encryption with DES and 3-DES algorithm is only 10 to 20% of the total time, thus additionally security is obtained with very small time overhead.

In the proposed 3-DES based steganographic model the strength of conventional DES and bundle of secrete key for encrypting secrete image, improves quality of image and security compare to existing systems. Steganography, especially combined with the cryptography is a powerful tool which enables to communicate safely with the little computational overload in the system. This model also counter to the meet in the middle attack with 168 bit key security.

ACKNOWLEDGMENT

The principal author acknowledgment is due to Dr. Dinesh Goyal, Principal, School of Engineering, Suresh Gyan Vihar University, Jaipur (India) and Dr. Naveen Hemrajani , Head Computer Engineering , JECRC University, Jaipur (India) for the valuable guidance, encouragement and blessing to carry the research.

REFERENCES

[1] Lt. James Caldwell, “Steganography”, CROSSTALK The Journal of Defence Software Engineering, pp. 25 – 27, June 2003.

[2] N. Provos and P. Honeyman, “Hide and Seek: an Introduction to Steganography”, IEEE Security and Privacy Vol 1 No. 3, pp.32–44, 2003.

[3] Ross J. Anderson and Fabien A.P. Petitcolas, “On The Limits of Steganography”, IEEE Journal of Selected Areas in Communications, Vol. 16 No. 4,pp 474-481, May 1998.

[4] Eugene T. Lin and Edward J. Delp, “A Review of Data Hiding in Digital Images”, CERIAS Tech Report, Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, pp.2086, 2001.

[5] J.C.Judge, “Steganography: past, present, future”, SANS Institute publication, /http://www.sans.org/reading_room/whitepapers/stenganography/552.phpS, 2001.

[6] N.F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen”, IEEE Computer Vol. 31 No. 2, pp.26–34, 1998.

[7] Shouchao Song, Jie Zhang, Xin Liao, Jiao Du and Qiaoyan Wen, “A Novel Secure Communication Protocol Combining Steganography and Cryptography”, Advanced in Control Engineering and Information Science , Procedia Engineering 15 , pp. 2767 – 2772, 2011.

[8] Ajit Singh and Swati Malik, “ Securing Data by Using Cryptography with Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 5, pp 404-409 , May 2013.

[9] Dhawal Seth, L. Ramanathan and Abhishek Pandey, “Security Enhancement: Combining Cryptography and Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, pp. 3-6, Nov 2010.

[10] Khalil Challita and Hikmat Farhat, “Combining Steganography and Cryptography: New Directions”, International Journal on New Computer Architectures and Their Applications (IJNCAA) Vol. 1 No., pp.199-208, 2011.

[11] Ankit Uppal, Rajni Sehgal, Renuka Ngapal and Aakash Gupta, “Merging Cryptography& Steganography Combination of Cryptography: Rc6 Enhanced Ciphering and Steganography: JPEG”, International Journal of Advanced Computational Engineering and Networking, Vol. 2, Issue-10, pp. 85-87, Oct.-2014.

[12] Dipti Kapoor Sarmah and Neha Bajpai, “Proposed System for Data Hiding Using Cryptographyand Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, pp. 7- 10, Oct 2010.

[13] Pye Pye Aung and Tun Min Naing, “ Novel Secure Combination Technique of Steganography and Cryptography”, International Journal of Information Technology, Modeling and Computing (IJITMC), Vol. 2, No. 1. Pp 55-62, February 2014.

[14] E. Thambiraja , G. Ramesh and R. Umarani , “A Survey on Various Most Common Encryption Techniques” , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7 , pp. 226-233, July 2012.

[15] William M. Daley and Raymond G. Kammer, “Data Encryption Standard (DES)”, Federal Information Processing Standards Publication FIPS Pub 46-3 National Institute Of Standards And Technology, pp. 1-22, 25 October 1999.

[16] D.Coppersmith, “The Data Encryption Standred (DES) and its Strength against attack”, IBM Journal Research Development, Vol 38,No. 3, pp. 243- 250, May 1994.

[17] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, “Security Improvisation in Image Steganography using DES”, 3rd IEEE International Advance Computing Conference (IACC), pp.1082 – 1087, 2013.

[18] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, “Improvisation of Security aspect in Steganography applying DES ”, IEEE International Conference on Communication Systems and Network Technologies (CSNT – 2013) , pp. 431 – 436, 2013.

[19] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.

BIOGRAPHY

Manoj Kumar Ramaiya received the B.E. in Computer Science & Engineering degree from Barakatullah University, Bhopal in 1997 and M.Tech in Computer Science & Engineering degree from Rajeev Gandhi Prodhyogiki Vishvidyalaya, Bhopal in 2006. He have 18 years teaching experience in the field of computer science and currently pursuing Ph.D. degree from Suresh Gyan Vihar University, Jaipur. Research Area of interest are Image Steganography, Cryptography, Information and Network security.

Dr. Dinesh Goyal, Director, Center for Cloud Infrastructure & Security and Principal, Engineering, SGVU, Jaipur, Rajasthan (India). He received the B.Tech degree from M.B.M. Engineering College, Jodhpur (Raj.), M.Tech from Arya College of Engineering & IT and Ph.D. from Suresh Gyan Vihar University Jaipur (Raj.). He have 18 years’ experience of research and academics. He have expertise in Information Security, Image Processing and Cloud Computing and has written more than 60 international and national paper of good quality. He have published 1 books and 2 patent.

Dr. Naveen Hemrajani , Professor and Head of the Department , Computer Science and Engineering, JECRC University , Jaipur, Rajasthan (India). He did B.E, M.Tech and Ph.D. in Computer Science and Engineering. He have 25 years’ experience of research and academics. He have expertise in Computer Network and Software Engineering and has written more than 62 international and national paper of good quality and published 2 books.