An Approach to Image Compression with Partial Encryption without sharing the Secret Key

Abdul Razzaque [1] **and** **Dr. Nileshsingh V.Thakur**[2]

[1] PG Scholar, Department of Computer Science & Engg. [2] Associate Professor, Department of Computer Science & Engg.

[1,2]Shri Ramdeobaba College of Engineering & Management, Nagpur, India

Summary

Existing methods when employ compression there is no consideration of security, similarly when it describe encryption there is no consideration of size i.e. compression. In this paper a simultaneous image compression and encryption scheme is discussed. The order of the two processes viz. compression and encryption is EC i.e. image encryption is performed first then the image compression is applied. For image encryption a symmetric key cryptography multiplicative cipher is used. Similarly for compression Discrete Cosine Transform is used. In the proposed approach a private key cryptography is used for encryption without sharing the secret key. But image transmission is required two times. Therefore to save the bandwidth partial encryption is carried out. Image compression is concerned with minimizing the number of bit required to represent an image. Image Encryption is hiding image from unauthorized access with the help of secret key that key can be private or public.

Key words

Image Compression, Image Encryption, Secret Key

1. Introduction

We are dealing with large amount of data in the field of image processing. Image compression algorithms use to reduce the amount of data required to represent a digital image and the basis of the reduction process is the removal of spatial and psychovisual redundancies. Mathematically, visual data compression typically involves transforming (encoding) a 2-D pixel array into a statistically uncorrelated data set. Two types of compression are lossless compression and lossy compression. If same image can be generated from the compressed image then it is *Lossless* compression otherwise it is *Lossy* compression.

However alone compression is not sufficient as it has an open access, anybody can access it. So if it is desired that it can be accessible only by authorized person it should be encrypted as well. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography. If same key is used for encryption and decryption then it is called as *Symmetric key cryptography* and if the different key is used for encryption and decryption then it is called as *Asymmetric key cryptography*.

The paper contains an approach to apply image compression with encryption using secret key which need not shared. The order followed in this paper is EC i.e. encryption followed by compression. For encryption a private key cryptography using multiplicative inverse is applied. For compression Discrete Cosine Transform (DCT) is used. Partial encryption is carried out to save the bandwidth since image is transmitted twice

The paper is organized as follows: Section 2 discusses the classification and description research work on image compression and encryption schemes. Section 3 describes the proposed approach. Section 4 shows experimental setup and result. Finally in Section 5 the conclusion is described.

2. Classification and Description of Research Work on Image Compression and Encryption

The literature work can be categorized with respect to the application of the two processes image compression and image encryption as:

2.1 Compression followed by Encryption (CE)

In this sequence an intruder have less clues to access image but encryption may again increase the size. The related work on CE approach is as follows.

1. Howard Cheng, Xiaobo li [1] performed compression using Quadtree compression Algorithm. But partial encryption is applied. Only 13–27% of the output from quadtree compression algorithms is encrypted for typical images, and less than 2% is encrypted for 512×512 images compressed by the set partitioning in hierarchical trees (SPIHT) algorithm. Suitable for image as well as video compression but limitation is that a different scheme has to be designed and analyzed for each compression algorithm.
2. Masanori Ito *et al*. [2] proposed a method combining encryption and compression based on Independent Component Analysis (ICA) and Discrete Cosine

Manuscript received July 5, 2012
Manuscript revised July 20, 2012

Transform (DCT). In their method for encryption, target images are covered with an insignificant image to hide them and their mixtures to be transmitted are obtained. The receiver reconstructs the original images applying some Independent Component Analysis (ICA) algorithm to the mixed images. For compression process they used DCT and simple low pass filter. Using the proposed method the higher frequency components are cut off, that is, the quality of the original image is reduced.

3. Younggap You, Hanbyeori Kim [3] performed compression using DWT (Discrete Wavelet Transform). For encryption Standard Encryption algorithm AES or ARIA is used. Algorithm is suitable for Medical image and video. It is fault tolerant algorithm to alleviate error avalanche effect due to the erroneous bits in the received encrypted image data.

4. A. Alfalou C. Brosseau *et al.* [4] performed compression based on the discrete cosine transform (DCT). Two levels of encryption are used. The first one is due to the grouping of the DCTs in the spectral domain and after a second transformation, i.e. to hide the target images, one of the input images is used as encryption key. The compression is better than JPEG in terms of PSNR. The proposed method achieves PSNR as 21.7186 on Lena image compared to that of JPEG as 20.6904.

5. N. V. Thakur and O. G. Kakde [5] proposed the compression and encryption based on the fractal coding and spiral architecture but the compression method are lossy. Additionally to reduce time complexity of fractal coding FFT based cross correlation is used. Any specific encryption method is not specified and any stream cipher algorithm can be used. Regression can be used for the encryption or even partial encryption is also possible Fractal coding is applicable for gray level however they consider the RGB color image as the combination of three gray level images. Their experimental results are better than that of quadtree method with respect to PSNR ratio and encoding time.

2.2 Encryption followed by Compression (EC)

In this sequence size is not again increased but an intruder may have more clues to access the image. The related work on EC approach is as follows.

1. A. Kingston *et al.* [6] proposed a technique which takes advantage of the Mojette transform properties. In their method standard encryption techniques, such as AES, DES, 3DES, or IDEA can be applied to encrypt very small percentages of high resolution images and can transmit uncorrelated data along with the encrypted part. Entropy coding is used for lossless compression. The compression ratios provided by the proposed technique cannot compete with lossless JPG2K but advantage is that the percentage of encrypted data can very strongly be reduced allowing the use of public key encryption algorithms, such as RSA.

2. Anil Kumar A, Anamitra Makur [7] suggested that compression of encrypted data is possible by using distributed source coding. They considered the encryption, followed by lossless compression of gray scale and color images. Decompression and decryption are performed in a single phase. They achieved compression ratios varying from 1.5 to 2.5 despite encryption. On Lena image they obtained the compression result as 5.39 bits per pixel.

3. Fawad Ahmed *et al.* [8] used encryption scheme that relies on some very interesting properties of orthogonal matrices containing columns that form a set of orthonormal basis vectors. Compression is performed using JPEG. Image format is not an issue in this method. The proposed scheme has the capability to recover the plaintext-image from the cipher image even if the cipher-image data is compressed using JPEG lossy compression. Encryption algorithm can also be adjusted to produce cipher-image with varying perceptual distortion.

4. Mingyu Li *et al.* [9] used a RC5 stream cipher based scalable encryption scheme for low complexity transparent transcoding. CCSDS compression method is used which consist of two part DWT and Bit plane coding. Advantage is that Encryption is scalable.

5. V. Radha, D. Maheswari [10] proposed image encryption algorithm consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete states variables of chaotic maps. Discrete Cosine transform is used for compression. The proposed algorithm is strong in providing security and is also very fast. Since the key space is large therefore the attacker cannot decrypt an encrypted image without the correct key.

2.3 Joint Compression and Encryption (JCE)

This approach is in use these days, which may be fast as compared to previous two but procedure is complicated. The related work on JCE approach is as follows.

1. A. Alfalou *et al.* [11] used DCT to jointly compress and encrypt the image with a new system able to amalgamate spectral information. That spectral fusion, nondestructive, allows the compression and the encryption of information at the same time. Authors also showed that it is possible to use the DCT to jointly realize a compression and an encryption of the data by spectral fusion thus allowing a very important gain in transmission time.

2. Yunpeng Zhang *et al.* [12] Compression is carried out using JPEG2000 & uses chaotic system to encrypt the coefficient-bit and the context according to the plane coding. Since it is carried out at the same time as coding/decoding, the scheme makes the compression ratio influence small and also retains the original compression algorithm’s stream elasticity, and also enjoys low cost and high security.

3. Maher Jridi, Ayman Alfalou [13] proposed a method that exploits the DCT properties to achieve the compression and the encryption simultaneously. First for compression, 8-point DCT applied to several images. Second, only some special points of DCT outputs are multiplexed. For the encryption process, a random number is generated and added to some specific DCT coefficients. This algorithm needs only 4 multiplications to compute relevant DCT output data. The FPGA implementation of the whole method shows improvements in terms of throughput, area and power consumption. A compression ratio higher than 65% and a PSNR about 28 dB are achieved.

4. Abraham Jun Jiang Lock *et al.* [14] performed image compression which is based on fractal image coding with little modification. Private Key cryptography using new method ‘Fractal Encryption’ is used. Encryption uses Mandelbrot Set. Fractal compression can provide higher compression ratio and fractal encryption can provide strong protection against the attacks.

5. Shiguo Lian *et al.* [15] proposed a totally different scheme. They carried out partial encryption before and after compression. JPEG is used for image compression. Using Chaotic stream cipher encryption is carried out. Encryption consists of three parts: color plane Confusion, Sign encryption and DCT coefficient confusion space. They achieved the 75% compression ratio and 7.6% encryption time ratio on Lena image of size 256X256.

4. Proposed Approach

In our proposed method experiment on some standard gray level images of size 512×512 is carried out. Secured image compression is performed by applying encryption followed by compression. The advantage of the proposed method is that the encryption and decryption of image is carried out at sender and receiver side without exchanging or sharing the secret key. But image transmission is required twice so to save the bandwidth partial encryption is done. For encryption any symmetric key cryptosystem can be used like AES, DES or multiplicative cipher. The experiments are performed using multiplicative cipher. Similarly for compression and decompression any lossless compression technique can be used. The experiments are performed using DCT (Discrete Cosine Transform).

The block schematic of the proposed scheme is shown in Fig. 1.

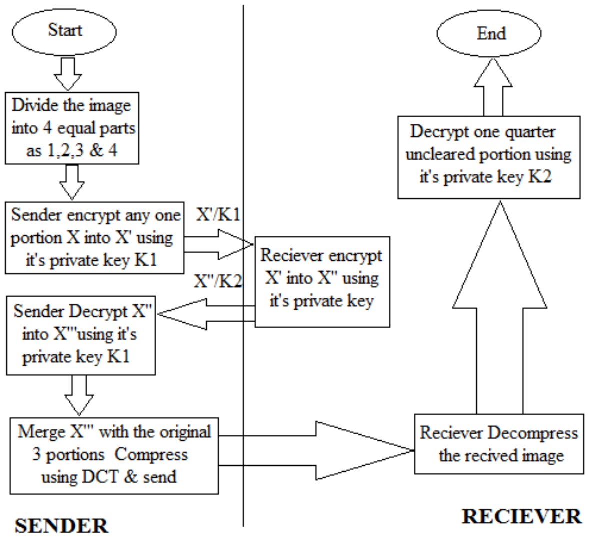

Start
Divide the image into 4 equal parts as 1,2,3 & 4
Sender encrypt any one portion X into X' using it's private key K1
X'/K1
Reciever encrypt X' into X'' using it's private key
X''/K2
Sender Decrypt X'' into X'''using it's private key K1
Merge X''' with the original 3 portions Compress using DCT & send
Reciever Decompress the recived image
Decrypt one quarter uncleared portion using it's private key K2
End
SENDER
RECIEVER

Fig. 1 Block Schematic of the proposed Approach

The idea of encryption is based on the locking system shown in Fig. 2. The problem is how A sends some valuable item to B in a locked box without sending his key so that X cannot get it.

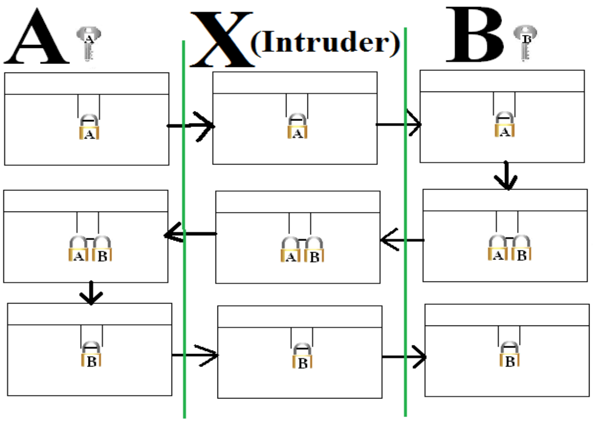


Fig. 2 Locking system without exchanging Key

The steps followed are as follows.

(i) Consider a standard gray level image of size 512×512 for experiment.

(ii) Divide the image into four equal blocks of size 256×256.

(iii) Encrypt any one of the important portion from the above four portions using sender’s own secret key K1 and send.

(iv) Receiver again encrypts the received image using his own secret key K2 and send back to sender.

(v) Sender decrypts it using its secret key then merges it with the three original portions. And after compression sends it to receiver.

(vi) Receiver decompresses the received image. Within that image one quarter portion of the image is in encrypted form which can be decrypted using its own secret key to retrieve the original image.

4. Experimental Setup and Result

The proposed compression and encryption mechanism is implemented with MATLAB 7.11.0(R2010b) and windows 7 operating system with i5 processor and 4GB RAM. The experiments are carried out on some standard gray level images of size 512×512 like Lena.bmp, Boat.gif, Lena.tif, Jetplane.gif and Mandril.tif. The performance evaluation factors compression ratios R and PSNR values obtained for different images is tabularized in table 1. The time requirement for compression and decompression algorithm is summarized in table 2. Similarly the time requirement for encryption and decryption is summarized in table 3. Since encryption is performed without any key exchange, the encryption time shown in the table3 includes encryption time by sender, encryption time by receiver and decryption time by sender on one quarter portion of image.

Table 1: Evaluation factors of proposed scheme on different images

Sr. No.	Standard Sample Image	Compression Ratio R	PSNR (dB)
1	Lena.bmp	8	30.0174
2	Boat.gif	8	28.3148
3	Lena.tif	8	26.5618
4	Jetplane.gif	8	23.4517
5	Mandril.tif	8	23.3837

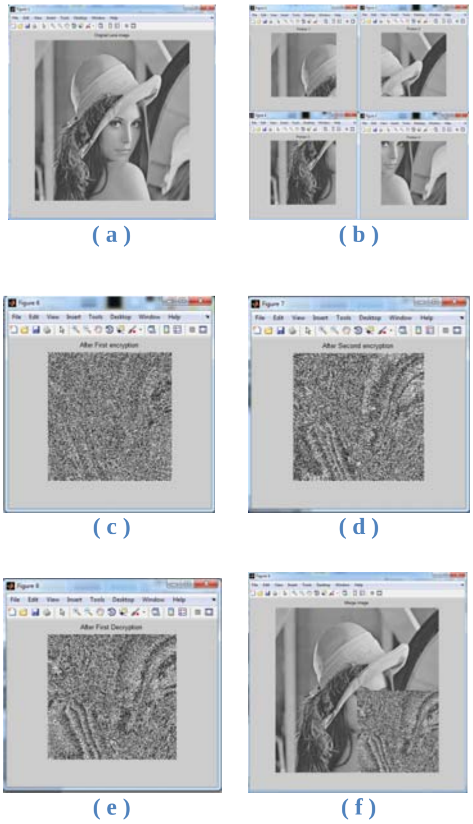
Table 2: Time for compression and decompression of different images

Sr. No.	Standard Sample Image	Compression time (Sec)	Decompression time (Sec)
1	Lena.bmp	0.203489	0.813930
2	Boat.gif	0.054794	0.077499
3	Lena.tif	0.052739	0.077758
4	Jetplane.gif	0.054085	0.075309
5	Mandril.tif	0.052745	0.080169

Table 3: Time for encryption and decryption of different images

Sr. No.	Standard Sample Image	Encryption time (Sec)	Decryption time (Sec)
1	Lena.bmp	1.304011	0.074329
2	Boat.gif	2.626828	0.029273
3	Lena.tif	4.637949	0.028381
4	Jetplane.gif	4.121273	0.028106
5	Mandril.tif	4.008271	0.028738

Two of the output results on Lena.bmp and Mandril.tif are shown in figure 3 and 4 respectively.



(a) (b)

(c) (d)

(e) (f)

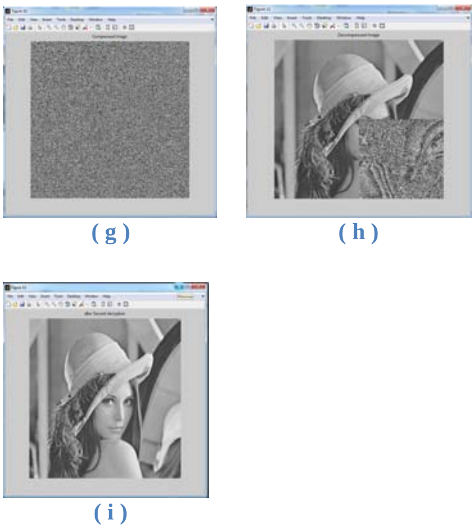
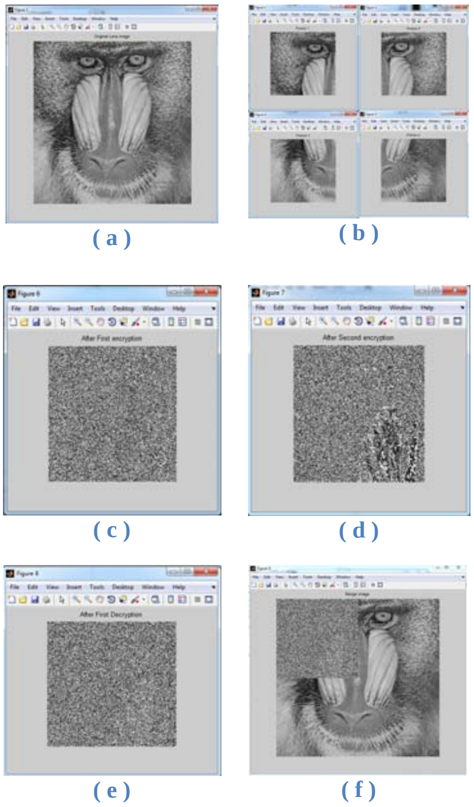


Fig. 3 (a) Original Lena.bmp image (512×512) (b) After dividing into four equal portions. (c) Encrypted form of the 3rd portion by sender (d) Encrypted form of the received portion by receiver (e) Decrypted form of the received portion by sender. (f) Merged image with one portion encrypted and 3 original portions. (g) After compression by DCT (h) After decompression by IDCT (i) Output image after applying decryption by receiver.



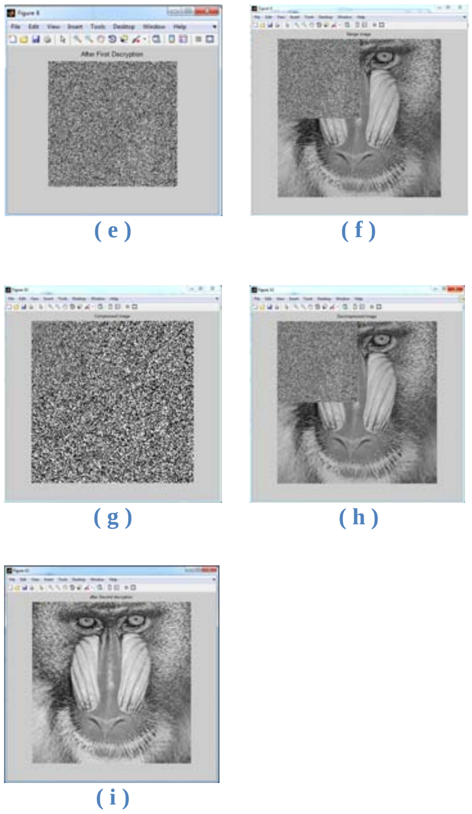


Fig. 4 (a) Original Mandril.tif image (512×512) (b) After dividing into four equal portions. (c) Encrypted form of the 1st portion by sender (d) Encrypted form of the received portion by receiver (e) Decrypted form of the received portion by sender. (f) Merged image with one portion encrypted and 3 original portions. (g) After compression by DCT (h) After decompression by IDCT (i) Output image after applying decryption by receiver

5. Conclusion

In this paper, many of the current important image compression and encryption techniques have been presented and analyzed. The best way of fast and secure transmission is by using compression and encryption of multimedia data like images.

The research works have been categorized in the following three categories based on the order of the two process viz. CE, EC or JCE.

Encryption applied by different researchers by means of encrypting algorithm which encrypt the entire or partial multimedia bit sequence using a fast conventional cryptosystem . Much of the past and current research targets encrypting only a carefully selected part of the image bitstream in order to reduce the computational load, and yet keep the security level high.

Thus image encryption is performed without exchanging the secret key on the cost of some more bandwidth requirement. PSNR value is different for different images. Compression ratio R is 8 which is constant for DCT. This security scheme can be used anywhere where time is not a constraint, even image can be fully encrypted. By applying the same scheme any advance encryption method like AES or DES can also be used.

The performance evaluation factors are PSNR ratio and coding decoding time for compression and encryption respectively. But the balancing parameter for the combined process is not yet been defined.

References

[1] Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and Videos" IEEE Transactions On Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000

[2] Masanori Ito, Noboru Ohnishi, Ayman Alfalou and Ali Mansour, "New Image Encryption And Compression Method Based On Independent Component Analysis", IEEE, 2007

[3] Younggap You, Hanbyeori Kim,"Endoscopy Image Compression and Encryption under Fault Tolerant Ubiquitous Environment" 978-1-4244-4918-7 IEEE, pp. 165-168, 2009

[4] A. Alfalou C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images", OPTICS EXPRESS 24024Vol. 19, No. 24 OSA, 2011

[5] N. V. Thakur, and O. G. Kakde, "Compression Mechanism for Multimedia System in consideration of Information Security" Proceeding of International workshop on Machine intelligence Research MIR Day GHRCE-Nagpur, India, pp. 87-97, 2009

[6] A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, " Lossless Image Compression And Selective Encryption Using A Discrete Radon Transform" IEEE-1-4244-1437-7/07,ICIP, pp.IV 465-468, 2007

[7] Anil Kumar A and Anamitra Makur, "Distributed Source Coding based Encryption and Lossless Compression of Gray Scale and Color Images" ,IEEE978-1-4244-2295-1, 760 MMSP Singapore, pp. 760-764, 2008

[8] Fawad Ahmed, M Y Siyal and Vali Uddin Abbas,"A Perceptually Scalable and JPEG Compression Tolerant Image Encryption Scheme", Fourth Pacific-Rim Symposium on Image and Video Technology 978-0-7695-4285-0/ IEEE pp. 232-238, 2010

[9] Mingyu Li, Xiaowei Yi and Hengtai Ma, "A Scalable Encryption Scheme for CCSDS Image Data Compression Standard" 978-1-4244-6943-7/ IEEE pp. 646-649, 2010

[10] V. Radha, D. Maheswari, "Secured Compound Image Compression Using Encryption Techniques", 978-1-4244-5967-4/ IEEE 2010

[11] A. Alfalou, A. Loussert, A. Alkholidi, R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimize image transmission", ISEN-BREST Laboratory L@BISEN, France, IEEE, 2007

[12] Yunpeng Zhang, Zhengjun Zhai, Xiaobin, "Bit-encryption Algorithm for JPEG2000 Image Based on Chaos", 2009 IEEE International Conference on Control and Automation Christchurch, New Zealand, December 9-11, 2009 978-1-4244-4707-7/ IEEE pp. 1521-1526, 2009

[13] Maher Jridi and Ayman AlFalou, "A VLSI Implementation of a New Simultaneous Images Compression and Encryption Method", IEEE-978-1-4244-6494-4/10, 2010

[14] Abraham Jun Jiang Lock, Chong Hooi Loh, Siti Hasanah Juhari, Azman Samsudin, "Compression-Encryption Based on Fractal Geometric", Second International Conference on Computer Research and Development, 978-0-7695-4043-6/ IEEE pp. 213-217, 2010

[15] Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "A Novel Image Encryption Scheme Based-on JPEG Encoding", Proceedings of the Eighth International Conference on Information Visualisation (IV'04) 1093-9547/IEEE, 2004

Abdul Razzaque received the Bachelor of Engineering degree in Computer Technology from Manoharbhai Patel Institute of Engineering & Technology Gondia, India in 2002. Presently he is pursuing his PG (M.Tech) in Computer Science and Engineering from Shri Ramdeobaba College of Engineering & Management, Nagpur, India. His research interest includes image processing and network security He is having 8 years of teaching experience. He is a life member of ISTE New Delhi India

Nileshsingh V. Thakur received Bachelor of Engineering degree in Computer Science Engineering from Government College of Engineering, Amravati, India and Master of Engineering degree from College of Engineering, Badnera under Amravati University and Sant Gadge Baba Amravati University in 1992 and 2005 respectively. He received Ph.D. degree in Computer Science Engineering under Department of Computer Science Engineering from Visvesvaraya National Institute of Technology, Nagpur, India on 1st February, 2010. His research interest includes image processing, sensor network, computer vision, pattern recognition, artificial neural network and evolutionary approaches. He is having over 20 years of teaching and research experience. Presently, he is Associate Professor in Department of Computer Science and Engineering at Shri Ramdeobaba College of Engineering and Management, Nagpur, India. He is the author or co-author of more than 40 scientific publications in International Journal, International Conferences and National Conferences. Dr. Thakur is a member of editorial board of over eight International journals; also, he is the life member of ISTE, India, IAENG and IAEME. He also worked as the reviewer for international journals and conferences.