Development of a Scalable Coding for the Encryption of Images using Diagonal Min-Max Block Truncation Code

Jeya Bright Pankiraj, Vishnuvarthanan Govindaraj, Pallikonda Rajasekaran Murugan, Arun Prasath Thiyagarajan

***Abstract:** This paper proposes a scalability coding on encrypted images, especially resolution scalability on lossy compression images. In the compression stage, the input gray level image is compressed using Diagonal Min-Max Block Truncation Coding technique. The compressed input image is encrypted using pseudorandom numbers masked by modulo-256, and then the encoded bit streams are transmitted. The pseudorandom numbers generated will be the encrypted key and the same is shared to the receiver. In the receiver side, the encoded bit stream is decrypted by using the shared encrypted key, which gives the compressed pixel value. Then the original image is reconstructed by using Diagonal Min-Max Block Truncation Coding Technique.*

***Keywords:** Diagonal Min-Max Block Truncation Coding, Image Encryption, Lossy Compression, Scalable Coding.*

I. INTRODUCTION

Image encryption and Image Compression play a vital role between transmitter and receiver. The purpose of image encryption is to protect the data from a hacker or intruder. In [1], the study about cryptographic primitives for existing solutions, challenges in multimedia content protection and issues in signal processing for processing of encrypted signals have been made. In [2], elaboration regarding the usage of Discrete Fourier Transform and homomorphic properties for processing the encrypted signals and thus, protecting the valuable signals have been done. In [3], encryption of signals is done through secure protocols using LMS algorithm. In [4], protection of sensitive signals through untrusted device is done through composite signal method by packing many signal samples and processing an unique sample. An invisible watermarking technique is introduced such that if illegal copies sold can be identified and proved by dispute resolution protocol [5]. In [6], a new watermarking technique for image encryption by using fingerprint image as an encrypted key by the seller such that the fingerprint is shared to the receiver, and the encrypted image can be decrypted by using fingerprint by the buyer have all been discussed [6].

Nowadays, usage of image data requires higher storage space, which leads to increase in bandwidth requirement. Image compression plays an inevitable role in reducing the size of storage space and bandwidth. The size of storage space can be reduced by removing the redundant data and it can be achieved by using Image compression techniques. Redundant data are nothing but irrelevant data or replication of a data in the digital image. Coding redundancy, Interpixel redundancy and Psychovisual redundancy are the three types of data redundancy present in digital images. These redundancies are eliminated through image compression without compromising the quality of the image. Totally, 10% of storage size is reduced through image compression. There are two broad categories of image compression techniques namely, lossless image compression and lossy image compression. Lossless image compression is useful in image archiving as in the storage of legal and medical records. Hence, the image is compressed and decompressed without losing information. Lossy compression is useful in many applications where minimum error is acceptable and the compression performance will be increased. Psychovisual redundant data are data's in which certain information has less relative importance than other information in normal visual processing. Lossy compression techniques are used to remove psychovisual redundant data which cannot be noticed by human eye. In [7], reversing the order from traditional way such that first encrypting and then compressing the data is possible without reduction in compression efficiency are proved. Similarly, in [8], the given data is first encrypted and then compressed during encoding and at receiver joint; decompression and decryption are carried out without the knowledge of memoryless source, and also with sources using Markov correlation for the error detection during decoding.

In [9], compression is carried out on grey level and color images, and it is achieved by dividing the image into bit planes, and discussion is made regarding the exploiting spatial and cross-plane correlation and possibility of correlation in color bands. In [10], lossy compression on encrypted data is possible by using compressive sensing technique and it can be performed on any linear operation are proposed. In [11], image encryption is done using pseudorandom permutation, and then the compression is achieved by removing excessive rough and fine information coefficients, and the principal content is reconstructed by

Revised Manuscript Received on December 16, 2019.
* Correspondence Author
Jeya Bright Pankiraj*, ECE, Kalasalingam Academy of Research and Education (Kalasalingam University), Srivilliputhur, India. Email: jeyabright@gmail.com
Vishnuvarthanan Govindaraj, BME, Kalasalingam Academy of Research and Education (Kalasalingam University), Srivilliputhur, India. Email: gvvarthanan@gmail.com
Pallikonda Rajasekaran Murugan, ECE, Kalasalingam Academy of Research and Education (Kalasalingam University), Srivilliputhur, India. Email: m.p.raja@klu.ac.in
Arun Prasath Thiyagarajan, Kalasalingam Academy of Research and Education (Kalasalingam University), Srivilliputhur, India. Email: arun.aklu@gmail.com

updating the coefficients iteratively.

Scalability is achieved by manipulating bit stream. Various types of scalability are there in which resolution scalability is used in Lossy Compression. Scalability is done on unencrypted images. In [12], a scalable image coder with reversible integer wavelet transform used for compression of images is proposed, since it has the advantage of generating embedded bitstream and though which resolution scalability is achieved for lossy images. The decoder will convert the lower resolution images to higher resolution to get the reconstructed image better. In [13], Scalable coding on unencrypted images is achieved by using EBCOT algorithm which exhibits resolution scalability and SNR Scalability. Scalable coding on encrypted images is reported by [14], Scalable coding for encrypted images is reported first, in which image compression is done by Hadamard Transform and then the compressed pixel value is added with encrypted key which is generated by pseudorandom number generator and then the encoded bitstreams are transmitted. At the decoding stage, the encoded bitstreams are decrypted by using encrypted key, which is shared by the transmitter and then the principal content is rebuilt by means of Hadamard Transform. In [16], BTC technique was used to do the operation of scalable coding on encrypted images in which the input image is compressed by using BTC technique first and then encryption process is done by pseudorandom number technique, and then the encoded bitstreams are transmitted along with the encrypted key. The decoder will first decrypt the received bitstream by the shared encrypted key, and then the principal content is rebuilt at receiver using BTC technique. Even though this technique has lower computational complexity, but it has lower PSNR, wPSNR, compression ratio, bit error rate and higher MSE and wMSE.

In this paper we propose a new technique called Diagonal Min-Max Block Truncation Coding (DMMBTC). In the proposed method, the input gray image is compressed by using DMMBTC technique and then the compressed pixel value is encrypted by pseudorandom number technique, and then the encoded bit streams are transmitted along with the encrypted key to the buyer. The gray image has a pixel value range between “0” and “255”. Pseudorandom number generator will generate a pixel value between “0” and “255” for the input image size which is taken as encrypted key. The compressed pixel value and the encrypted pixel value are added together to obtain the encoded bitstream. In the decoder, the encoded bitstream is first decrypted using encrypted key and then the extracted compressed pixel value is used to reconstruct the principal content using DMMBTC Technique. Our proposed method has lower computational complexity and improved PSNR, wPSNR, compression ratio, bit error rate, MSE and wMSE. This technique is widely acceptable since it favours parallel processing, and coding of each block is totally independent.

II. PROPOSED METHOD

The Diagonal Min-Max Block Truncation coding is shown in Fig.1. In this, the input gray image is compressed by using Min-Max Block Truncation Coding Technique. The output of compression will have values “0” and “1” in binary form. Then we encrypt the compressed pixel value through Image encryption technique before transmission. The image encryption process is carried out by using pseudorandom phenomena. The random numbers are generated between the values between 0 and 255 for the given image size. Then the encrypted pixel values and compressed pixel values are added together and the encoded bit stream is transmitted. The encrypted key is chosen as secret key and shared to receiver. Then during the decoding stage at receiver, the first stage is image decryption process. The shared secret key namely the

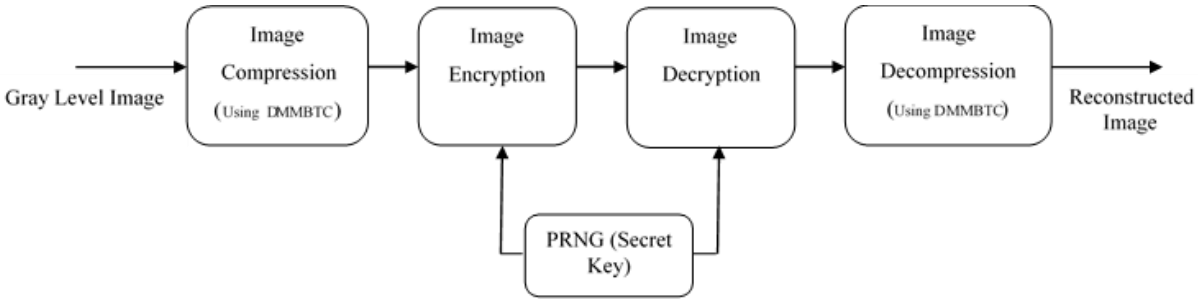

Fig.1. Proposed System

Encrypted key is used for decryption. The secret key pixel value is subtracted with the encoded pixel value and the output will be the decrypted pixel value which is in binary form. The decrypted pixel value is nothing but the compressed pixel value. Then by using DMMBTC technique, the original input image is reconstructed. The reconstructed image is better than existing technique and reflects higher resolution and improved compression ratio, PSNR, wPSNR, MSE, wMSE and bit error rate.

A. Image Encoding

Image Compression

The input image is taken as gray image of size G1*G2 of rows and columns. As we know that the gray level pixel values are in the range between 0 and 255, the input image pixel values will also have the same range. The Diagonal Min-Max Block Truncation Coding technique has the following steps: -

Step1: - The input image chosen size is 512*512 and divided into non-overlapping blocks of size G*G typically, 4 * 4.
Step 2: - Get the diagonal maximum ($dhval$) and minimum value ($dlval$) for each non-overlapping blocks.
Step 3:- Calculate the threshold value ($dmval$) as given by

$$dmval = \left(\frac{dhval + dlval}{2}\right) \quad (1)$$

Step 4: - Construct the binary block by assigning value "1" for pixel values greater than or equal threshold value and "0" for values less than threshold value for each non-overlapping blocks. The binary block built is denoted as dmb_i and the bit amount value is 8N, which is given as:

$$dmb_i(i,j) = \begin{cases} 1, & GraylevelPixelvalue \geq dmval \\ 0, & GraylevelPixelvalue < dmval \end{cases} \quad (2)$$

Image Encryption

Image encryption process is done with the help of pseudorandom number generator. The random numbers between the values 0 and 255 of size G1*G2 are generated by pseudorandom number generator. The length of the sequence is 8N. The random number generated will be used as an encryption key and shared to the receiver. The compressed pixel value and encrypted pixel value are added together to obtain the encoded bit stream. The encoded bit stream is checked with modulo-256 operations to ensure that encoded pixel values are within the range 0 and 255. If the values are greater than 255, then it is subtracted with the 256 value. Then the resultant encoded bit stream is transmitted.

$$edm(i,j) = mod[dmb(i,j) + rdm(i,j), 256] \quad (3)$$
$$1 \leq i \leq G_1, \quad 1 \leq j \leq G_2$$

Where, $dmb(i,j)$ is the compressed value, $rdm(i,j)$ is the secret key and $edm(i,j)$ is the encrypted values. Along with the encoded bit stream, the secret key, diagonal maximum value and the diagonal minimum value of each block values are transmitted. Fig. 2(a) and Fig.2(b) show the input gray image and its encrypted image.

Fig.2(a). Original Image

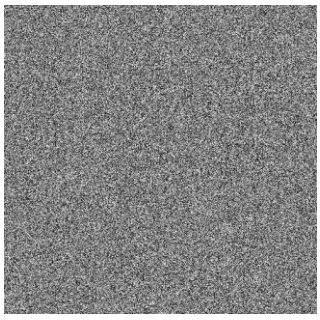

Fig.2(b). Encrypted Image

B. Image Decoding

Image Decryption

The encoded bit stream is first decrypted through the image decoding process. In the Image decryption process, we subtract the encoded bit stream with encrypted key pixel value and then taking modulo 256 operations for each non-overlapping block. The decrypted pixel value will be in binary form having values "0" and "1" for each non-overlapping block. The decrypted pixel value is nothing but the compressed pixel value of each non-overlapping block. The expression for image decryption is given in equation 4.

$$dmd(i,j) = mod[edm(i,j) - rdm(i,j), 256] \quad (4)$$

Where, $edm(i,j)$ represents the transmitted encoded pixel value and $rdm(i,j)$ represents the secret key which is shared by the transmitter, and $dmd(i,j)$ is the decrypted pixel value. The decrypted pixel value contains the binary values "0" and "1".

Image Reconstruction

The Diagonal Min-Max Block Truncation Coding method is used in the process of Image Reconstruction. The diagonal maximum value and the diagonal minimum value of each non overlapping block are obtained from the transmitter. In the decrypted pixel value, the binary value "1" is replaced by diagonal maximum value ($dhval$) and the binary value "0" is replaced by diagonal minimum value ($dlval$) for each non-overlapping block. By this way, the original image content is rebuilt and the equation to rebuild the original image content is given as below:

$$dmout(i,j) = \begin{cases} dhval, & dmd(i,j) = 1 \\ dlval, & dmd(i,j) = 0 \end{cases} \quad (5)$$

Where, $dhval$ is the diagonal maximum value of each non-overlapping block and $dlval$ is the diagonal minimum value of each non-overlapping block, respectively. The decrypted image and the reconstructed image are shown in Fig.3(a) and Fig. 3(b).

Fig.3(a). Decrypted Image

Fig.3(b). Reconstructed Image

III. EXPERIMENTAL RESULTS AND DISCUSSION

i. Reconstructed Image using BTC

Fig. 4(a) and Fig.4(b) show the original image and the reconstructed image using Diagonal Min-Max Block Truncation Coding Technique. This method uses resolution scalability such that higher resolution image is reconstructed. The experimental results show that the reconstructed image is similar to the original image.

Fig.4(a). Original Image
Fig.4(b). Reconstructed Image

ii. Comparison Parameters

Compression Ratio (CR):

The equation to calculate compression ratio is given as:

$$Compression\ Ratio = \frac{file\ size\ of\ uncompressed\ image}{file\ size\ of\ compressed\ image} \quad (6)$$

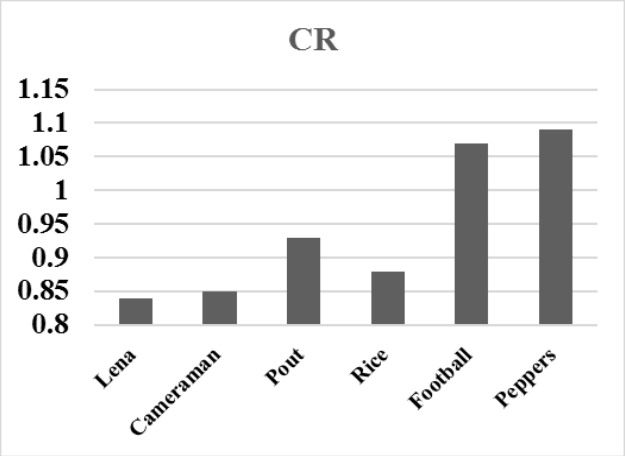

Fig.5. CR for Various Input Images

The Fig.5 shows the results of CR for various input images.

Bit Rate (BR):

The equation to calculate bit rate is given as:

$$bit\ rate = \frac{b}{compression\ ratio} \quad (7)$$

Where, b is an uncompressed image bit per pixel. The Fig.6 shows the results of BR for various input images.

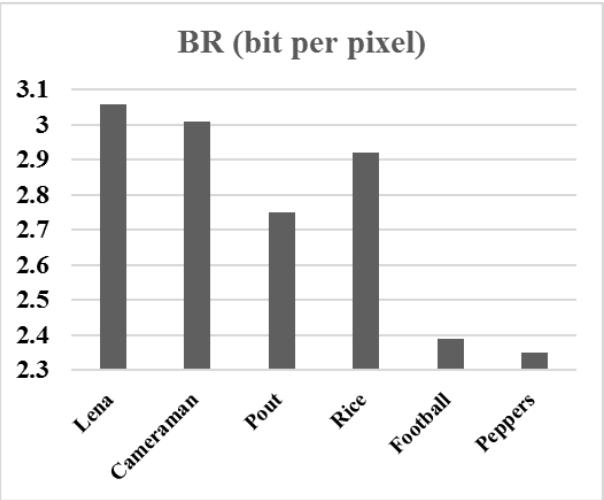

Fig.6. BR for Various Input Images

Mean Square Error (MSE)

The equation to calculate MSE is given as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[dmout(i,j) - dmin(i,j)]^2 \quad (8)$$

Where, $dmout(i,j)$ is the reconstructed principal content, and $dmin(i,j)$ is the original principal content and m and n are size of rows and columns.. The Fig.7 shows the results of MSE for various input images.

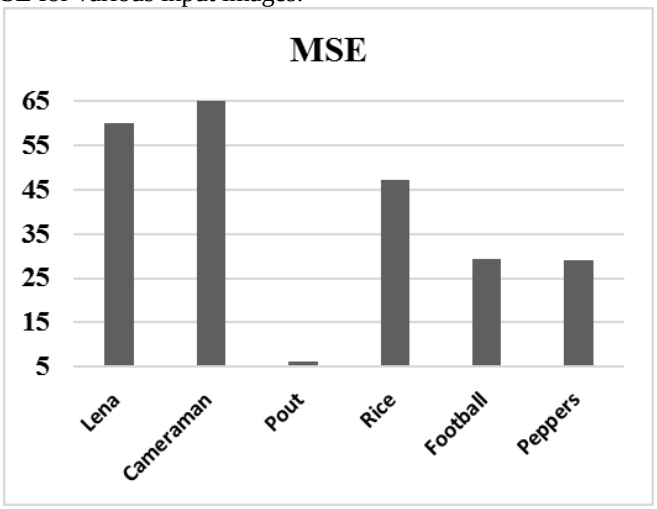

Fig.7. MSE for Various Input Images

Weighted Mean Square Error (wMSE):

The equation to calculate wMSE is given as:

$$wMSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(2\left|\frac{dmout(i,j) - dmin(i,j)}{dmout(i,j) + dmin(i,j)}\right|\right)^2 \quad (9)$$

Where, $dmout(i,j)$ is the reconstructed principal content and $dmin(i,j)$ is the original principal content and m and n are size of rows and columns. The Fig.8 shows the results of wMSE for various input images.

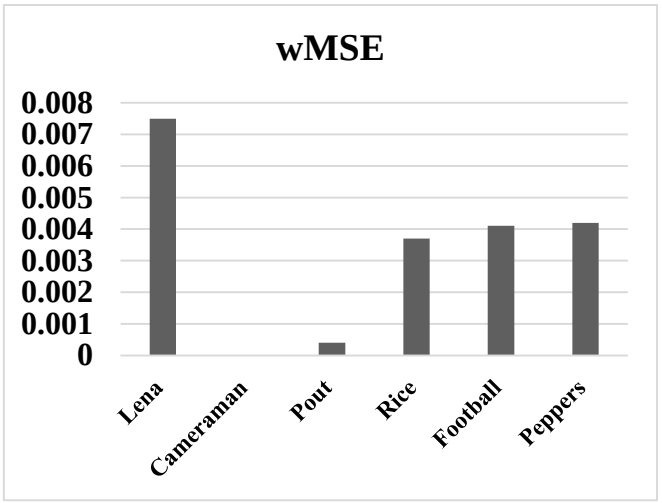

Fig.8. wMSE for Various Input Images

Peak Signal to Noise Ratio (PSNR):

The PSNR ratio will reflect the quality of reconstructed image. PSNR ratio is inversely

proportional to MSE and lower value of MSE will achieve higher PSNR ratio.

The equation to calculate PSNR is given as:

$$PSNR = 10\ log_{10} \frac{255^2}{MSE} \quad (10)$$

Where, MSE represents Mean Square Error. The Fig.9 shows the results of PSNR for various input images.

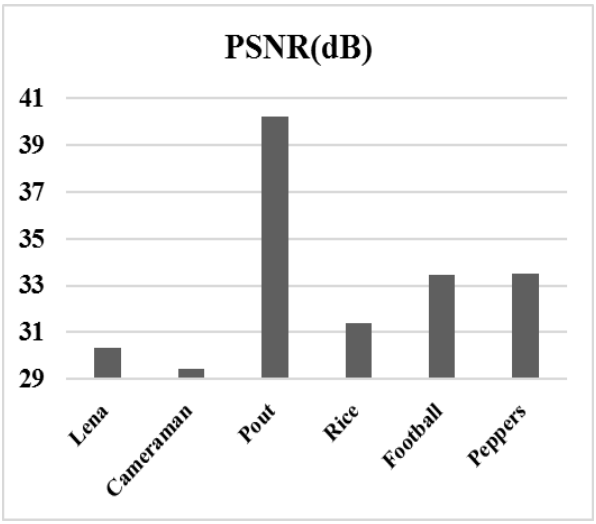

Fig.9. PSNR for Various Input Images

Weighted Peak Signal to Noise Ratio (wPSNR)

The equation to calculate wPSNR is given as:

$$wPSNR = 10\ \log_{10}\left(\frac{255^2}{wMSE}\right) \quad (11)$$

Where wMSE is the weighted Mean Square Error. The Fig.10 shows the results of wPSNR for various input images.

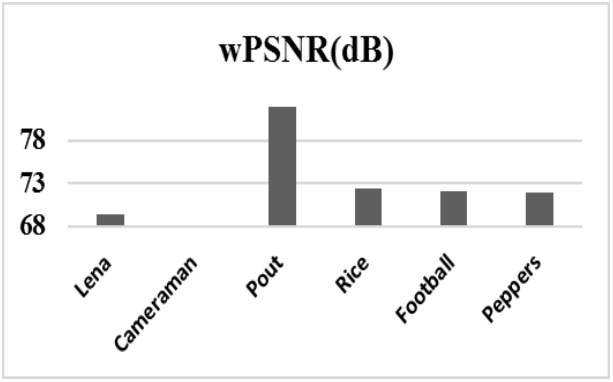

Fig.10. wPSNR for Various Input Images

Table I given below shows the results of comparison parameter values for various input images using DMMBTC.

Table- I: Comparison Parameter values for Input Images

INPUT IMAGE	CR	BR	MSE	wMSE	PSNR	wPSNR
Lena	0.84	3.06	60.10	0.0075	30.34	69.40
Cameraman	0.85	3.01	74.32	-	29.42	-
Pout	0.93	2.75	6.19	0.0004	40.21	81.84
Rice	0.88	2.92	47.27	0.0037	31.38	72.45
Football	1.07	2.39	29.23	0.0041	33.47	72.04
Peppers	1.09	2.35	28.95	0.0042	33.51	71.95

IV. CONCLUSION

In this paper, we have proposed a new method namely the Diagonal Min-Max Block Truncation Coding Technique for scalable coding on encrypted images. In this method, diagonal minimum value and diagonal maximum value of each non-overlapping block are chosen as quantizers and it exhibits better quality of the reconstructed image. In this method the input gray image is compressed by Diagonal Min-Max Block Truncation Coding Technique and then the compressed pixel value is encrypted by using pseudorandom number technique in which, generated pseudorandom number is taken as encrypted key. Then the encoded bit stream is transmitted along with encrypted key. In decoder, image decryption is done by decrypting the encoded bit stream with encrypted key and thus compressed pixel value are both extracted. Then the principal content is rebuilt by using Diagonal Min-Max Block Truncation Coding Technique. This technique is experimented on various images such as Lena, Cameraman etc. and the results for parameters such as Compression ratio, Bit rate, PSNR, wPSNR, MSE and wMSE are measured and listed in Table 1. The computational complexity of our proposed method is lower than existing methods since threshold value is diagonal maximum values and diagonal minimum values and also the same values are used for reconstruction purpose. Our method supports parallel processing because coding of each block is independent, and the computational complexity will be much lower. The experimental results of our proposed method showed better compression ratio, Bit rate, PSNR, wPSNR, MSE and wMSE. Our method shows that reconstructed image quality is equivalent to the original input image.

We have chosen diagonal minimum value and diagonal maximum value as the threshold value to construct the binary block, and also the same values serve as a quantizer to reconstruct the principal content. This can be modified further for better results.

REFERENCES

1. Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP J. Inf. Security, vol. 2007, Jan. 2007, pp. 1–20.
2. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, Mar. 2009, pp. 86–97.
3. J. R. Troncoso-Pastoriza and F. Pérez-González, "Secure adaptive filtering," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, Jun. 2011, pp. 469–485..
4. T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, Mar. 2010, pp. 180–187.
5. N. Memon and P. W. Wong, "A buyer-seller watermarking protocol,"IEEE Trans. Image Process., vol. 10, no. 4, Apr. 2001, pp. 643–649.
6. M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Trans. Image Process., vol. 14, no. 12, Dec. 2005, pp. 2129–2139.

7. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, Oct. 2004, pp. 2992–3006.
8. D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., Allerton, IL, 2005.
9. R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in Proc. 16th EUSIPCO, Lausanne, Switzerland, Aug. 2008.
10. A. Kumar and A. Makur, "Lossy compression of encrypted image by Compressing sensing technique," in Proc. IEEE TENCON, 2009, pp. 1–6.
11. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, Mar. 2011, pp. 53–58.
12. A. Bilgin, P. J. Sementilli, F. Sheng, and M. W. Marcellin, "Scalable image coding using reversible integer wavelet transforms," IEEE Trans.Image Process., vol. 9, no. 11, Nov. 2000, pp. 1972–1977.
13. D. Taubman, "High performance scalable image compression with EBCOT," IEEE Trans. Image Process., vol. 9, no. 7, Jul. 2000, pp. 1158–1170.
14. Xinpeng Zhang, GuoruiFeng, YanliRen and Zhenxing Qian, "Scalable Coding of Encrypted Images," IEEE Trans Image Process., vol 21, no 6, June 2012, pp. 3108-3114.
15. Edward J. Delp and O. Robert Mitchell, "Image Coding Using Block Truncation Coding,"IEEE Transactions on Communications, vol 27, no 9, Sep 1979, pp. 1335-1342.
16. P.Jeya Bright and Dr G.Vishnuvarthanan, "Development of scalable coding for the encryption of Images using Block Truncation Code," In Proceedings of 3rd International Conference on Trends in Electronics and Informatics (ICOEI 2019), Tirunelveli, India, Apr 2019, pp. 934-938. [IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8]

AUTHORS PROFILE

Jeya Bright Pankiraj is a part time research scholar in Department of Electronics and Communication Engineering at Kalasalingam Academy of Research and Education. He was born in 1973 and had his schooling in Nagercoil, Kanyakumari District, Tamilnadu..He received his BE in Electronics and Communication Engineering in 1994 from Madurai Kamaraj University (Mohammed Sathak Engineering College) and ME in Applied Electronics in 2013 from Anna University, Chennai (University College of Engineering, Trichy). He completed his Master of Business Administration in Education Management in 2017 from Alagappa University, Karaikudi and currently pursuing Ph.D in Kalasalingam Academy of Research and Education in the field of Image Processing. He has 10 years' experience in Mainframes with 3 years worked in USA and 15 years teaching experience and presently working as Associate Professor and Head, ECE Department, DMI Engineering college, Aralvoimozhi, Kanyakumari District. He is a member of Institute of Electrical and Electronics Engineers (IEEE)..

Dr G Vishnuvathanan born in 1986, has research stints in the avenues of medical image processing and artificial intelligence. He was awarded PhD in the year 2015 and bachelor's degree in Instrumentation and Control Engineering by 2007, and Master's Degree in VLSI by 2009. He has more than ten years of teaching and research experience and has his affiliation as Associate Professor with the Department of Biomedical Engineering of School of Bio and Chemical Sciences in the Kalasalingam Academy of Research and Education, Tamilnadu, India.

Pallikonda Rajasekaran Murugan, Born in Srivilliputhur, Virudhunagar District of Tamil Nadu in 1980, he had his schooling in the same town and graduated in Electronics and Instrumentation Engineering in 2001 from Shanmugha College of Engineering, Thanjavur and completed his M.Tech. degree in 2002 with second Rank in SASTRA University. He pursued his doctoral programme in Anna University, Chennai. Starting as a Lecturer in 2003, he became Asst. Professor in 2008, Associate Professor in 2009 and Professor in 2012 in Kalasalingam Academy of Research and Education. He had a deep involvement in Bio-signal Processing research. His work on the Image Segmentation for identification of brain tumour and image reconstruction and compression using medical images for diagnosis. Over 150 B.Tech students, 75 M.Tech students, and 8 Doctorates stand testimony for his productivity in Image Processing, Wireless Sensor Networks, and Biomedical Instrumentation research. He has so far published more than 50 papers in national and international journals and conferences. He is a Fellow of Indian Society For Technical Education (ISTE), Institute of Electrical and Electronics Engineers (IEEE), Asia-Pacific Chemical, Biological& Environmental Engineering Society (APCBEES), Institution of Engineers (India)(IE), International Association of Engineers (IAENG) and International Association of Computer Science and Information Technology (IACSIT).

Dr.T.Arun Prasath, is an Associate professor in Department Biomedical Engineering at Kalasalingam Academy of Research and Education. Dr.T.ARUNPRASATH received his Ph.D. in Electronics and Communication Engineering from Kalasalingam University, Krishnankoil in 2015, his M.E. in Applied Electornics from Anna University in 2009 (Mohamed Sathak Engineering College) and his B.E. in Electrical and Electronics Engineering from Anna University (Syed Ammal Engineering College) in 2006. Dr.T.ARUNPRASATHresearch interests include biomedical instrumentation, image processing, image segmentation cloud computing, image segmentation. He has published 16 technical journals and 20 technical papers in refereed conferences in these areas.He is a life member of ISTE.